ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61800-5-2— 2015

СИСТЕМЫ СИЛОВЫХ ЭЛЕКТРОПРИВОДОВ С РЕГУЛИРУЕМОЙ СКОРОСТЬЮ

Часть 5-2

Требования функциональной безопасности

**(IEC 61800-5-2:2007,
Adjustable speed electrical power drive systems —
Part 5-2: Safety requirements — Functional,
IDT)**

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 58 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2015 г. № 2221-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61800-5-2:2007 «Системы силовых электроприводов с регулируемой скоростью. Часть 5-2. Требования функциональной безопасности» (IEC 61800-5-2:2007 «Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном 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 (*gost.e-ecolog.ru

© Стандартинформ, 2016

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 и цель применения ... 1
2 Нормативные ссылки ... 2
3 Термины и определения ... 3
4 Предусмотренные функции безопасности ... 8
4.1 Общие положения ... 8
4.2 Функции безопасности ... 8
5 Управление функциональной безопасностью ... 10
5.1 Цель ... 10
5.2 Жизненный цикл разработки СЭРС (СБ) ... 10
5.3 Планирование функциональной безопасности ... 11
5.4 Спецификация требований безопасности СЭРС (СБ) ... 12
6 Требования к проектированию и разработке СЭРС (СБ) ... 14
6.1 Общие требования ... 14
6.2 Требования к проектированию СЭРС (СБ) ... 15
6.3 Поведение при обнаружении сбоев ... 21
6.4 Дополнительные требования к передаче данных ... 22
6.5 Требования к интеграции и тестированию СЭРС (СБ) ... 23
7 Информация для применения ... 23
7.1 Информация и инструкции для применения СЭРС (СБ) в системах безопасности ... 23
8 Верификация и подтверждение соответствия ... 25
8.1 Общие положения ... 25
8.2 Верификация ... 25
8.3 Подтверждение соответствия ... 25
8.4 Документация ... 25
9 Требования к проведению испытаний ... 25
9.1 Планирование проведения испытаний ... 25
9.2 Документация по испытаниям ... 25
10 Модификация ... 26
10.1 Цель ... 26
10.2 Требования ... 26
Приложение А (справочное) Таблица последовательности выполнения задач ... 27
Приложение В (справочное) Пример определения *PFH* ... 31
Приложение С (справочное) Доступные базы данных интенсивностей отказов ... 40
Приложение D (справочное) Список сбоев и методы их предотвращения ... 41
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации ... 51
Библиография ... 53

Введение

В результате развития производства и его автоматизации, что приводит к снижению физического труда, элементы систем управления оборудованием и производством играют все возрастающую роль в достижении полной безопасности. Такие системы управления используют все более сложные электрические/электронные/программируемые электронные устройства и системы.

Наиболее важными среди этих устройств и систем являются системы силовых электроприводов с регулируемой скоростью (СЭРС), которые можно использовать в связанных с безопасностью промышленных применениях [СЭРС (СБ)].

Примерами таких промышленных применений являются:

- станочные системы, роботы, оборудование для производственных испытаний, испытательные стенды;
- бумагоделательные машины, оборудование для текстильного производства, каландры в резинотехнической отрасли;
- производственные линии для изготовления изделий из пластмасс, металла, химической продукции, для металлопрокатных заводов;
- камнедробилки для изготовления цемента, цементные печи, миксеры, центрифуги, экструдеры;
- сверлильные станки;
- конвейеры, погрузочно-разгрузочные устройства материалов, подъемное оборудование (подъемные краны, порталы подъемных кранов и т. д.);
- насосы, вентиляторы и т. д.

Настоящий стандарт также могут применять разработчики, использующие СЭРС (СБ) для других применений.

Специалисты, использующие настоящий стандарт, должны знать, что некоторые стандарты типа С для машинного оборудования в настоящее время ссылаются на ИСО 13849-1 в случаях, связанных с безопасностью систем управления. Поэтому производители СЭРС (СБ) могут требовать дополнительную информацию (например, категорию и/или уровень безопасности), чтобы упростить интеграцию СЭРС (СБ) в связанные с безопасностью системы управления таким машинным оборудованием.

Примечание — «Стандарты типа С» определены в ИСО 12100-1 как стандарты безопасности механического оборудования, рассматривающие подробные требования безопасности для конкретного механического оборудования или группы таких машин.

Ранее, в отсутствие стандартов, было не принято применять электронные и, в особенности, программируемые электронные устройства и системы для реализации связанных с безопасностью функций из-за неуверенности в характеристиках безопасности таких технологий.

Существует много ситуаций, где системы управления, которые включают СЭРС (СБ), используются, например, в качестве мер безопасности, обеспечивающих достижение необходимого снижения риска. Типичный случай — защитная взаимная блокировка, чтобы исключить опасные ситуации для персонала, где доступ к опасной зоне возможен, только когда вращающиеся детали достигли безопасного состояния. Настоящий стандарт содержит методологию, которая определяет вклад СЭРС (СБ) в специфицируемые функции безопасности, обеспечивает соответствующее проектирование СЭРС (СБ) и верификацию, а также достижение требуемых рабочих характеристик.

Представлены меры, связывающие характеристики безопасности СЭРС (СБ) с необходимым снижением риска, учитывая вероятности и последствия от случайных и систематических сбоев.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ СИЛОВЫХ ЭЛЕКТРОПРИВОДОВ С РЕГУЛИРУЕМОЙ СКОРОСТЬЮ

Часть 5-2

Требования функциональной безопасности

Adjustable speed electrical power drive systems.
Part 5-2. Functional safety requirements

Дата введения — 2016—11—01

1 Область и цель применения

Настоящий стандарт определяет требования и дает рекомендации для проектирования и разработки, интеграции и подтверждения соответствия СЭРС (СБ), применяя методологию функциональной безопасности. Настоящий стандарт применяется к системам силовых электрических приводов с регулируемой скоростью, описанных в других частях комплекса стандартов МЭК 61800.

Примечание — Термин «интеграция» относится к самой СЭРС (СБ), а не к ее включению в связанное с безопасностью применение.

Настоящий стандарт применим только там, где требуется функциональная безопасность СЭРС (СБ), а СЭРС (СБ) работает в режиме с высокой интенсивностью запросов или в непрерывном режиме (см. 3.10). Для применений с низкой интенсивностью запросов см. МЭК 61508.

Настоящий стандарт, который является стандартом на изделие, рассматривает связанные с безопасностью вопросы СЭРС (СБ) в соответствии с методологией МЭК 61508 и устанавливает требования к СЭРС (СБ) как к подсистемам, связанной с безопасностью системы. Настоящий стандарт предназначен для того, чтобы облегчить реализацию электрических/электронных/программируемых электронных (Э/Э/ПЭ) элементов СЭРС (СБ) в соответствии с показателем безопасности функции(й) безопасности PDS.

Производители и поставщики СЭРС (СБ), используя нормативные требования настоящего стандарта, укажут пользователям (интеграторам системы управления, разработчикам оборудования и предприятия и т. д.) показатели безопасности для их оборудования. Это облегчит включение СЭРС (СБ) в связанную с безопасностью систему управления, создаваемую на принципах МЭК 61508 и, возможно, на их применении в конкретных секторах (например, представленных в МЭК 61511, МЭК 61513, МЭК 62061) или ИСО 13849.

Соответствие с настоящим стандартом означает выполнение всех требований МЭК 61508, которые необходимы для СЭРС (СБ).

Настоящий стандарт не определяет требования для:

- анализа опасностей и риска для конкретного применения;
- идентификации функции безопасности для этого применения;
- начального распределения значений УПБ для этих функций безопасности;
- приводного оборудования, за исключением интерфейсов;
- вторичных (производных) опасностей (например, от отказов в процессе изготовления или производства);
- электрической, тепловой и энергетической безопасности, которые рассмотрены в МЭК 61800-5-1;
- процесса производства СЭРС (СБ);
- подтверждения соответствия сигналов и команд для СЭРС (СБ).

Примечания

1 Требования функциональной безопасности СЭРС (СБ) зависят от применения и должны рассматриваться как часть полной оценки риска установки. Если поставщик СЭРС (СБ) также не несет ответственность за

Издание официальное

приводное оборудование, то разработчик установки ответственен за оценку риска и за определение функциональных требований и требований к полноте безопасности СЭРС (СБ).

2 Даже при том, что злонамеренные действия могут повлиять на функциональную безопасность СЭРС (СБ), вопросы защиты в настоящем стандарте не рассматриваются.

Настоящий стандарт применяется только к СЭРС (СБ), реализующих функции безопасности, со значением УПБ не больше, чем 3.

На рисунке 1 представлены функциональные элементы СЭРС (СБ), которые рассматриваются в настоящем стандарте.

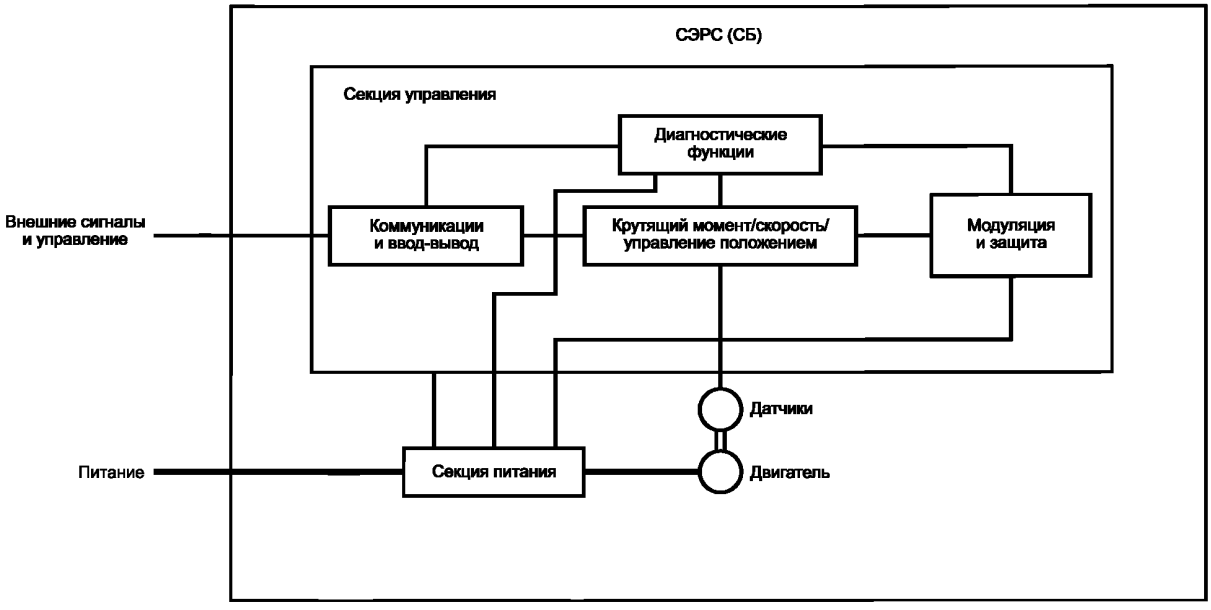


Рисунок 1 — Функциональные элементы СЭРС (СБ)

Примечание — На рисунке 1 показано логическое представление СЭРС (СБ), а не ее физическое представление.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие документы (для датированных ссылок следует использовать указанное издание, для недатированных ссылок — последнее издание указанного документа, включая все поправки к нему).

Примечания

1 Это не означает, что требуется соответствие со всеми разделами используемых нормативных ссылок, скорее настоящий стандарт делает ссылку на то, что остается непонятным в отсутствие ссылочных документов.

2 Ссылки на различные части МЭК 61508 недатированные, кроме тех, где указаны конкретные пункты.

МЭК 60204-1, Безопасность оборудования. Электрооборудование машин. Часть 1. Общие требования (IEC 60204-1, Safety of machinery — Electrical equipment of machines — Part 1: General requirements)

МЭК 61508 (все части), Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью (IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems)

МЭК 61508-1:1998[1)], Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования (IEC 61508-1:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements)

[1)] Отменен. Действует МЭК 61508-1:2010.

МЭК 61508-2:2000[1)], Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к электрическим, электронным, программируемым электронным системам, связанным с безопасностью (IEC 61508-4:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2. Requirements for electrical/electronic/programmable electronic safety-related systems)

МЭК 61508-3:1998[2)], Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению (IEC 61508-3:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements)

МЭК 61508-5:2000[3)], Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности (IEC 61508-5:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5. Examples of methods for the determination of safety integrity levels)

МЭК 61508-6:2000[4)], Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3 (IEC 61508-5:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6. Guidelines on the application of IEC 61508-2 and IEC 61508-3)

МЭК 61508-7:2000[5)], Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Анализ методов и средств (IEC 61508-7:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures)

МЭК 61800-1, Системы силовых электроприводов с регулируемой скоростью. Часть 1. Общие требования. Номинальные технические характеристики низковольтных систем электроприводов постоянного тока с регулируемой скоростью (IEC 61800-1, Adjustable speed electrical power drive systems — Part 1: General requirements — Rating specifications for low voltage adjustable speed d.c. power drive systems)

МЭК 61800-2, Системы силовых электроприводов с регулируемой скоростью. Часть 2. Общие требования. Номинальные технические характеристики низковольтных систем силовых электроприводов переменного тока с регулируемой частотой (IEC 61800-2, Adjustable speed electrical power drive systems — Part 2: General requirements — Rating specifications for low voltage adjustable frequency a.c. power drive systems)

МЭК 61800-3, Системы силовых электроприводов с регулируемой скоростью. Часть 3. Требования к электромагнитной совместимости и специальные методы испытаний (IEC 61800-3, Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods)

МЭК 61800-4-2002, Системы силовых электроприводов с регулируемой скоростью. Часть 4. Общие требования. Номинальные технические характеристики систем силовых приводов переменного тока свыше 1000 В и не более 35 кВ (IEC 61800-4:2002, Adjustable speed electrical power drive systems — Part 4: General requirements — Rating specifications for a.c. power drive systems above 1000 V a.c. and not exceeding 35 kV)

МЭК 61800-5-1:2007, Системы силовых электрических приводов с регулируемой скоростью. Часть 5-1. Требования к электрической, термической и энергетической безопасности (IEC 61800-5-1:2007, Adjustable speed electrical power drive systems — Part 5-1: Safety requirements — Electrical, thermal and energy)

МЭК 62280 (все части), Системы связи, сигнализации и обработки данных на железных дорогах (IEC 62280 (all parts), Railway applications — Communication, signalling and processing systems

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

Примечания

1 Алфавитный список определений представлен в таблице 1.

2 В настоящем стандарте употребление терминов, определение которых дано ниже, выделено курсивом.

[1)] Отменен. Действует МЭК 61508-2:2010.

[2)] Отменен. Действует МЭК 61508-3:2010.

[3)] Отменен. Действует МЭК 61508-5:2010.

[4)] Отменен. Действует МЭК 61508-6:2010.

[5)] Отменен. Действует МЭК 61508-7:2010.

Таблица 1 — Алфавитный список определений

Термин	Номер определения	Термин	Номер определения
безопасный отказ	3.14	полнота безопасности	3.17
верификация	3.26	полнота безопасности, связанная с систематическими отказами	3.24
возможный УПБ	3.21	режим работы	3.10
диагностическая(ие) проверка(и)	3.4	система, связанная с безопасностью	3.19
доля безопасных отказов	3.15	систематический отказ	3.23
заданная продолжительность работы	3.9	система силовых электроприводов с регулируемой скоростью, используемая в связанных с безопасностью применениях [СЭРС (СБ)]	3.11
контрольная проверка	3.13	спецификация требований безопасности	3.20
опасность	3.7	уровень полноты безопасности	3.18
опасный отказ	3.2	установка	3.8
отказ по общей причине	3.1	функциональная безопасность	3.6
охват диагностикой	3.3	функция(и) безопасности СЭРС (СБ)	3.16
подсистема	3.22	функция реакции на отказ	3.5
подтверждение соответствия	3.25	*PFH*	3.12

3.1

отказ по общей причине (common cause failure): Отказ, являющийся результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной системе, ведущих к отказу системы.

[МЭК 61508-4:2010, статья 3.6.10]

3.2

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

[МЭК 61508-4:1998, статья 3.6.7]

3.3

охват диагностикой, ОД (diagnostic coverage, DC): Относительное уменьшение вероятности опасных отказов аппаратных средств, связанное с выполнением автоматических *диагностических проверок*.

[МЭК 61508-4:1998, статья 3.8.6]

Примечания

1 Охват диагностикой может быть также определен с помощью отношения суммы интенсивностей выявленных опасных отказов λ_{DD} к сумме общей интенсивности опасных отказов λ_D:

$$DC = \sum \lambda_{DD} / \sum \lambda_D.$$

2 *Охват диагностикой* может относиться ко всей *системе, связанной с безопасностью*, или к ее части. Например, *охват диагностикой* может относиться к датчикам и/или к логической системе, и/или к исполнительным элементам.

3.4 **диагностическая(ие) проверка(и)** (diagnostic test(s)): Испытание(я), которое(ые) предназначено(ы) для обнаружения сбоев или отказов и формирования конкретной выходной информации или действий в случае обнаружения сбоя или отказа.

3.5 **функция реакции на отказ** (fault reaction function): Функция, которая выполняется при обнаружении сбоя или отказа в СЭРС (СБ), который может вызвать потерю функции безопасности, и предназначена поддержать условие безопасности в установке или предотвратить опасные условия, возникающие в установке.

3.6

функциональная безопасность (functional safety): Часть общей безопасности, которая относится к управляемому оборудованию (УО) и системам управления УО и зависит от корректного функционирования Э/Э/ПЭ систем, связанных с безопасностью, систем обеспечения безопасности, основанных на других технологиях, и внешних средств уменьшения риска.

[IEC 61508-4:1998, 3.1.9]

Примечание — Настоящий стандарт рассматривает только те аспекты в определении функциональной безопасности, которые зависят от корректного функционирования СЭРС (СБ).

3.7

опасность (hazard): Потенциальный источник причинения вреда.

[ИСО/МЭК Руководство 51: 1999, статья 3.5].

Примечания

1 Термин включает в себя возможную опасность для людей в короткий промежуток времени (например, при пожаре и взрыве), а также опасность, имеющую долгосрочное воздействие на здоровье людей (например, при утечке токсического вещества).

2 МЭК 6150-4:1988 (модифицированный) определяет опасную ситуацию как обстоятельства, при которых люди, имущество или окружающая среда подвергаются одной или нескольким опасным событиям.

3.8 **установка** (installation): Оборудование или технические средства, включающие, по крайней мере, СЭРС (СБ) и управляемое оборудование.

Примечание — Слово «установка» также используется в настоящем стандарте, чтобы обозначить процесс ввода в эксплуатацию СЭРС (СБ). В этих случаях оно не выделяется курсивом.

3.9 **заданная продолжительность работы** (mission time): Заданное общее время работы СЭРС (СБ) за время его срока службы.

3.10

режим работы (mode of operation): Способ предполагаемого использования системы, связанной с безопасностью, в зависимости от частоты обращений к ней.

[МЭК 61508-4:1998, статья 3.5.12, модифицированное]

Примечания

1 В МЭК 61508 рассматриваются два режима работы:

- режим с низкой частотой запросов, когда частота запросов на выполнение операции системы, связанной с безопасностью, не превышает одного в год или не превышает более чем в два раза частоту контрольных испытаний;
- режим с высокой частотой запросов или режимом непрерывной работы, когда частота запросов на выполнение операции системы, связанной с безопасностью, превышает один в год или превышает более чем в два раза частоту контрольных испытаний.

Режим с низкой частотой запросов обычно не рассматривается для применений СЭРС (СБ). Поэтому в настоящем стандарте рассматривается работа СЭРС (СБ) только в режиме с высокой частотой запросов или непрерывном режиме.

2 Режим запроса означает, что функция безопасности выполняется только по запросу (требованию), чтобы перевести установку в заданное состояние.

3 Непрерывный режим означает, что функция безопасности выполняется непрерывно, т. е. СЭРС (СБ) постоянно управляет установкой, и (опасный) отказ ее функции может привести к опасности.

3.11 **СЭРС (СБ)** (PDS(SR)): Система силовых электроприводов с регулируемой скоростью, используемая в связанных с безопасностью применениях.

3.12 ***PFH***: Вероятность опасных случайных отказов аппаратных средств в час.

Примечание — В МЭК 62061:2005 используется сокращение PFH_D.

3.13

контрольная проверка (proof test): Периодическая проверка, проводимая для того, чтобы обнаружить сбои в системе, связанной с безопасностью, с тем чтобы при необходимости система могла быть восстановлена настолько близко к «исходному» состоянию, насколько это возможно в данных условиях.

Примечание — Контрольные проверки обычно предпринимаются, чтобы обнаружить опасные отказы, которые не обнаружены *диагностическими проверками*. Эффективность контрольных проверок зависит от того, насколько близко к «исходному» состоянию восстанавливается система. Для того чтобы контрольная проверка была полностью эффективна, она должна быть в состоянии обнаруживать 100 % опасных отказов. Хотя на практике достигнуть 100 % не просто, если только это не Э/Э/ПЭ система, связанная с безопасностью, имеющая низкую сложность, однако такая цель должна стоять.

[МЭК 61508-4:1998, статья 3.8.5, модифицированное]

3.14 **безопасный отказ** (safe failure): Отказ, который не переводит систему, связанную с безопасностью, в опасное состояние или в состояние отказа при выполнении функции.

3.15 **доля безопасных отказов**, ДБО (safe failure fraction, SFF): Отношение суммы средних частот безопасных отказов и обнаруженных *опасных отказов* подсистемы к сумме средних частот безопасных и опасных отказов этой подсистемы.

$$ДБО = (\sum\lambda_S + \sum\lambda_{DD})/(\sum\lambda_S + \sum\lambda_D).$$

Примечание — См. приложение С МЭК 61508-2:2000.

3.16 **функция(и) безопасности СЭРС (СБ)** (safety function(s) (of a PDS(SR)): Функция(и) с определенными показателями безопасности, реализованная полностью или частично с помощью СЭРС (СБ), которая(ые) предназначена(ы) поддержать условие безопасности установки или предотвратить опасные условия, возникающие в установке.

3.17

полнота безопасности (safety integrity): Вероятность того, что СЭРС (СБ) удовлетворительно выполняет требуемую функцию безопасности при всех оговоренных условиях.

Примечания

1 Чем выше уровень полноты безопасности СЭРС (СБ), тем ниже вероятность того, что СЭРС (СБ) не смогут выполнить требуемые функции безопасности.

2 Полнота безопасности не может быть одинаковой для каждой функции безопасности, выполняемой СЭРС (СБ).

[IEC 61508-4:1998, статья 3.5.2, модифицированное]

3.18

уровень полноты безопасности, УПБ (safety integrity level, SIL): Дискретный уровень (принимающий одно из четырех возможных значений), определяющий требования к полноте безопасности функции безопасности, распределенной (полностью или частично) для СЭРС (СБ).

Примечания

1 Уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности.

2 Уровень полноты безопасности, равный 4, в настоящем стандарте не рассматривается, поскольку он не включается в требования снижения риска, связанные обычно с СЭРС (СБ).

[IEC 61508-4:1998, статья 3.5.6, модифицированное]

3.19 **система, связанная с безопасностью** (safety-related system): Система, которая:

- реализует необходимые функции безопасности, требующиеся для достижения или поддержки безопасного состояния управляемого оборудования, и
- предназначена для достижения своими средствами или в сочетании с другими Э/Э/ПЭ системами, связанными с безопасностью, системами, связанными с безопасностью, основанными на других технологиях или внешними средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности.

3.20 **спецификация требований безопасности** (safety requirements specification, SRS): Спецификация, содержащая все требования функций безопасности, которые должны быть выполнены СЭРС (СБ).

3.21 **возможный УПБ** (SIL capability): Максимальное значение УПБ, о котором заявляется, что оно может быть достигнуто проектом СЭРС (СБ), в терминах систематической полноты безопасности и архитектурных ограничений на полноту безопасности аппаратных средств.

Примечание — Каждая из предусмотренных функций безопасности, которые СЭРС (СБ) должна выполнить, может иметь различные возможные значения УПБ.

3.22 **подсистема** (subsystem): Часть проекта архитектуры верхнего уровня системы, связанной с безопасностью, отказ которой приводит к отказу функции безопасности.

Примечание — СЭРС (СБ) сама может быть подсистемой или состоять из ряда отдельных подсистем, которые при объединении реализуют рассматриваемую функцию безопасности. У подсистемы может быть больше чем один канал.

2 Примерами подсистем СЭРС (СБ) являются: устройство кодирования, секция питания, секция управления (см. рисунок 1).

3.23

систематический отказ (systematic failure): Отказ, связанный детерминированным образом с какой-либо причиной, которая может быть исключена только путем модификации проекта либо производственного процесса, операций, документации, либо других факторов.

[МЭК 60050-191:1990, 191-04-19]

Примечание — Примерами причин систематических отказов являются ошибки человека:

- в спецификации требований безопасности;
- в проекте, при изготовлении, вводе в эксплуатацию или в процессе работы аппаратных средств;
- при проектировании, реализации и т.п. программного обеспечения.

[МЭК 61508-4:1998, статья 3.6.6]

3.24

полнота безопасности, связанная с систематическими отказами (systematic safety integrity): Составляющая полноты безопасности системы, связанной с безопасностью, по отношению к систематическим отказам, проявляющимся в опасном режиме.

[МЭК 61508-4:1998, статья 3.5.4]

Примечание — Обычно полнота безопасности, связанная с систематическими отказами, не может быть охарактеризована количественно.

3.25

подтверждение соответствия (validation): Подтверждение, путем испытаний и представления объективных свидетельств, выполнения конкретных требований к предусмотренному конкретному использованию.

[МЭК 61508-4:1998, статья 3.8.2]

Примечание — Подтверждение соответствия представляет собой выполнение действий, демонстрирующих, что СЭРС (СБ) до или после ввода в эксплуатацию удовлетворяет во всех отношениях спецификации требований безопасности.

3.26

верификация (verification): Подтверждение выполнения требований путем испытаний и сбора объективных свидетельств.

[МЭК 61508-4:1998, статья 3.8.1]

4 Предусмотренные функции безопасности

4.1 Общие положения

Настоящий раздел описывает функции СЭРС (СБ), которые могут определяться как связанные с безопасностью, поставщиком СЭРС (СБ). Предусмотренные функции безопасности, рассматриваемые в настоящем разделе, не представляют исчерпывающий список. В некоторых случаях связанные с безопасностью системы, но внешние к СЭРС (СБ) (например, механический тормоз), в дальнейшем могут быть необходимы, чтобы поддержать безопасное состояние при отключении питания.

Технические меры, необходимые для реализации этих функций, зависят от возможного УПБ и требуемой вероятности опасных отказов аппаратных средств, которая указана в спецификации требований безопасности. Технические меры описаны в разделе 6.

Каждая функция безопасности может потребовать сигнализацию о безопасном входе и/или выходе для выполнения необходимого взаимодействия (или активизации) с другими функциями, подсистемами или системами (которые могут быть или не могут быть связаны с безопасностью). При определении УПБ соответствующей функции безопасности должна быть учтена полнота безопасности интерфейсов.

Некоторые функции безопасности выполняют только задачи контроля, некоторые выполняют важное для безопасности управление или другие действия. Поэтому необходимо различать между:

- реакцией функции на нарушение предельных значений (только для функций, относящихся к контролю): реакция возникает, когда нарушение предельных значений обнаружено во время корректной работы функции безопасности; и
- реакцией на сбой функции: реакция возникает, когда диагностика обнаруживают сбой внутри функции безопасности.

Обе реакции функций безопасности должны рассматривать возможные безопасные состояния для конкретного применения.

При выборе подходящей реакции функции безопасности необходимо учитывать, что части СЭРС (СБ) могут не функционировать.

Временные ограничения для действий, необходимых после обнаружения сбоя, определены в спецификации требований безопасности (см. 5.4.2).

В названиях функций безопасности используют слова «безопасные» или «безопасность», чтобы указать, что эти функции могут использоваться в связанном с безопасностью применении на основе обоснования (т. е. анализа рисков) того, что это конкретное применение, описываемое функциями, относящимися к безопасности, и их значениями полноты, будет выполняться в СЭРС (СБ).

4.2 Функции безопасности

4.2.1 Предельные значения

Если функция безопасности контролирует предельное(ые) значение(я) для любого параметра(ов), то должно(ы) быть определено(ы) максимальное(ые) отклонение(я) для этого(их) предельного(ых) значения(ий).

Примечание — Спецификация любого предельного значения должна учитывать возможное превышение предельного значения в случае нарушения предела. Например, спецификация предельного(ых) значения(й) положения в 4.2.3.8 должна учитывать максимальное допустимое расстояние(я) перехода(ов) за установленный предел.

Отдельная функция безопасности может иметь одно или несколько заданных предельных значений, которые могут быть выбраны во время выполнения.

4.2.2 Функции останова

4.2.2.1 Общие положения

Для каждого типа СЭРС существует несколько методов останова.

Требования к управлению запуском последовательности действий по останову и поддержанию способа захвата для достижения неподвижного состояния определяются для конкретного применения. Для достижения желаемых рабочих характеристик функций останова могут быть необходимы отдельные ручные операции и связи со схемами управления.

Любые конкретные требования для рабочих характеристик останова должны быть определены при проектировании устройства. Ниже рассмотрены примеры функций останова, часто использующиеся на практике.

4.2.2.2 Безопасное отключение крутящего момента (STO)

На двигатель не подается питание, которое может вызвать вращение (или движение в случае линейного двигателя). СЭРС (СБ) не обеспечивает питание двигателя, который может произвести крутящий момент (или усилие в случае линейного двигателя).

Примечания

1 Эта функция безопасности выполняет неуправляемую остановку и соответствует категории остановки 0 по МЭК 60204-1.

2 Эта функция безопасности может использоваться, если требуется отключение питания для предотвращения неожиданного запуска.

3 Если существуют внешние влияния (например, падение висящих грузов), то для предотвращения какой-либо опасности могут быть необходимы дополнительные меры (например, механические тормоза).

4 Электронных средств и контакторов недостаточно для защиты от удара током и для изоляции могут быть необходимы дополнительные меры.

4.2.2.3 Безопасное отключение 1 (SS1)

СЭРС (СБ) также:

a) запускает и управляет интенсивность торможения двигателя в рамках установленных пределов, чтобы остановить двигатель, и запускает функцию STO (см. 4.2.2.2), когда частота вращения двигателя окажется ниже заданного предела; или

b) запускает и контролирует интенсивность торможения двигателя в рамках установленных пределов, чтобы остановить двигатель, и запускает функцию STO, когда частота вращения двигателя окажется ниже заданного предела; или

c) запускает торможение двигателя и запускает функцию STO после определенной временной задержки.

Примечание — Эта функция безопасности выполняет управляемую остановку и соответствует категории остановки 1 по МЭК 60204-1.

4.2.2.4 Безопасное отключение 2 (SS2)

СЭРС (СБ) также:

a) запускает и управляет интенсивностью торможения двигателя в рамках установленных пределов, чтобы остановить двигатель, и запускает функцию SOS (см. 4.2.3.1), когда частота вращения двигателя окажется ниже заданного предела; или

b) запускает и контролирует интенсивность торможения двигателя в рамках установленных пределов, чтобы остановить двигатель, и запускает функцию SOS, когда частота вращения двигателя окажется ниже заданного предела; или

c) запускает торможение двигателя и запускает функцию SOS после определенной временной задержки.

Примечание — Эта функция безопасности выполняет управляемую остановку и соответствует категории остановки 2 по МЭК 60204-1.

4.2.3 Другие функции безопасности

4.2.3.1 Безопасный рабочий останов (SOS)

Функция SOS следит за тем, чтобы положение двигателя не отклонялось от положения останова на величину больше заданной. СЭРС (СБ) обеспечивает питание двигателя, чтобы позволить ему сопротивляться внешним силам.

Примечание — Данное описание функции регулируемого отключения основано на применении средств СЭРС (СБ) без внешнего (например, механического) тормоза.

4.2.3.2 Безопасное ограничение ускорения (SLA)

Функция SLA предотвращает превышение двигателем заданного предельного значения ускорения.

4.2.3.3 Безопасный диапазон ускорения (SAR)

Функция SAR обеспечивает ускорение и/или замедление двигателя в пределах заданных значений.

4.2.3.4 Безопасное ограничение скорости (SLS)

Функция SLS предотвращает превышение двигателем заданного предельного значения скорости.

4.2.3.5 Безопасный диапазон скоростей (SSR)

Функция SSR поддерживает частоту вращения двигателя в пределах заданных значений.

4.2.3.6 Безопасное ограничение крутящего момента (SLT)

Функция SLT предотвращает превышение двигателем заданного предельного значения крутящего момента (или силы, в случае линейного двигателя).

4.2.3.7 Безопасный диапазон крутящего момента (STR)

Функция STR поддерживает крутящий момент двигателя (или силу, в случае линейного двигателя) в пределах заданных значений.

4.2.3.8 Безопасное ограничение положения (SLP)

Функция SLP предотвращает превышение валом двигателя заданного(ых) предельного(ых) значения(й) положения(й).

4.2.3.9 Безопасное ограничение приращения (SLI)

Функция SLI предотвращает превышение для вала двигателя заданного предельного значения приращения положения.

Примечание — В данной функции СЭРС (СБ) управляет приращениями движений двигателя следующим образом:

- входной сигнал (например, запуска) инициирует приращение движения с заданным максимальным путем приводного элемента;
- после завершения пути, соответствующего этому приращению, двигатель останавливается и остается в этом состоянии, как готовый для применения.

4.2.3.10 Безопасное направление (SDI)

Функция SDI предотвращает движение вала двигателя в непреднамеренном направлении.

4.2.3.11 Безопасная температура двигателя (SMT)

Функция SMT предотвращает превышение температур(ы) двигателя заданных(ого) предельных(ого) значений(я).

4.2.3.12 Безопасное управление тормозом (SBC)

Функция SBC обеспечивает выходной(ые) сигнал(ы) безопасности, чтобы управлять внешним тормозом(ами).

4.2.3.13 Кулачок безопасности (SCA)

Функция SCA обеспечивает выходной(ые) сигнал(ы) безопасности, чтобы указать, находится ли положение вала двигателя в пределах заданного диапазона.

4.2.3.14 Контроль безопасного уровня скорости (SSM)

Функция SSM обеспечивает выходной сигнал безопасности, чтобы указать, является ли частота вращения двигателя ниже указанного уровня.

5 Управление функциональной безопасностью

5.1 Цель

Цель настоящего раздела состоит в определении управленческих действий и информации, необходимых для всего процесса разработки СЭРС (СБ), чтобы гарантировать достижение целей функциональной безопасности.

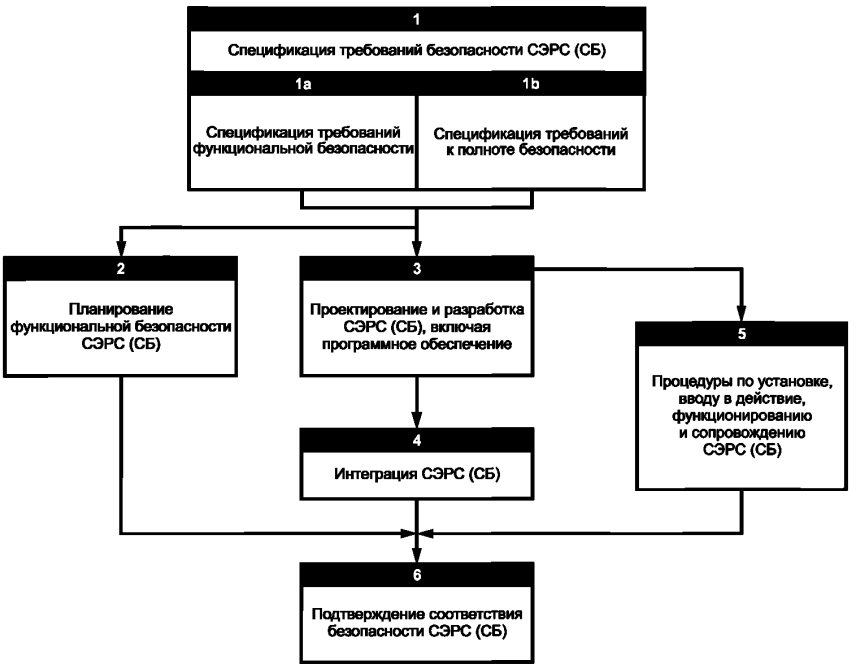
Примечание — Настоящий раздел исключительно нацелен на достижение функциональной безопасности СЭРС (СБ), а также не связан и отличается от лечебно-профилактических мер и мер по обеспечению безопасности, необходимых для достижения безопасности на рабочем месте.

5.2 Жизненный цикл разработки СЭРС (СБ)

На рисунке 2 представлен жизненный цикл разработки СЭРС (СБ) с перекрестными ссылками к соответствующим подразделам настоящего стандарта.

Примечание — Это соответствует стадии реализации (стадия 9) полного жизненного цикла системы безопасности, описанного в МЭК 61508-1.

Приложение А представляет эту информацию в форме таблицы последовательности задач.



Стадию 1 см. в 5.4	Стадию 1a см. в 5.4.2	Стадию 1b см. в 5.4.3	Стадию 2 см. в 5.3
Стадию 3 см. в разделе 6	Стадию 4 см. в 6.5	Стадию 5 см. в разделе 7	Стадию 6 см. в 8.3

Рисунок 2 — Жизненный цикл разработки СЭРС (СБ)

5.3 Планирование функциональной безопасности

План обеспечения функциональной безопасности должен быть сформирован и обновляться по мере необходимости в процессе всей разработки СЭРС (СБ). Этот план должен определить действия, удовлетворяющие требования разделов 5–10, а также определить лиц, подразделение(я) или организацию(и), ответственных за выполнение этих действий. План обеспечения функциональной безопасности может быть разделом с названием «План обеспечения функциональный безопасности» в общем плане обеспечения качества для СЭРС (СБ) или это может быть отдельный документ, названный «План обеспечения функциональный безопасности».

В частности, план обеспечения функциональной безопасности должен рассмотреть или включать следующее в соответствии со сложностью СЭРС (СБ):

a) Формирование спецификации требований безопасности (см. 5.4), включая:

- рассмотрение требований из рекомендаций и стандартов для конкретных целевых применений СЭРС (СБ);
- выбор методов для предотвращения ошибок во время формирования спецификации требований безопасности;
- персональную ответственность за формирование и соблюдение спецификации требований безопасности;
- персональную ответственность за верификацию спецификации требований безопасности;
- процесс изменения спецификации требований безопасности после начала разработки.

b) Проектирование и разработку функции(й) безопасности для СЭРС (СБ), включая (если применимо):

- рассмотрение применимых руководств и стандартов по функциональной безопасности при проектировании оборудования целевого применения, такого как средства управления процессом или машинное оборудование, которое включает СЭРС (СБ);

- выбор методологий разработки изделия и управления проектами (см. МЭК 61508-7:2000, пункт В.1.1);
- персональную ответственность за проектирование и разработку;
- методологию документирования проекта (см. МЭК 61508-7:2000, пункт В.1.2);
- применение методов структурного проектирования (см. МЭК 61508-7:2000, пункт В.3.2);
- использование моделирования или других средств компьютерного проектирования;
- методологию верификации проекта;
- методы интеграции и функционального испытания, регрессионное тестирование и ответственность персонала;
- управление изменениями проекта (для аппаратных средств и для программного обеспечения).

c) План верификации функции(й) безопасности, включая:
- выбор стратегий и методов верификации;
- выбор действий по верификации;
- персональную ответственность за верификацию;
- выбор и использование испытательного оборудования;
- оценку результатов верификации, полученных от испытательного оборудования и от тестов.

d) План подтверждения соответствия функции(й) безопасности, включающий:
- персональную ответственность за проверку подтверждения соответствия;
- идентификацию соответствующих режимов работы СЭРС (СБ);
- техническую стратегию подтверждения соответствия, например аналитические методы или статистические тесты;
- критерии принятия;
- действие, выполняемое в случае несоответствия критерию принятия.

e) Планирование установки и ввода в действие, включающее (если применимо):
- специальные инструкции по установке и по последовательности установки;
- персональную ответственность за установку и ввод в действие;
- действия по вводу в действие и тесты, связанные с функциональной безопасностью;
- методология создания отчетов для приемо-сдаточных испытаний и их результатов;
- механизм для разрешения отказов тестов и проблем при тестировании.

f) Планирование связанной с безопасностью пользовательской документации, включая:
- список существенной связанной с безопасностью информации, которая должна быть представлена в документах;
- персональную ответственность за пользовательскую документацию;
- процесс экспертизы, чтобы обеспечить точность документации.

g) Если требуется оценка (см. МЭК 61508-1:1998, раздел 8), то должен быть доступен план оценки функциональный безопасности, включающий:
- область применения оценки функциональной безопасности;
- персональную ответственность за оценку функциональной безопасности;
- стадии, на которых должны быть выполнены действия по оценке функциональной безопасности (например, после разработки спецификации требований безопасности, после разработки связанной с безопасностью системы управления);
- информацию, которая должна быть сформирована в результате действия по оценке функциональной безопасности;
- ресурсы, требуемые для выполнения действий по оценке функциональной безопасности;
- уровень независимости команды по оценке;
- средства, которыми оценка функциональной безопасности должна быть повторно подтверждена после модификаций СЭРС (СБ).

5.4 Спецификация требований безопасности СЭРС (СБ)

5.4.1 Общие положения

Спецификация требований безопасности СЭРС (СБ) должна быть документально оформлена и должна включать:
- спецификацию требований функциональности безопасности (см. 5.4.2) и
- спецификацию требований к полноте безопасности (см. 5.4.3).

Они должны быть записаны так, чтобы они были:
- ясными;
- точными;

- определенными;
- выполнимыми;
- поддающимися проверке;
- тестируемыми;
- удобными в сопровождении.

Для предотвращения ошибок во время компиляции таких спецификаций должны быть применены надлежащие методы и меры (см. МЭК 61508-2:2000, таблица В.1).

5.4.2 Спецификация требований к функциональности безопасности

Спецификация требований к функциональности безопасности должна обеспечить всесторонние подробные требования, достаточные для проектирования и разработки СЭРС (СБ).

Спецификация требований к функциональности безопасности должна описать должным образом:

a) все функции безопасности, которые должны быть выполнены;

b) все возможные состояния СЭРС (СБ), которые могут использоваться для достижения безопасного состояния для предназначенного применения;

c) рабочие режимы СЭРС (СБ) — например, установка, запуск, обслуживание, нормальная планируемая работа;

d) все требуемые режимы поведения СЭРС (СБ);

e) приоритет среди тех функций, которые одновременно активны и могут конфликтовать друг с другом;

f) требуемое действие(я), когда будет обнаружено нарушение предельных значений во время корректной работы функции безопасности (т. е. реакция на нарушение предельных значений (см. 4.1));

g) функция(и) реакции на сбой (см. 4.1 и 6.3);

h) максимальное время реакции на сбой, обеспечивающее соответствующую реакцию на сбой, которая будет выполняться перед появлением опасности в предназначенном применении (требуется только там, где используются диагностические тесты для достижения возможного УПБ);

i) максимальное время отклика каждой связанной с безопасностью функции [т. е. и функции безопасности, и функции реакции на сбой (см. 6.3)];

j) значение всех взаимодействий между аппаратными средствами и программным обеспечением (где необходимо), любые требуемые ограничения между аппаратными средствами и программным обеспечением должны быть идентифицированы и документально оформлены.

Примечание — Если эти взаимодействия не известны перед завершением проекта, то могут быть установлены только общие ограничения;

k) все средства, с помощью которых оператор взаимодействует с СЭРС (СБ), и которые могут влиять на функции, связанные с безопасностью (т. е. функции безопасности и функции реакции на сбой);

l) все интерфейсы между СЭРС (СБ) и любыми другими системами (либо непосредственно связанные с ней внутри или снаружи установки).

5.4.3 Спецификация требований полноты безопасности

Спецификация требований полноты безопасности для СЭРС (СБ) должна содержать:

a) для каждой связанной с безопасностью функции (или группы одновременно используемых функций безопасности) как возможный УПБ, так и максимальную вероятность опасного случайного отказа аппаратных средств.

Примечания

1 Возможный УПБ важен, если СЭРС (СБ) рассматривается как компонент, который реализует функцию безопасности в сочетании с другими компонентами.

2 Чтобы учитывать вероятность *опасных отказов* других включенных компонентов, необходимо, чтобы вероятность опасных случайных отказов аппаратных средств СЭРС (СБ) была, как правило, ниже, чем целевая мера отказов, связанная с УПБ, определенным для всей функции безопасности. Однако она также может быть и выше, если СЭРС (СБ) должен использоваться для реализации функции безопасности в избыточной конфигурации (в схеме с резервированием) с другими компонентами.

3 Если СЭРС (СБ) реализует функцию безопасности полностью сама, то в спецификации требований полноты безопасности будет определен УПБ, а не возможный УПБ.

4 Если общие аппаратные средства используются для реализации более одной функции безопасности и функции безопасности используются одновременно, то вероятность опасного случайного отказа оборудования общих аппаратных средств необходимо рассмотреть только один раз при определении полной вероятности опасных случайных отказов аппаратных средств.

5 Для многоосевой СЭРС (СБ), где функция безопасности требуется для более чем одной оси, вероятность опасного случайного отказа оборудования общих аппаратных средств необходимо рассмотреть только один раз при определении полной вероятности опасного случайного отказа аппаратных средств;

b) экстремальные значения всех условий окружающей среды (включая электромагнитные), с которыми, вероятно, встретится СЭРС (СБ) во время хранения, транспортировки, тестирования, установки, ввода в действие, эксплуатации и обслуживания.

Примечание — Данная информация может быть получена, чтобы удовлетворить требования МЭК 61800-1, МЭК 61800-2 или МЭК 61800-4, и в таком случае не должна вновь документально оформляться;

c) любое требование для увеличения ЭМ совместимости (см. 6.2.5).

6 Требования к проектированию и разработке СЭРС (СБ)

6.1 Общие требования

6.1.1 Изменение в процессе эксплуатации

Любое изменение в процессе эксплуатации для СЭРС (СБ), которое может привести к опасной ситуации (например, неожиданный запуск), должно быть инициировано только оператором, как осознанное действие.

Примечание — Например, любой отказ СЭРС (СБ), находящейся в состоянии блокировки, не должен приводить к неожиданному запуску элементов машинного оборудования и/или предприятия.

6.1.2 Стандарты проектирования

СЭРС (СБ) должны быть разработаны в соответствии с МЭК 61800-5-1 и, по мере необходимости, с другими применимыми стандартами комплекса МЭК 61800.

6.1.3 Реализация

СЭРС (СБ) должна быть реализована в соответствии с ее спецификацией требований безопасности (см. 5.4).

6.1.4 Полнота безопасности и обнаружение сбоев

СЭРС (СБ) должна выполнять все требования a)– c) следующим образом:

a) требования полноты безопасности аппаратных средств, включающие:

- архитектурные ограничения на полноту безопасности аппаратных средств (см. 6.2.2) и
- требования к вероятности опасных случайных отказов аппаратных средств в час (см. 6.2.1);

b) требования систематической полноты безопасности, включающие:

- требования к предотвращению отказов (см. 6.2.4.1) и требования к управлению систематическими отказами (см. 6.2.4.2) или
- доказательства того, что используемые компоненты «доказаны использованием». В этом случае такие компоненты должны выполнить соответствующие требования МЭК 61508-2;

c) требования к поведению при обнаружении сбоя (см. 6.3).

6.1.5 Функция безопасности и функция, не связанная с безопасностью

Если СЭРС (СБ) должна выполнять и функцию безопасности, и функцию, не связанную с безопасностью, то все ее аппаратные средства и программное обеспечение необходимо рассматривать как связанные с безопасностью, если нельзя показать, что реализация функции безопасности и функции, не связанной с безопасностью, достаточно независима (т. е. отказ любой не связанной с безопасностью функции не вызывает *опасный отказ* связанных с безопасностью функций).

Примечание — Достаточная независимость устанавливается демонстрацией того, что вероятность зависимого отказа между не связанной с безопасностью деталью и деталью, связанной с безопасностью, достаточно низкая по сравнению с вероятностью *опасного отказа* для самого высокого уровня полноты безопасности, связанного с реализуемыми функциями безопасности.

6.1.6 Применяемый УПБ

Требования к аппаратным средствам и программному обеспечению должны определяться уровнем полноты безопасности функции безопасности, имеющей самый высокий уровень полноты безопасности, если нельзя будет показать, что реализация функций безопасности с различными уровнями полноты безопасности достаточно независима.

Примечание — Достаточная независимость устанавливается демонстрацией того, что вероятность зависимого отказа между деталями, реализующими функции безопасности с различными уровнями полноты, достаточно низкая по сравнению с вероятностью *опасного отказа* для самого высокого уровня полноты безопасности, связанного с реализуемыми функциями безопасности.

6.1.7 Требования к программному обеспечению

Если программное обеспечение используется для реализации функции безопасности СЭРС (СБ) с конкретным УПБ или возможным УПБ (см. 5.4.3), то это программное обеспечение должно быть реализовано в соответствии с требованиями, определенными в МЭК 61508-3 для этого конкретного УПБ.

6.1.8 Обзор требований

Требования для связанных с безопасностью аппаратных средств и программного обеспечения должны быть проанализированы, чтобы гарантировать, что они определены адекватно. В частности, необходимо рассмотреть следующее:

a) функции безопасности;

b) требования полноты безопасности;

c) оборудование и интерфейсы оператора.

6.1.9 Проектная документация

Помимо документации проекта и реализации, проектная документация СЭРС (СБ) должна указать на методы и меры, использование которых обеспечит достижение требуемого УПБ (например, анализ вида и последствий отказов, анализ дерева сбоев).

6.2 Требования к проектированию СЭРС (СБ)

6.2.1 Требования к вероятности случайных опасных отказов аппаратных средств в час (*PFH*)

6.2.1.1 Общие требования

6.2.1.1.1 *PFH* для каждой функции безопасности

Значение *PFH* каждой функции безопасности (или группы одновременно используемых функций безопасности), выполняемой СЭРС (СБ), оценивается согласно 6.2.1.1.2 и приложению В и должно быть равно или меньше целевой меры отказов (см. таблицу 2), как определено в спецификации требований полноты безопасности (см. 5.4.3).

Величина *PFH*, определенная УПБ, относится ко всей функции безопасности. Если СЭРС (СБ) предназначена для выполнения только части функции безопасности в связанной с безопасностью системе управления, то *PFH* двигателя должна быть несколько ниже, чем величина, определенная УПБ.

Примечание — Целевая мера отказов, выраженная в терминах *PFH*, определяется значением УПБ функции безопасности (см. МЭК 61508-1:1998, таблица 3), если не существует требования в спецификации требований полноты безопасности СЭРС (СБ) (см. 5.4.3) о том, что функция безопасности должна удовлетворять конкретному значению целевой меры отказов, а не определяться значением УПБ.

Таблица 2 — Уровни полноты безопасности: целевые меры отказов для функции безопасности СЭРС (СБ)

Уровень полноты безопасности	*PFH*
3	$> 10^{-8}$ — $< 10^{-7}$
2	$> 10^{-7}$ — $< 10^{-6}$
1	$> 10^{-6}$ — $< 10^{-5}$
Примечание — *PFH* иногда упоминается как частота *опасных отказов* или интенсивность *опасных отказов* в единицах *опасных отказов* в час.	

Значение *PFH* каждой функции безопасности (или группы одновременно выполняющихся функций безопасности) СЭРС (СБ) должно оцениваться отдельно.

Примечания

1 Различные функции безопасности могут использовать общие компоненты и/или различные компоненты, приводящие к различным значениям *PFH* для каждой функции безопасности (или группы одновременно выполняющихся функций безопасности).

2 Существует ряд доступных методов моделирования, и выбор наиболее подходящего, который должен выполнить аналитик, будет зависеть от ряда обстоятельств. Доступные методы включают:

- анализ дерева сбоев (см. МЭК 61025);
- модели Маркова (см. МЭК 61165);

- блок-схемы надежности (см. МЭК 61078).

См. также МЭК 60300-3-1.

3 Среднее время восстановления (см. IEV 191-13-08), которое рассматривают в модели надежности, должно учитывать диагностический интервал, интервал контрольной проверки, время ремонта и любые другие задержки до восстановления, а также заданную продолжительность работы.

4 Отказы по общей причине и в процессах передачи данных могут появиться вследствие причин, отличных от фактических неисправностей компонентов аппаратных средств (например, ошибки декодирования). Однако в целях настоящего стандарта такие отказы рассматривают как случайные отказы аппаратных средств. (См. приложение D МЭК 61508-6:2000.)

5 В приложении В МЭК 61508-6:2000 описан упрощенный подход, который может использоваться для оценки вероятности *опасных отказов* функции безопасности из-за случайных отказов аппаратных средств, чтобы определить, что архитектура удовлетворяет требуемой целевой мере отказов.

6.2.1.1.2 Оценка *PFH*

Значение *PFH* каждой функции безопасности (или группы одновременно используемых функций безопасности), выполняемой СЭРС (СБ), из-за случайных отказов аппаратных средств должно быть оценено, используя приложение А МЭК 61508-2:2000, учитывая:

a) архитектуру СЭРС (СБ), поскольку это касается каждой рассматриваемой функции безопасности;

b) оцениваемую интенсивность отказов каждой подсистемы СЭРС (СБ) в любых режимах, которые вызвали бы *опасный отказ* СЭРС (СБ), но которые обнаруживаются *диагностическими тестами*;

c) оцениваемую интенсивность отказов каждой подсистемы СЭРС (СБ) в любых режимах, которые вызвали бы *опасный отказ* СЭРС (СБ), не обнаруженных *диагностическими проверками*;

d) чувствительность СЭРС (СБ) к *отказам по общей причине* (см. приложение D МЭК 61508-6:2000);

e) *охват диагностикой* (ОД) *диагностическими проверками* (определенный согласно приложениям А и С МЭК 61508-2:2000) и связанный с ним интервал *диагностических проверок*.

Примечание — При установлении *диагностических проверок* интервала необходимо рассмотреть интервалы между всеми тестами, которые вносят вклад в *охват диагностикой*;

f) интервалы, с которыми выполняются контрольные проверки для обнаружения опасных отказов, которые не были обнаружены *диагностическими проверками*.

Примечание — На практике контрольные проверки бывает трудно осуществить для определенных деталей СЭРС (СБ). В таких случаях можно предположить, что интервал контрольных проверок является временем заданной продолжительности работы этой детали или самой СЭРС (СБ). Необходимо отметить, что время заданной продолжительности работы, равное 20 годам, может требоваться многими применениями машинного оборудования;

g) времена ремонта для обнаруженных отказов.

Примечание — Время ремонта составляет часть среднего времени восстановления (см. IEV 191-13-08), которое также включает время обнаружения отказа и некоторый период времени, во время которого ремонт невозможен (в приложении В МЭК 61508-6:2000 дан пример того, как среднее время к восстановлению может использоваться при вычислении вероятности отказов). Для ситуаций, где ремонт может быть выполнен только в течение определенного промежутка времени, например в то время, когда управляемое оборудование остановлено и находится в безопасном состоянии, особенно важно, чтобы все внимание было уделено периоду времени, когда никакой ремонт не может быть выполнен, особенно когда оно относительно большое;

h) вероятность *опасного отказа* любого процесса передачи данных (см. 6.4).

6.2.1.1.3 Данные об интенсивности отказов

Компоненты данных об интенсивности отказов должны быть получены из:

- признанных источников или
- оценки, основанной на тех компонентах, которые рассматриваются как «доказанные практикой» (см. МЭК 61508-2:2000, пункты 7.4.7.6 — 7.4.7.12).

Для компонента при оценке его интенсивности отказов должна использоваться ожидаемая средняя рабочая температура.

У любых используемых данных об интенсивности отказов должен быть доверительный уровень, по крайней мере, 60 %.

Примечания

1 Данные могут быть получены из ряда изданных промышленных источников (см. приложение С).

2 Если доступны данные об отказах, зависящие от местных условий, то они предпочтительнее. Если они недоступны, то, вероятно, придется использовать общие данные.

3 Хотя большинство вероятностных методов оценки предполагает, что интенсивность отказов постоянна, это предположение применяется только при условии, что для компонентов не превышен срок их полезной службы. Вне срока их полезной службы (т. е. когда вероятность отказов значительно увеличивается со временем), результаты большинства вероятностных методов расчета по этой причине бесполезны. Таким образом, любая вероятностная оценка должна включать спецификацию срока полезной службы компонентов. Срок полезной службы очень зависит от самого компонента и его условий работы — от температуры в частности (например, электролитические конденсаторы могут быть очень чувствительны к температуре). Опыт показал, что срок их полезной службы часто находится в диапазоне от 8 лет до 12 лет. Однако он может быть значительно меньше, если компоненты эксплуатируются вблизи допустимых границ их рабочих характеристик.

4 Списки сбоев, данные в приложении D, могут использоваться, чтобы помочь в определении видов отказов.

6.2.1.1.4 Интервал диагностических проверок

Интервал *диагностических проверок* любой подсистемы СЭРС (СБ) должен быть таким, который позволяет СЭРС (СБ) соответствовать требованию для *PFH* (см. 6.2.1.1.1).

Если опасный сбой может привести к потере функции безопасности, то для предотвращения опасности требуется обнаружение этого сбоя в пределах ОД и инициирование реакции на сбой. Функции диагностики и функции реакции на сбой должны быть выполнены в течение заданного максимального времени реакции на сбой (см. 5.4.2).

6.2.1.1.5 Интервал проверок в случае отказоустойчивости аппаратных средств, равной нулю

Интервал *диагностических проверок* любой подсистемы СЭРС (СБ), отказоустойчивость аппаратных средств которой равна нулю и от которой полностью зависит функция безопасности, должен быть таков, чтобы сумма интервала *диагностических проверок* и времени выполнения заданного действия (функции реакции на сбой) для достижения или поддержания безопасного состояния была меньше, чем заданное максимальное время реакции на сбой.

6.2.2 Архитектурные ограничения

6.2.2.1 Ограничения УПБ

В контексте полноты безопасности аппаратных средств наибольший уровень полноты безопасности, который можно заявить для функции безопасности, ограничен отказоустойчивостью аппаратных средств и долей безопасных отказов подсистем СЭРС (СБ), которые выполняют эту функцию безопасности. Отказоустойчивость аппаратных средств *N* означает, что *N*+1 сбой может вызвать потерю функции безопасности. Таблицы 3 и 4 определяют наибольший уровень полноты безопасности, который можно заявить для функции безопасности, использующей подсистему, учитывая отказоустойчивость аппаратных средств и долю безопасных отказов этой подсистемы (см. приложение С МЭК 61508-2:2000). Требования таблицы 3 или таблицы 4, в зависимости от того, какая подходит, должны быть применены к каждой подсистеме, выполняющей функцию безопасности, и, следовательно, к каждой детали СЭРС (СБ); в 6.2.2.2.1 и 6.2.2.2.2 определяется, какая из таблиц, 3 или 4, используется для любой конкретной подсистемы. Относительно этих требований:

a) при определении отказоустойчивости аппаратных средств не должны учитываться другие меры (такие, как диагностика), которые могут управлять результатами сбоев;

b) если один сбой непосредственно приводит к возникновению одного или более последующих сбоев, то их рассматривают как одиночный сбой;

c) при определении отказоустойчивости аппаратных средств некоторые сбои могут быть исключены, при условии, что вероятность их появления достаточно низкая относительно требований полноты безопасности подсистемы. Любые такие исключения сбоев должны быть обоснованы и документально оформлены (см. примечание 3 ниже).

Примечания

1 Для достижения достаточно устойчивой архитектуры с учетом уровня сложности подсистемы были включены ограничения архитектуры. Уровень полноты безопасности аппаратных средств для СЭРС (СБ), полученный в результате применения этих требований, является максимальным, который можно заявить даже при том, что в некоторых случаях теоретически может быть получен более высокий уровень полноты безопасности, если для СЭРС (СБ) применить строго математический подход.

2 Полученная архитектура подсистемы удовлетворяет требованиям отказоустойчивости аппаратных средств при нормальных условиях эксплуатации. Требования отказоустойчивости могут быть снижены во время восстановления СЭРС (СБ) в неавтономном режиме. Однако основные параметры, касающиеся любого снижения, должны быть заранее оценены (например, среднее время восстановления по отношению к вероятности запроса).

3 Это необходимо, так как если у компонента явно очень низкая вероятность отказа в результате свойств, присущих его проекту и конструкции (например, механическая связь привода), то обычно нет необходимости рассматривать ограничения (связанные с отказоустойчивостью аппаратных средств) полноты безопасности любой функции безопасности, которая использует этот компонент.

6.2.2.2 Подсистемы типа А и типа В

6.2.2.2.1 Тип А

Подсистема может быть отнесена к типу А, если для ее компонентов, необходимых для реализации функции безопасности, одновременно выполняются следующие условия:

a) виды отказов всех составляющих компонентов хорошо определены;

b) поведение подсистемы в условиях сбоя может быть полностью определено;

c) существуют достаточные надежные данные об отказах из опыта эксплуатации, показывающие, что обнаруженные и необнаруженные *опасные отказы* удовлетворяют требуемым интенсивностям отказов.

Примечание — В приложении D представлены списки отказов и возможные способы их исключения.

6.2.2.2.2 Тип В

Подсистема может быть отнесена к типу В, если для ее компонентов, необходимых для реализации функции безопасности, не выполняется хотя бы одно из условий, перечисленных в 6.2.2.2.2.

Примечания

1 Это означает, что если, по крайней мере, один из компонентов подсистемы удовлетворяет условиям для подсистемы типа В, то вся подсистема должна быть отнесена к типу В, а не к типу А.

2 Например, устройство управления, состоящее из микроконтроллеров и т. д., рассматривают как подсистему типа В.

3 В приложении D представлены списки отказов и возможные способы их исключения.

6.2.2.3 Ограничения архитектуры

Должны применяться ограничения архитектуры из таблицы 3 или из таблицы 4. Таблица 3 применяется для каждой подсистемы типа А, являющейся частью СЭРС (СБ). Таблица 4 применяется для каждой подсистемы типа В, являющейся частью СЭРС (СБ).

Таблица 3 — Полнота безопасности аппаратных средств. Ограничения архитектуры для связанных с безопасностью подсистем типа А

Доля безопасных отказов элемента[a)]	*N* — отказоустойчивость аппаратных средств (см. 6.2.2.1)		
	N = 0	*N* = 1	*N* = 2
Менее 60 %	УПБ 1	УПБ 2	УПБ 3
От 60 % до менее 90 %	УПБ 2	УПБ 3	УПБ 3[b)]
От 90 % до менее 99 %	УПБ 3	УПБ 3[b)]	УПБ 3[b)]
Не менее 99 %	УПБ 3	УПБ 3[b)]	УПБ 3[b)]

[a)] Более подробно, как оценить долю безопасных отказов, см. в 6.2.2.1.

[b)] Настоящий стандарт применяется только к функциям безопасности со значением УПБ не больше, чем УПБ 3. Для функций безопасности с УПБ 4 должны быть применены требования МЭК 61508.

Таблица 4 — Полнота безопасности аппаратных средств. Ограничения архитектуры для связанных с безопасностью подсистем типа В

Доля безопасных отказов элемента[a)]	*N* — отказоустойчивость аппаратных средств (см. 6.2.2.1)		
	N = 0	*N* = 1	*N* = 2
Менее 60 %	Не оговаривается	УПБ 1	УПБ 2
От 60 % до менее 90 %	УПБ 1	УПБ 2	УПБ 3
От 90 % до менее 99 %	УПБ 2	УПБ 3	УПБ 3[b)]
Не менее 99 %	УПБ 3	УПБ 3[b)]	УПБ 3[b)]

[a)] Более подробно, как оценить долю безопасных отказов, см. в 6.2.2.1.

[b)] Настоящий стандарт применяется только к функциям безопасности со значением УПБ не больше, чем УПБ 3. Для функций безопасности с УПБ 4 должны быть применены требования МЭК 61508.

6.2.3 Оценка доли безопасных отказов (ДБО)

6.2.3.1 Методы анализа

Для оценки ДБО подсистемы должен быть выполнен анализ (например, анализ дерева отказов или анализ видов и последствий отказов), чтобы определить все соответствующие сбои и их соответствующие виды отказов. Вероятность каждого вида отказов подсистемы должна быть определена на основе вероятности соответствующей(их) неисправности(ей).

6.2.3.2 Основные источники данных

Оценка ДБО должна быть основана на:

- либо статистически значимых данных об интенсивности отказов, собранных из опыта реальной эксплуатации;
- либо данных об отказах компонентов из признанного источника.

См. также 6.2.1.1.3.

Примечание — В приложении С представлен информативный список известных источников.

6.2.3.3 Реле безопасности

В подсистеме с отказоустойчивостью аппаратных средств, равной нулю, когда используется реле безопасности с принудительным управлением контактом обратной связи, чтобы обеспечить функцию безопасности и *охват диагностикой* этой функции, полнота безопасности из-за архитектурных ограничений этой подсистемы ограничена предельным значением УПБ 2.

6.2.3.4 Вычисление ДБО

Доля безопасных отказов подсистемы должна быть вычислена, используя приложения А и С МЭК 61508-2:2000.

6.2.4 Требования к систематической полноте безопасности СЭРС (СБ) и подсистем СЭРС (СБ)

6.2.4.1 Требования по предотвращению систематических отказов

6.2.4.1.1 Общие положения

Должны использоваться методы и меры, минимизирующие введение неисправностей во время проектирования и разработки аппаратных средств СЭРС (СБ).

Должны быть выполнены тесты, как запланировано согласно 6.2.4.1.4. См. также раздел 9.

6.2.4.1.2 Выбор методов проектирования

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

a) прозрачности, модульности и другим характеристикам, которые минимизируют сложность и увеличивают доступность для понимания проекта;

b) ясности и точности представления:

- функциональных возможностей,
- интерфейсов между подсистемами,
- информации, устанавливающей последовательность и время,
- параллелизма и синхронизации;

c) ясности и точности документирования и передачи информации;

d) проверке и подтверждению соответствия.

6.2.4.1.3 Меры при проектировании

Должны быть применены следующие меры при проектировании.

a) Надлежащего качества проект СЭРС (СБ) и/или подсистем, включая:

- использование компонентов в пределах технических требований производителей этих компонентов, например для таких параметров, как температура, нагрузка, электропитание, номинальная мощность и синхронизация;
- снижение номинальных значений параметров проекта, чтобы в случае необходимости улучшить надежность достижения целевой интенсивности отказов;
- надлежащее объединение и сборку подсистем, например кабельную разводку, монтаж и любые соединения;
- использование осмотров и проверок для раннего обнаружения дефектов проекта.

b) Совместимость:

- использование подсистем с совместимыми эксплуатационными характеристиками.

c) Устойчивость к заданным условиям окружающей среды:

- проект СЭРС (СБ) должен быть способен к безопасной работе для всех заданных условий окружающей среды, например таких, как температура, влажность, вибрация, электромагнитные явления, уровень загрязнения, категория перегрузки по напряжению, высота.

6.2.4.1.4 Планирование испытаний

В процессе проектирования по мере необходимости должны быть запланированы следующие различные типы испытаний:

a) испытание подсистемы;

b) испытание интеграции;

c) проверка подтверждения соответствия;

d) испытание конфигурации (см. 7.1).

Документация по планированию испытаний должна включать:

e) типы выполняемых тестов и процедуры их выполнения;

f) условия, инструменты, конфигурацию и программы испытаний;

g) критерии оценки «прошел испытание»/«не прошел испытание».

Если применимо, то должны использоваться автоматические инструменты испытаний и интегрированные средства разработки.

Примечание — Полнота таких инструментов может быть продемонстрирована конкретными испытаниями, обширной историей удовлетворительного применения или независимой проверкой их результатов для конкретных СЭРС (СБ) в процессе их разработки.

6.2.4.1.5 Требования к поддержке проекта

На стадии проектирования должен быть определен процесс поддержки проекта и повторного испытания, гарантирующий, что полнота безопасности СЭРС (СБ) остается на требуемом уровне во время последующих версий проекта.

6.2.4.2 Требования по управлению систематическими сбоями

6.2.4.2.1 Характеристики проекта

Для управления систематическими сбоями проект должен обладать характеристиками, которые делают СЭРС (СБ) и ее подсистемы устойчивыми к любым:

a) остаточным сбоям в проекте аппаратных средств, если вероятность сбоев проекта аппаратных средств не может быть исключена, применяя раздел А.3 и таблицу А.16 МЭК 61508-2:2000;

b) внешним воздействиям, включая электромагнитные, применяя раздел А.3 и таблицу А.17 МЭК 61508-2:2000;

c) ошибкам оператора СЭРС (СБ) (см. раздел А.3 и таблицу А.18 МЭК 61508-2:2000);

d) остаточным ошибкам в проекте программного обеспечения (см. пункт 7.4.3 МЭК 61508-3:1998 и соответствующие таблицы);

e) ошибкам и последствиям, возникающим в результате выполнения любого процесса передачи данных (см. 6.4).

6.2.4.2.2 Контролепригодность и ремонтопригодность

Контролепригодность и ремонтопригодность необходимо рассмотреть во время выполнения действий по проектированию и разработке, чтобы обеспечить выполнение этих свойств при завершении СЭРС (СБ).

6.2.4.2.3 Ограничения человека

Проект СЭРС (СБ) должен учитывать способности и ограничения человека и быть пригодным для действий, предписанных операторам и штату обслуживания. Проект интерфейсов оператора должен соответствовать хорошей практике учета человеческого фактора и должен приспособиться к наиболее вероятному уровню подготовки или знаний операторов.

6.2.4.2.4 Защита от непредумышленной модификации

СЭРС (СБ) должна включать меры для защиты (или упрощения защиты) от непредумышленных модификаций, связанных с безопасностью программного обеспечения, аппаратных средств, параметризации и конфигурации СЭРС (СБ).

Примечание — См. В.4.8 МЭК 61508-7:2000.

6.2.4.2.5 Подтверждение ввода и ошибки оператора

Проект СЭРС (СБ) должен включать подтверждение ввода для управления отказами эксплуатации. Проект должен также защищать от ошибок оператора, связанных с функциями безопасности СЭРС (СБ), с помощью контроля достоверности данных.

Примечание — См. В.4.6 и В.4.9 МЭК 61508-7:2000.

6.2.4.2.6 Потеря электропитания

СЭРС (СБ) должна быть специфицирована и спроектирована с учетом последствий при потере электропитания.

6.2.5 Требования к электромагнитной устойчивости СЭРС (СБ)

6.2.5.1 Общие положения

Критерии рабочих характеристик, которые должны быть применены при формировании испытаний на электромагнитную устойчивость СЭРС (СБ), определены в 6.2.5.3. Эти критерии не относятся к обычным (не связанным с безопасностью) функциям оборудования (функциональная электромагнитная совместимость (ЭМС) СЭРС (СБ) достигается, если для СЭРС (СБ) выполняются требования МЭК 61800-3).

6.2.5.2 Предназначенная окружающая среда

Электромагнитное окружение, заданное или ожидаемое для предназначенного использования СЭРС (СБ), должно использоваться для определения уровней испытаний на электромагнитную устойчивость.

Если электромагнитное окружение не известно производителю СЭРС (СБ), то уровни испытаний (МЭК 61800-3) должны использоваться для тестов на электромагнитную устойчивость.

6.2.5.3 Критерий работы

Следующий критерий работы должен быть удовлетворен предназначенными функциями безопасности СЭРС (СБ). Поведение всех функций СЭРС (СБ), не связанных с безопасностью, не рассматривается, за исключением рассмотренной в 6.2.5.4.

Предназначенные для применения безопасности функции безопасности СЭРС (СБ):

- не должны выходить за значения пределов, заданных для них требованиями функциональной безопасности, или
- могут отклоняться временно или постоянно от значений пределов, заданных для них требованиями функциональной безопасности, если СЭРС (СБ) реагируют на электромагнитное возмущение так, что заданное безопасное состояние СЭРС (СБ) сохраняется или достигается в течение указанного максимального времени реакции на сбой.

Постоянное ухудшение функции безопасности или разрушение компонентов разрешены при условии, что безопасное состояние сохраняется или достигается в течение указанного максимального времени реакции на сбой.

Этот критерий относится ко всем электромагнитным явлениям, относящимся к СЭРС (СБ) в ее предназначенном применении.

6.2.5.4 Введение опасностей

Если применяется испытание на электромагнитную устойчивость, то никакие небезопасные условия или опасности не должны вводиться в СЭРС (СБ).

6.2.5.5 Верификация

Если выполняются испытания на электромагнитную устойчивость, то должны существовать заданные меры по смягчению.

В зависимости от анализа электромагнитного окружения, предназначенного применения СЭРС (СБ), при проверке роста устойчивости (как требуется в МЭК 61508-2):

- либо при необходимости (в зависимости от электромагнитного явления и требуемого УПБ) увеличивается уровень испытаний, и/или продолжительность испытания, и/или число циклов испытаний;
- либо проверяется эффективность любых дополнительных мер по смягчению (см. МЭК 61508-7:2000, подраздел 11.3), которые были определены.

6.3 Поведение при обнаружении сбоев

6.3.1 Обнаружение сбоев

Обнаружение сбоев в СЭРС (СБ) может быть выполнено *диагностическими проверками.*

Если обнаруживается опасный сбой, который может привести к потере функции безопасности, то должна быть инициирована функция реакции на сбой, чтобы предотвратить опасность. Диагностики и функции реакции на сбой должны быть выполнены в течение указанного максимального времени реакции на сбой.

6.3.2 Отказоустойчивость больше нуля

Обнаружение опасного сбоя (с помощью *диагностических проверок* или иными методами) в любой подсистеме с отказоустойчивостью аппаратных средств больше нуля должно завершаться:

a) конкретным действием функции реакции на сбой или

b) изоляцией дефектной части подсистемы для обеспечения возможности продолжения безопасной эксплуатации машинного оборудования и/или агрегатов, пока дефектная часть не будет отремонтирована. Если ремонт не завершен в пределах средней продолжительности ремонта (*MRT*), принятого при вычислении вероятности случайных отказов аппаратных средств (см. 6.2.1), то должно начаться выполнение функции реакции на сбой.

6.3.3 Отказоустойчивость равна нулю

Обнаружение опасного сбоя (с помощью *диагностических проверок* или иными методами) в любой подсистеме с отказоустойчивостью аппаратных средств, равной нулю, от которой полностью зависит функция безопасности, должно привести к выполнению функции реакции на сбой.

6.4 Дополнительные требования к передаче данных

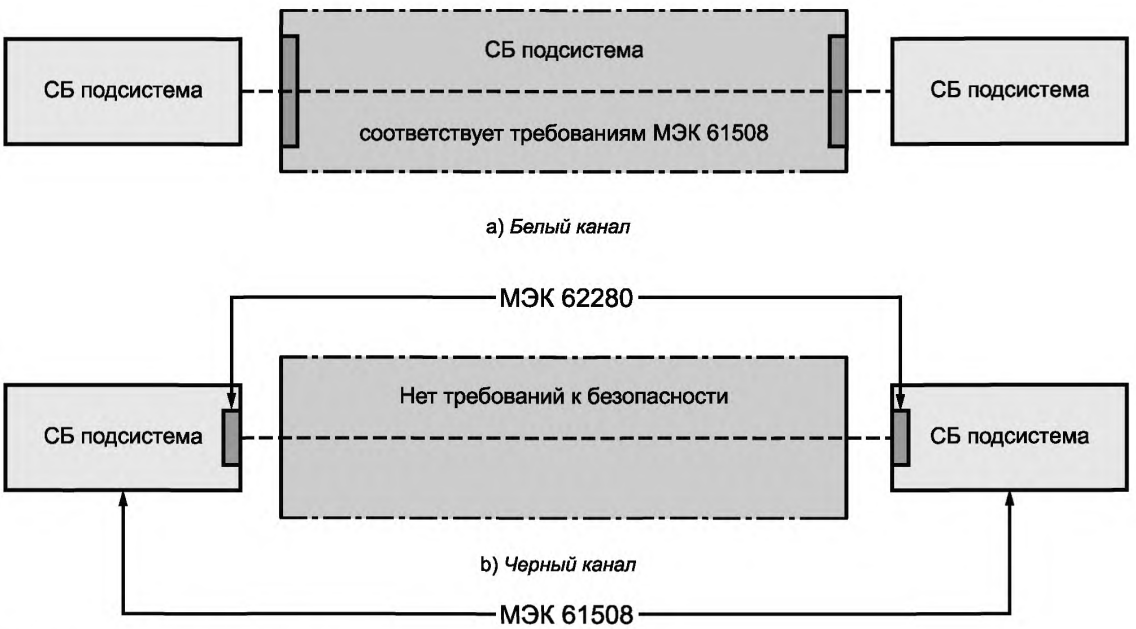
Если при реализации функции безопасности используются средства передачи данных, то должна быть оценена вероятность необнаруженных отказов коммуникационного процесса с учетом ошибок передачи, повторения, исключения, вставки, повторного упорядочивания, искажения, задержки и нелегального проникновения. Эта вероятность должна быть учтена при оценке *PFH* функции безопасности из-за случайных отказов (см. 6.2.1.1.2).

Примечание — Термин «нелегальное проникновение» означает, что истинное содержание сообщения не идентифицировано правильно. Например, сообщение от элемента, не связанного с безопасностью, неправильно идентифицировано как сообщение от элемента, связанного с безопасностью.

Меры, гарантирующие необходимую меру отказов коммуникационного процесса, должны быть реализованы в соответствии с требованиями МЭК 61508-2 и МЭК 61508-3. Допускается два возможных подхода:

a) канал связи должен быть полностью разработан, реализован, и для него должна быть проведена процедура подтверждения соответствия в соответствии со стандартами комплекса МЭК 61508 (так называемый «белый канал», см. рисунок 3a); или

b) части канала связи не разработаны или для них не проведена процедура подтверждения соответствия в соответствии со стандартами серии МЭК 61508 (так называемый «черный канал», см. рисунок 3b). В этом случае для того, чтобы гарантировать обработку отказа, коммуникационный процесс должен быть осуществлен с помощью связанных с безопасностью компонентов СЭРС (СБ), которые взаимодействуют с каналом связи. Это должно быть выполнено в соответствии с МЭК 62280 (при необходимости).



СБ – связанная с безопасностью

Рисунок 3 — Архитектуры для передачи данных

Если передача данных используется для обмена связанными с безопасностью данными с подсистемами, внешними к СЭРС (СБ), то вышеупомянутые требования применяются к СЭРС (СБ) вместе с этими связанными подсистемами.

6.5 Требования к интеграции и тестированию СЭРС (СБ)

6.5.1 Интеграция аппаратных средств

СЭРС (СБ) должна быть интегрирована в соответствии с ее конкретным проектом. В процессе интеграции всех подсистем и компонентов в СЭРС (СБ) СЭРС (СБ) должна быть испытана в соответствии с конкретными тестами интеграции. Эти тесты определены в плане проверки и должны показать, что все модули взаимодействуют правильно и выполняют предназначенные для них функции и не выполняют не предназначенные для них функции.

Кроме того, охватываются требования интеграции аппаратных средств, если успешно выполняются типовые испытания СЭРС (СБ) согласно 6.2.5 и МЭК 61800-5-1 и, кроме того, МЭК 61800-1, или МЭК 61800-2, или МЭК 61800-4 (при необходимости).

6.5.2 Интеграция программного обеспечения

Интеграция части/модуля связанного с безопасностью программного обеспечения СЭРС (СБ) должна быть выполнена согласно МЭК 61508-3. Она должна включать тесты, которые определены в плане проверки программного обеспечения, чтобы гарантировать совместимость программного обеспечения с аппаратными средствами так, чтобы были удовлетворены функциональные требования и требования показателей безопасности.

Примечание — Такое тестирование не подразумевает испытание для всех входных комбинаций. Может быть достаточным испытание для всех классов эквивалентности (см. МЭК 61508-7:2000, пункт В.5.2). Статический анализ (см. МЭК 61508-7:2000, пункт В.6.4), динамический анализ (см. МЭК 61508-7:2000, пункт В.6.5) или анализ отказов (см. МЭК 61508-7:2000, пункт В.6.6) могут сократить количество тестовых сценариев до приемлемого уровня.

6.5.3 Модификации в процессе интеграции

В процессе интеграции для любой модификации или любого изменения СЭРС (СБ) должны быть выполнены анализ влияния, который должен определить все затронутые компоненты, и дополнительная проверка.

6.5.4 Применимые тесты интеграции

Тест(ы) интеграции должен(ны) быть определен(ы) в плане проверки. Должен быть применен функциональный тест, в котором на вход СЭРС (СБ) подаются данные или набор значений, которые адекватно характеризуют обычно ожидаемую работу. Запрашивается функция безопасности (например, активацией STO или нарушением ограничения скорости для SLS) и наблюдается результат ее выполнения, который сравнивается с заданным в спецификации. (См. также раздел 9.)

6.5.5 Документальное оформление поверки

Во время тестирования интеграции СЭРС (СБ) должно быть документально оформлено следующее:

a) используемая версия плана тестирования;

b) критерии принятия тестов интеграции;

c) тип и версия тестируемой СЭРС (СБ);

d) используемые инструменты и оборудование вместе с калибровочными данными;

e) результаты каждого теста;

f) любое несоответствие между ожидаемыми и фактическими результатами.

7 Информация для применения

7.1 Информация и инструкции для применения СЭРС (СБ) в системах безопасности

Следующая информация должна быть документально оформлена производителем и должна быть доступна пользователю.

a) Функциональная спецификация каждой функции и интерфейса, которые доступны для использования в реализации функций безопасности. Она должна включать:

- подробное описание функции безопасности (включая реакцию(и) на нарушение предельных значений);
- функцию реакции на сбой;
- время отклика каждой связанной с безопасностью функции и связанных функций реакции на сбой;
- условие(я) (например, рабочий режим), при котором(ых) функция безопасности предназначена быть активной или отключенной;
- указание приоритета для тех функций, которые одновременно активны и могут конфликтовать друг с другом.

b) Информация о полноте безопасности для каждой функции безопасности, включая:

- возможный УПБ;
- значение *PFH*.

c) Определение условий окружающей среды и условий эксплуатации (включая электромагнитные), при которых предназначено использование СЭРС (СБ) (см. также МЭК 61800-1, или МЭК 61800-2, или МЭК 61800-4, МЭК 61800-3 и МЭК 61800-5-1). Их необходимо учитывать при хранении, транспортировке, установке, вводе в действие, тестировании, эксплуатации и обслуживании.

d) Указание любых ограничений для СЭРС (СБ) на:

- условия окружающей среды, которые должны быть выполнены, чтобы обеспечить подтверждение соответствия предполагаемой интенсивности отказов;
- заданную продолжительность работы СЭРС (СБ) и интервал(ы) контрольной(ых) проверки(ок) при необходимости;
- любое тестирование требований по калибровке или техобслуживанию;
- любые пределы применения СЭРС (СБ), которые должны быть выполнены во избежание систематических отказов;
- возможное УПБ каждой функции безопасности;
- любую информацию, которая требуется, чтобы идентифицировать конфигурацию аппаратных средств и программного обеспечения СЭРС (СБ), чтобы обеспечить управление конфигурацией в соответствии с разделом 4.

e) Руководство по установке и вводу в действие (см. раздел 6 МЭК 61800-5-1:2003), включая наладку и оценивание параметров.

f) Требования для испытания конфигурации функций безопасности в случаях, где полнота средств конфигурации функции безопасности не может быть обеспечена (например, инструменты конфигурирования РС).

Испытание конфигурации выполняется после ввода в действие или модификации конкретного применения, чтобы гарантировать, что используемые функции безопасности СЭРС (СБ) сконфигурированы, как предназначено. В частности, испытание подтверждает намеченные значения параметров СЭРС (СБ). Испытание обычно выполняется и документально оформляется стороной, ответственной за ввод в действие СЭРС (СБ), используя процедуры тестирования, разработанные производителем СЭРС (СБ).

Руководство по испытанию конфигурации должно требовать регистрацию, по крайней мере, следующих элементов:

- описание применения, включая рисунок;
- описание связанных с безопасностью компонентов (включая версии программного обеспечения), которые будут использоваться в применении;
- список функций безопасности, которые будут использоваться в применении СЭРС (СБ);
- результаты каждого испытания этих функций безопасности, используя заданные процедуры тестирования;
- список всех относящихся к безопасности параметров и их значений для СЭРС (СБ);
- контрольные суммы, дата испытаний и подтверждение персоналом, выполняющим испытания.

Испытание конфигурации для СЭРС (СБ) в тиражируемых применениях может быть выполнено как одиночное типовое испытание тиражируемого применения при условии, что оно может гарантировать, что функции безопасности будут сконфигурированы, как предназначено, во всех модулях.

g) *Диагностические проверки* будут выполняться или пользователем, или компонентами устройства, которое включает СЭРС (СБ) (например, PLC, управляющий контроллер).

h) Должны быть обеспечены процедуры эксплуатации и технического обслуживания СЭРС (СБ), которые должны определить следующее:

- стандартные действия, которые должны быть выполнены, чтобы поддержать функциональную безопасность СЭРС (СБ), включая замену компонентов с ограниченным сроком эксплуатации (например, вентиляторы, батареи и т. д.);
- действия и ограничения, необходимые для предотвращения небезопасного состояния и/или уменьшения последствия опасного события;
- процедуры техобслуживания, которые будут выполняться в случае появления сбоев или отказов в СЭРС (СБ), включая:
- процедуры для обнаружения ошибок и восстановления; и
- процедуры для повторного подтверждения соответствия;

- инструментальные средства, необходимые для обслуживания и повторного подтверждения соответствия, а также процедуры для поддержания инструментальных средств и оборудования.

Примечание — Процедуры эксплуатации и технического обслуживания СЭРС (СБ) должны постоянно обновляться, отслеживая, например:

- аудиты функциональной безопасности;
- испытания СЭРС (СБ).

8 Верификация и подтверждение соответствия

8.1 Общие положения

Цель настоящего раздела состоит в том, чтобы гарантировать соответствие с планом обеспечения функциональной безопасности (см. 5.3).

8.2 Верификация

Во время процесса проектирования после каждой стадии проектирования должно быть проверено, что требования данной стадии проектирования были выполнены. Верификация может быть выполнена, используя оценку, анализ, исследование, просмотр и/или тестирование.

8.3 Подтверждение соответствия

После процесса проектирования должно быть проверено, что СЭРС (СБ) выполняет все требования спецификации требований безопасности. Подтверждение соответствия может быть выполнено, используя оценку, анализ, исследование, просмотр и/или тестирование. Рекомендации для предотвращения сбоев во время подтверждения соответствия даны в МЭК 61508-2:2000, таблица В.5.

8.4 Документация

Должна быть подготовлена надлежащая документация по верификации и подтверждению соответствия СЭРС (СБ), включая:

a) версию(и) используемого плана(ов) верификации и подтверждения соответствия;

b) тестируемую(ые) или анализируемую(ые) функцию(и) безопасности вместе со ссылкой на требование(я), определенное(ые) во время планирования верификации и подтверждения соответствия безопасности СЭРС (СБ);

c) используемые инструментальные средства и оборудование;

d) результаты каждой верификации и каждого подтверждения соответствия.

9 Требования к проведению испытаний

9.1 Планирование проведения испытаний

Испытание функций безопасности СЭРС (СБ) должно быть запланировано одновременно с каждой стадией процесса разработки.

План испытания должен быть документально оформлен и должен включать подробное описание:

a) функционального испытания каждой функции безопасности;

b) функционального испытания каждой диагностической функции для каждой функции безопасности;

c) критериев испытаний: «прошла испытания / не прошла испытания».

Испытания могут быть выполнены методами «черного ящика», где никак не учитывается внутренняя реализация функции безопасности, или методами «белого ящика», где используются специальные знания о реализации, чтобы определить тест (например, включение отказа).

Испытание может быть отклонено или заменен метод выполнения верификации и подтверждения соответствия, если разрешено соответствующими требованиями.

9.2 Документация по испытаниям

Во время испытаний функций безопасности СЭРС (СБ) должно быть документально оформлено следующее:

a) используемая версия плана испытаний;

b) критерии принятия тестов;
c) тип и версия тестируемой СЭРС (СБ);
d) используемые инструментальные средства и оборудование вместе с калибровочными данными;
e) условия испытания;
f) персонал, выполняющий испытания;
g) подробные результаты каждого испытания;
h) любое несоответствие между ожидаемыми и фактическими результатами;
i) заключение испытания: либо СЭРС (СБ) «прошла испытания» либо причины отказа.

10 Модификация

10.1 Цель

Цель настоящего раздела состоит в том, чтобы гарантировать, что функциональная безопасность СЭРС (СБ) сохраняется при выполнении модификации проекта после того, как первоначальный проект выпущен для изготовления.

10.2 Требования

До выполнения любого действия по модификации должны быть запланированы соответствующие процедуры. Модификации должны выполняться, по крайней мере, с тем же уровнем знаний и опыта, автоматизированных инструментальных средств, на том же уровне планирования и управления, как и первоначальная разработка СЭРС (СБ). Модификация должна быть выполнена в соответствии с планом модификации.

10.2.1 Запрос на модификацию

Модификация должна инициироваться только проблемой в запросе на модификацию в соответствии с процедурами по управлению функциональной безопасностью (см. раздел 5). В запросе должно быть подробно указано следующее:

a) причины изменения;
b) предложенное изменение (как для аппаратных средств, так и для программного обеспечения).

10.2.2 Анализ влияния

Должна быть выполнена оценка влияния предложенной модификации на функциональную безопасность СЭРС (СБ). Оценка должна включать анализ, достаточный для определения глубины, с которой должен быть предпринят возврат к соответствующим стадиям разработки согласно 5.2.

10.2.3 Авторизация

Авторизация для выполнения требуемой модификации должна зависеть от результатов анализа влияния.

10.2.4 Документация

Для каждого действия по модификации СЭРС (СБ) должна устанавливаться и поддерживаться надлежащая документация, которая должна включать:

a) подробную спецификацию модификации;
b) результаты анализа влияния;
c) все разрешения для выполнения изменений;
d) тестовые примеры для компонентов, включая данные для повторного подтверждения соответствия;
e) историю управления конфигурацией СЭРС (СБ) (для аппаратных средств и программного обеспечения);
f) отклонение от предыдущих операций и условий;
g) необходимые изменения в информации для использования;
h) все применяемые стадии разработки согласно 5.2.

Приложение А
(справочное)

Таблица последовательности выполнения задач

Представленная в таблице А.1 методика проектирования, соответствующая жизненному циклу, описанному в МЭК 61508, подходит для СЭРС (СБ). В ней описан порядок необходимых шагов разработки и даны ссылки на соответствующие разделы или подразделы настоящего стандарта или МЭК 61508.

Примечания

1 Жизненный цикл проектирования и разработки был разделен на «формирование концепции» и «проектирование и разработку», как это установилось в практике проектирования.

2 Если желательна сертификация третьей стороной, то в начале методики проектирования должна быть установлена связь между производителем СЭРС (СБ) и органом по сертификации.

3 В следующей таблице ссылки на МЭК 61508 применяются к первой редакции процитированной части. Номера разделов или подразделов могут измениться в последующих редакциях.

Таблица А.1 — Последовательность выполнения задач

№	Задачи	Ссылки
1	Общие требования	
	Все соответствующие документы должны находиться под контролем соответствующей схемы управления документацией. Описание управления проектом. Сертифицированная система управления качеством	МЭК 61508-1:1998, раздел 5 МЭК 61508-2:2000, подразделы 7.3, 7.7, 7.8, 7.9 МЭК 61508-3:1998, раздел 6, подраздел 7.3, подпункт 7.4.2.1, подразделы 7.7, 7.8, 7.9
2	Спецификация требований безопасности PDS(SR)	Стадия 1 жизненного цикла PDS(SR) (см. 5.2)
	Разработка спецификации требований техники безопасности, включая требования функций безопасности и требования полноты безопасности	См. подраздел 5.4 настоящего стандарта МЭК 61508-1:1998, подраздел 7.6 МЭК 61508-2:2000, подраздел 7.2, таблицы В.1, В.6 МЭК 61508-2:2000, пункты 7.4.4—7.4.6, приложение А МЭК 61508-3:1998, подраздел 7.2, таблицы А.1, В.7 МЭК 61508-3:1998, пункты 7.4.2-7.4.4, таблицы А.3, В.1 МЭК 61508-7:2000, таблица С.1 Примеры в МЭК 61508-5, примеры в МЭК 61508-6:2000, приложение А
3	Верификация требований безопасности СЭРС (СБ)	
	a) Анализ спецификации требований безопасности; b) Проверка независимым лицом или подразделением при необходимости	a) См. подраздел 8.2 настоящего стандарта; b) МЭК 61508-2:2000 и МЭК 61508-3:1998, подраздел 7.9

Продолжение таблицы А.1

№	Задачи	Ссылки
4	Формирование концепции	Стадия 3 жизненного цикла СЭРС (СБ) (см. 5.2)
	a) Проектирование аппаратных средств на уровне архитектуры, включая: - блок-схемы связанных с безопасностью аппаратных средств; интерфейсы пользователя и процесса; - безопасность путей, соответствующих сигналов; - источник питания; - разделение независимых каналов для обеспечения отказоустойчивости; - связи между независимыми каналами, для обеспечения охвата диагностикой; b) проектирование программного обеспечения на уровне архитектуры, включая: - описание функций, выполняемых связанным с безопасностью программным обеспечением; - взаимодействие с аппаратными средствами; - диаграммы состояний предполагаемого поведения программного обеспечения; - интерфейсы пользователя и процесса; - возможности обнаружения сбоев и реакции на сбой; - анализ структуры программного обеспечения, например на уровне блок-схем; - управление и хранение данных, связанных с безопасностью; - версии процедур; - используемые инструменты, например компилятор, средство проверки кода, и т. д. c) Рекомендация Предварительная оценка вероятности отказов функции безопасности из-за случайных отказов аппаратных средств на уровне функциональных блок-схем	a) См. раздел 6 настоящего стандарта МЭК 61508-2:2000, подраздел 7.4, приложение А, таблицы В.2, В.6 Примеры в МЭК 61508-6:2000, приложения А и D b) 61508-2:2000 МЭК, подпункт 7.2.3.1 (h) 61508-3:1998 МЭК, подпункты 7.2.2.8, 7.2.2.10, 7.4.2.3, таблицы А.2, В.1, В.7, В.9 МЭК 61508-7:2000, таблица С.1 c) МЭК 61508-1:1998, таблица 2 МЭК 61508-2:2000, пункт 7.4.3, таблицы 3, А.1, приложение С МЭК 61508-3:1998, таблица В.4 (FMEA) Примеры в МЭК 61508-6:2000, приложения С и D
5	Верификация концепции	
	a) Анализ проекта системы; b) Проверка независимым лицом или подразделением при необходимости	a) См. подраздел 8.2 настоящего стандарта; b) МЭК 61508-2:2000 и МЭК 61508-3:1998, подраздел 7.9

Продолжение таблицы А.1

№	Задачи	Ссылки
6	Планирование подтверждения соответствия	Стадия 2 жизненного цикла СЭРС (СБ) (см. 5.2)
	a) Подробное планирование подтверждения соответствия связанной с безопасностью СЭРС (СБ); b) План подтверждения соответствия должен быть сформирован параллельно со стадией 9.3 «Проектирование и разработка»	a) См. подраздел 8.3 настоящего стандарта; b) МЭК 61508-2:2000, подраздел 7.3, таблица В.5. МЭК 61508-3:1998, подраздел 7.3, таблицы А.7, В.3, В.5
7	План верификации и подтверждения соответствия	
	a) Анализ плана подтверждения соответствия; b) Проверка независимым лицом или подразделением при необходимости	a) См. подраздел 8.2 настоящего стандарта; b) МЭК 61508-2:2000 и МЭК 61508-3:1998, подраздел 7.9
8	Проектирование и разработка	
	a) проектирование аппаратных средств; b) проектирование программного обеспечения; c) прогноз надежности (вычисление вероятности отказа функции безопасности из-за случайных отказов аппаратных средств), включая: - тип СЭРС (СБ); - ДБО; - функциональную блок-схему; - модель надежности; - базу данных модели (списки устройства); - вычисление *PFH*; - заданную продолжительность работы; - время восстановления, интервал контрольных проверок (при необходимости)	См. раздел 6 настоящего стандарта a) МЭК 61508-2:2000, подраздел 7.4, приложение А, таблицы В.2, В.3, В.6; b) МЭК 61508-3:1998, пункты 7.4.5, 7.4.6, таблица А.4; c) МЭК 61508-1:1998, таблица 2. МЭК 61508-2:2000, пункты 7.4.3, 7.4.7, таблицы 3, А.1, приложение С. МЭК 61508-3:1998, таблица В.4 (FMEA). Примеры в МЭК 61508-6:2000, приложения С и D
9	Верификация проекта	
	a) Анализ проекта системы; b) Функциональные испытания на уровне модуля; c) Проверка независимым лицом или подразделением при необходимости	a) См. подраздел 8.2 настоящего стандарта; c) МЭК 61508-2:2000, подраздел 7.9; МЭК 61508-3:1998, пункты 7.4.7, 7.4.8, 7.5, 7.9, таблицы А.5, А.9
10	Интеграция СЭРС (СБ)	Стадия 4 жизненного цикла СЭРС (СБ) (см. 5.2)
	Интеграция и тестирование связанной с безопасностью СЭРС (СБ)	См. 6.5

Окончание таблицы А.1

№	Задачи	Ссылки
11	Верификация интеграции СЭРС (СБ)	
	Анализ результатов интеграционного теста аппаратные средства/программное обеспечение и его документальное оформление	См. подраздел 8.2 настоящего стандарта; МЭК 61508-2:2000, подразделы 7.5, 7.9, таблицы В.3, В.6; МЭК 61508-3:1998, подпункты 7.4.3,2(f), 7.4.5.5, 7.4.6.2, пункт 7.4.7, подразделы 7.5, 7.9, таблицы А.5, А.6, А.9
12	Установка, ввод в действие и эксплуатация (документация пользователя)	Стадия 5 жизненного цикла СЭРС (СБ) (см. 5.2)
	Разработка документации пользователя по установке, вводу в действие, эксплуатации и сопровождению СЭРС (СБ)	См. раздел 7 настоящего стандарта; МЭК 61508-2:2000, подраздел 7.6, таблица В.4
13	Верификация документации пользователя	
	a) Анализ документации пользователя по установке, вводу в действие, эксплуатации и сопровождению СЭРС (СБ); b) Проверка независимым лицом или подразделением при необходимости	a) См. подраздел 8.2 настоящего стандарта; b) МЭК 61508-2:2000 и МЭК 61508-3:1998, подраздел 7.9
14	Подтверждение соответствия СЭРС (СБ)	Стадия 6 жизненного цикла СЭРС (СБ) (см. подраздел 5.2)
	a) Предоставление всей информации, необходимой для подтверждения соответствия СЭРС (СБ); b) Полное программное обеспечение с надлежащей документацией; c) Тесты и процедуры подтверждения соответствия согласно плану подтверждения соответствия; d) Документация по результатам тестов подтверждения соответствия; e) Подготовка надлежащей документации к подтверждению соответствия третьей стороной в случае необходимости	a) См. подраздел 8.3 настоящего стандарта; c) МЭК 61508-2:2000, подраздел 7.7, таблицы В.5, В.6; МЭК 61508-3:1998, подпункт 7.5.2.7, подразделы 7.7, 7.9, таблица А.7
15	Процедура модификации СЭРС (СБ)	
	a) Запрос на модификацию и его анализ; b) Надлежащая документация всех модифицируемых частей СЭРС (СБ); c) Повторная верификация модифицируемых частей; d) Обновление прогноза надежности, если модификация оказывает влияние на: отказоустойчивость, вероятность опасных отказов, охват диагностикой или отказы по общей причине; e) Повторное подтверждение соответствия, по крайней мере, модифицируемых частей СЭРС (СБ); f) Модификация программного обеспечения	a) См. раздел 10 настоящего стандарта; b) МЭК 61508-2:2000, подраздел 7.16; МЭК 61508-3:1998, подпункт 7.5.2.5, подраздел 7.8, пример в МЭК 61508-1:1998, рисунок 9; f) МЭК 61508-3:1998, подпункты 7.1.2.8, 7.5.2.6, пункты 7.6.2, 7.8.2, таблица А.8

Приложение В
(справочное)

Пример определения *PFH*

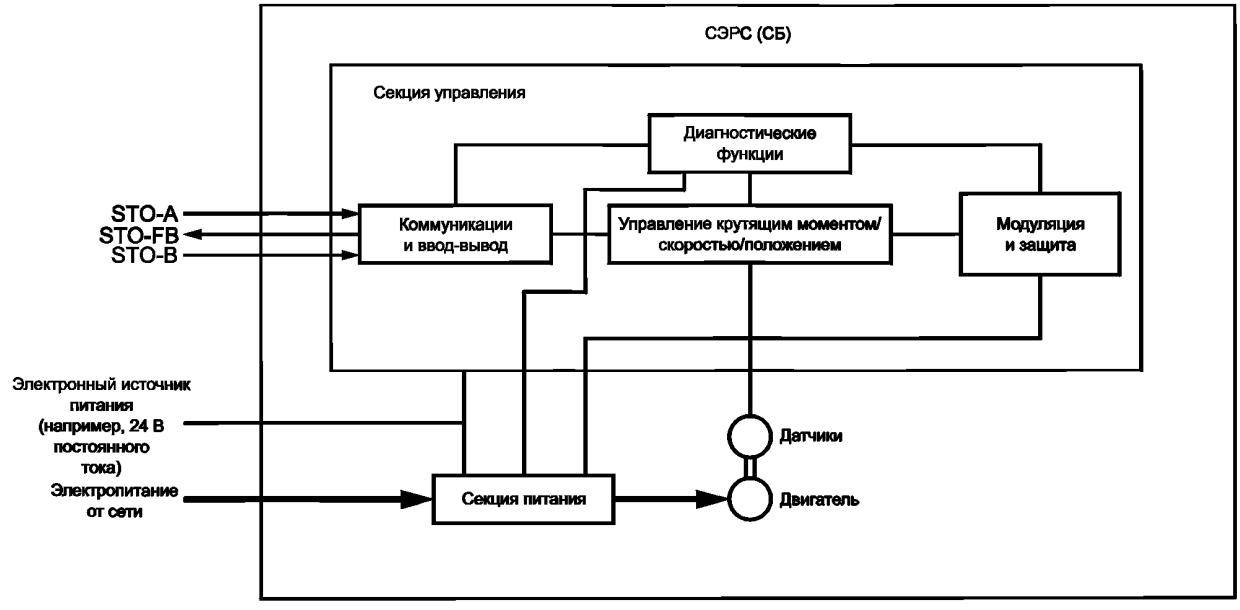
В.1 Общие положения

Данное приложение описывает определение *PFH* примера СЭРС (СБ) с функцией безопасности — безопасное отключение крутящего момента (STO). Чтобы подробно показать, как может быть вычислено значение *PFH*, представлены все необходимые требования для СЭРС (СБ) и ее внутренних структурных частей.

В.2 Структура СЭРС (СБ), рассматриваемого примера

В.2.1 Общие положения

СЭРС (СБ), описанная в настоящем пункте, реализует функцию безопасности STO, которая запускается через два дублирующих входных цифровых интерфейса и выдает сигнал обратной связи через один выходной цифровой интерфейс (см. рисунок В.1).



STO-A – входной канал А сигнала запуска STO;
STO-B – входной канал В сигнала запуска STO;
STO-FB – выходной сигнал обратной связи STO

Рисунок В.1 — Пример СЭРС (СБ)

Требования:
- УПБ 2;
- непрерывный режим работы.

В СЭРС (СБ) функция безопасности STO реализована вместе со стандартной функциональностью СЭРС (СБ), использующей только некоторые отдельные компоненты функции безопасности.

Так как канал подачи питания один, то СЭРС (СБ) разделена на две независимые подсистемы: двухканальная подсистема A/B и подсистема электропитания / контроля напряжения (PS/VM). См. рисунок В.2.

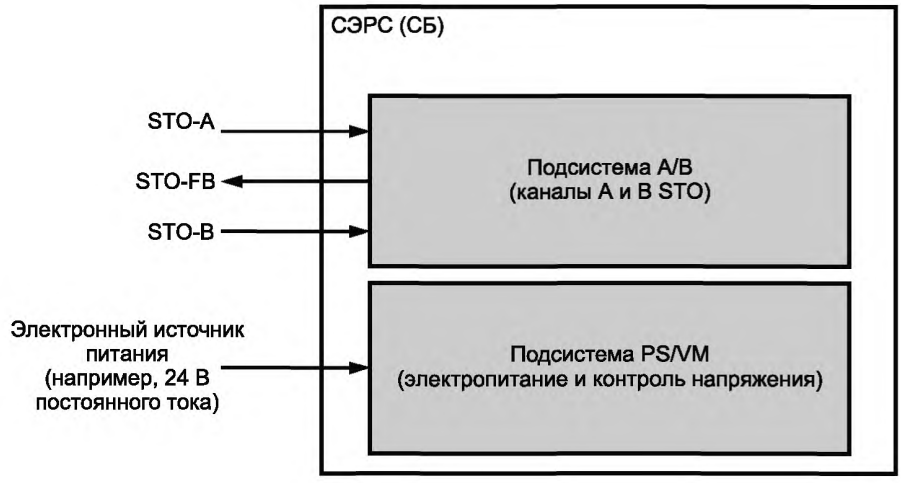


Рисунок В.2 — Подсистемы СЭРС (СБ)

Значение *PFH* функции безопасности STO рассматриваемого примера СЭРС (СБ) вычисляется следующим образом:

$$PFH_{\text{СЭРС (СБ)}} = PFH_{\text{A/B}} + PFH_{\text{PS/VM}},$$

где $PFH_{\text{A/B}}$ и $PFH_{\text{PS/VM}}$ — значения *PFH* подсистем A/B и PS/VM соответственно.

В.2.2 Подсистема A/B

Функция безопасности STO реализована двумя каналами, чтобы достигнуть отказоустойчивости аппаратных средств, равной 1, и ее моделирует подсистема A/B, для которой вычисляется независимое значение *PFH*. Реализация этой подсистемы обеспечивает следующие системные свойства, связанные с функцией безопасности:

- тип B (сложные аппаратные средства);
- отказоустойчивость аппаратных средств равна 1 (двухканальная реализация).

Архитектурные ограничения подсистемы типа B (см. 6.2.2.3) показывают, что для УПБ 2 и отказоустойчивости аппаратных средств, равной 1, доля безопасных отказов (ДБО) должна составить, по крайней мере, 60%.

В.2.3 Подсистема PS/VM

Поскольку внутренний источник электропитания выполнен по одноканальной схеме, то реализован монитор напряжения (VM). Внутренний источник электропитания и монитор напряжения моделируются отдельной подсистемой PS/VM, для которой вычисляется независимое значение *PFH*. Реализация этой подсистемы обеспечивает следующие системные свойства, связанные с функцией безопасности:

- тип B (сложные аппаратные средства);
- отказоустойчивость аппаратных средств равна 0 (одноканальная реализация).

Архитектурные ограничения подсистемы типа B (см. 6.2.2.3) показывают, что для УПБ 2 и отказоустойчивости аппаратных средств, равной 0, доля безопасных отказов (ДБО) должна составить, по крайней мере, 90%.

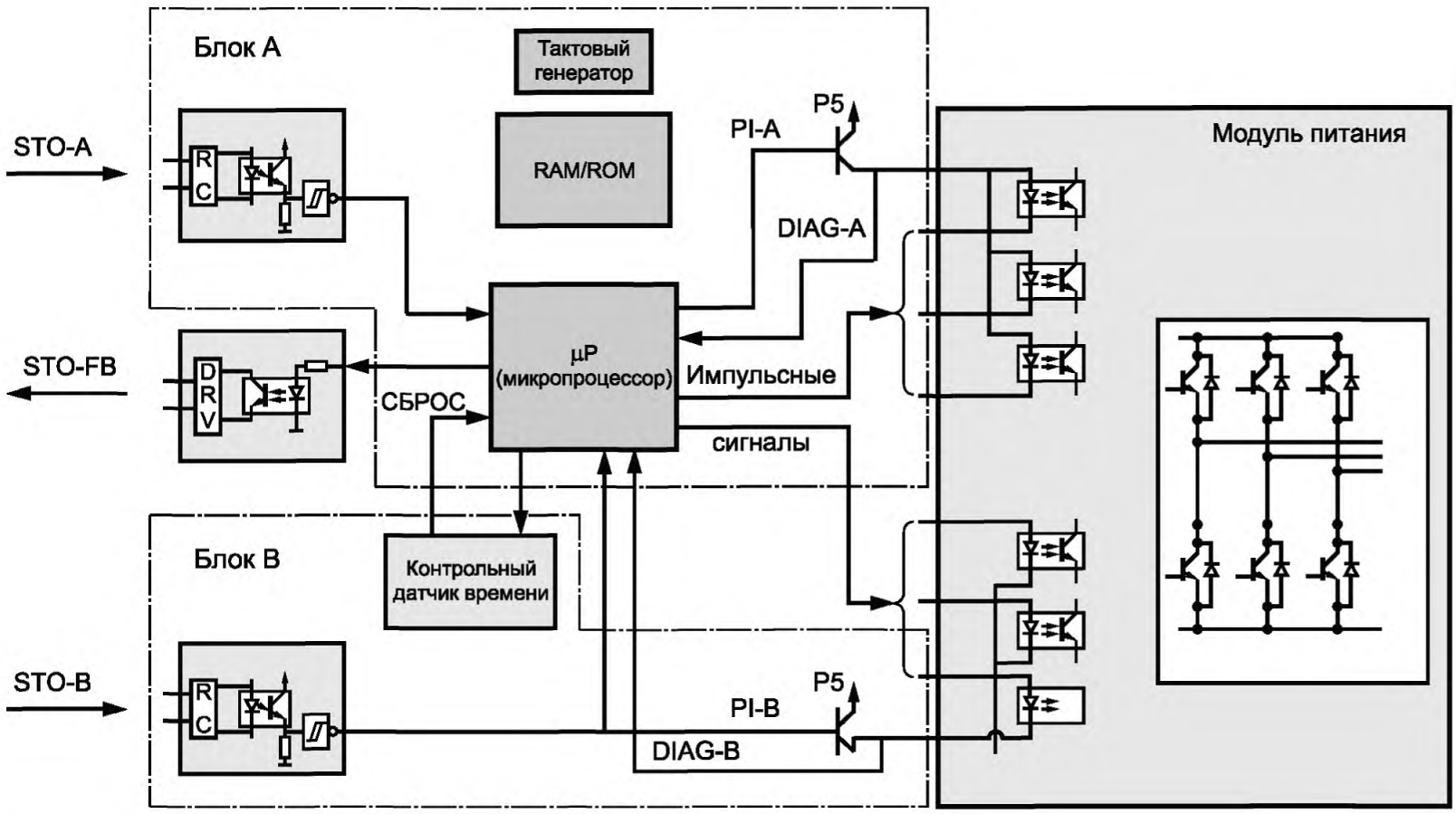
В.3 Пример определения величины *PFH* для СЭРС (СБ)

В.3.1 Подсистема A/B (главная подсистема)

В.3.1.1 Деление на функциональные блоки

Подсистема A/B в СЭРС (СБ) является частью реализации функции безопасности STO и состоит из двух каналов, что необходимо для отказоустойчивости аппаратных средств, равной 1. На рисунке В.3 схематически представлена блок-схема СЭРС (СБ), на которой выделены части, выполняющие функцию безопасности STO.

Для вычисления значения *PFH* подсистема A/B далее декомпозируется на функциональные блоки и для каждого из них определяется интенсивность отказов. Из-за малого числа компонентов в цифровых триггерах на входе схемы и в схемах отключения, достаточно рассмотреть только два функциональных блока.



P5 – напряжение питания 5 В;
PI-A(B) – импульс блокирования канала A(B);
DIAG-A(B) – диагностический сигнал канала A(B);
RC – резисторно-емкостной фильтр;
DRV – выходное задающее устройство

Рисунок В.3 — Функциональные блоки подсистемы A/B

Примечание — Отказы компонентов в самом модуле питания не вызывают потерю функции безопасности. Поэтому модуль питания не должен быть включен в какую-либо подсистему, вносящую вклад в значение *PFH*.

В.3.1.2 Определение интенсивности отказов функциональных блоков

В.3.1.2.1 Анализ функционального блока

Для каждого функционального блока необходимо определить, какие отказы должны рассматриваться как *опасные отказы*. Это позволяет далее применить анализ вида и последствий отказов (*FMEA*) для компонентов функционального блока.

В.3.1.2.2 *FMEA* компонентов

FMEA компонентов схемы функционального блока определяет, какие компоненты связаны с реализацией функции безопасности, а затем распределяет каждому виду отказов каждого компонента, связанного с реализацией функции безопасности, атрибут безопасности или опасности, используя критерии, определенные в процессе анализа функционального блока, упомянутого в В.3.1.2.1. Для простых компонентов, если надежные данные о соотношении безопасных и опасных видов отказа не доступны, то одиночный опасный отказ, приводящий к полному отказу компонента, рассматривают как опасный отказ. Для сложных компонентов в соответствии с приложением С МЭК 61508-6:2000 принимают, что такие компоненты имеют 50% безопасных и 50% *опасных отказов*.

Кроме того, FMEA определяет долю интенсивности *опасного отказа* каждого компонента, который обнаружен доступной диагностической функциональностью. Для сложных компонентов доля обнаруживаемых опасных отказов должна быть определена с помощью таблиц в МЭК 61508-2. Это позволяет определить интенсивность λ_{DD} (опасных обнаруживаемых) и λ_{DU} (опасных необнаруживаемых) отказов компонента.

Общие интенсивности отказов функционального блока (λ_S, λ_{DD}, λ_{DU}) вычисляются сложением значений интенсивностей безопасных отказов, значений интенсивностей обнаруживаемых *опасных отказов* и значений интенсивностей необнаруживаемых *опасных отказов* всех связанных с безопасностью компонентов функционального блока.

В.3.1.2.3 Упрощенный метод определения различающихся интенсивностей отказов

Для сложных схем аппаратных средств с большим количеством компонентов покомпонентный анализ с помощью FMEA не всегда возможен практически. Поэтому обычно выбирают упрощенный метод, представленный в приложении С МЭК 61508-6:2000.

Общая интенсивность отказов функционального блока со сложной схемой, вычисляемая как сумма интенсивностей отказов всех компонентов, определяется при условии, что суммы значений интенсивностей опасных и интенсивностей безопасных отказов для данного функционального блока являются равными. Доля обнаруживаемых отказов определяется при помощи таблиц МЭК 61508-2.

Данный метод также позволит получить интенсивности отказов λ_S, λ_{DD}, λ_{DU} функционального блока.

В.3.1.3 Доля безопасных отказов

Используя упрощенный метод, упомянутый в В.3.1.2.3, интенсивность отказов функциональных блоков определяется следующим образом:

- доля безопасных отказов среди отказов схем печатной платы составляет 50% (см. примечание).

Примечание — Доля *опасных отказов* схем печатной платы в таком случае также составляет 50%.

Охват диагностикой (ОД) оценивается при помощи таблиц МЭК 61508-2.

Таблица В.1 — Определение значения ОД для подсистемы A/B

Метод (МЭК 61598-2)	Уровень ОД	Реализация диагностического теста
Таблица А.3. Обнаружение отказов путем мониторинга в неавтономном режиме	90 %	Циклический тест проверяет избыточные каналы
Таблица А.3. Контролируемая избыточность	99 % / 90 %	Циклический тест проверяет избыточные каналы
Таблица А.4. Самотестирование с помощью программного обеспечения: «блуждающий бит» (один канал)	90 %	Самотестирование микропроцессора
Таблица А.6. Тест ОЗУ «GALPAT»	90 %	Выполняется микропроцессором
Таблица А.10. Контрольный датчик времени с отдельной временной базой и временным окном	90 %	При проектировании контрольного датчика времени
Таблица А.8. Анализ с использованием тестирующих комбинаций	99 %	Выполняется при тестировании RAM
Таблица А.15. Перекрестный контроль нескольких исполнительных устройств	99 %	Циклический тест контролирует отключение у обоих исполнительных устройств

- $ОД_A$ для функционального блока А = 90 % (см. таблицу В.1);
- $ОД_B$ для функционального блока В = 90 % (см. таблицу В.1).

Интенсивность отказов схемы функциональных блоков *A* и *B* (реальные значения примера, выраженные как число отказов в единицу времени (FIT) в единицах 10^{-9}/ч):

Блок А

λ_A (общая интенсивность отказов)		450 FIT
λ_{AS} (доля безопасных отказов)	0,5·450 FIT	225 FIT
λ_{AD} (доля *опасных отказов*)	0,5·450 FIT	225 FIT
$\lambda_{ADD} = ОД_A \cdot \lambda_{AD}$	0,9·225 FIT	202,5 FIT
$\lambda_{ADU} = (1 - ОД_A) \cdot \lambda_{AD}$	(1– 0,9)·225 FIT	22,5 FIT

Блок В

λ_B (общая интенсивность отказов)		70 FIT
λ_{BS} (доля безопасных отказов)	0,5·70 FIT	35 FIT
λ_{BD} (доля опасных отказов)	0,5·70 FIT	35 FIT
$\lambda_{BDD} = ДО_B \cdot \lambda_{BD}$	0,9·35 FIT	31,5 FIT
$\lambda_{BDU} = (1 - ОД_B) \cdot \lambda_{BD}$	(1– 0,9) ·35 FIT	3,5 FIT

Доля безопасных отказов (ДБО) подсистемы *A/B* вычисляется согласно МЭК 61508-2:2000, подраздел С.1, перечисление g).

$$ДБО_{A/B} = [(\lambda_{AS} + \lambda_{BS}) + (ОД_A \cdot \lambda_{AD}) + (ДО_B \cdot \lambda_{BD})] / [(\lambda_{AS} + \lambda_{BS}) + (\lambda_{AD} + \lambda_{BD})] =$$

$$= [(225 + 35) + (0{,}9 \cdot 225) + (0{,}9 \cdot 35)]\ \text{FIT} / [(225 + 35) + (225 + 35)\ \text{T}]\ \text{FIT} = 494\ \text{FIT}/520\ \text{FIT}.$$

$ДБО_{A/B}$ = 95 %.

B.3.1.4 $\beta_{A/B}$ фактор отказа по общей причине

$\beta_{A/B}$ фактор отказа по общей причине оценивается с помощью таблицы D.4 приложения D МЭК 61508-6:2000.

$\beta_{A/B}$ = 2 %.

B.3.1.5 Модель надежности (Маркова)

Модель надежности подсистемы A/B реализована как модель Маркова в виде графа состояний и показана на рисунке B.4.

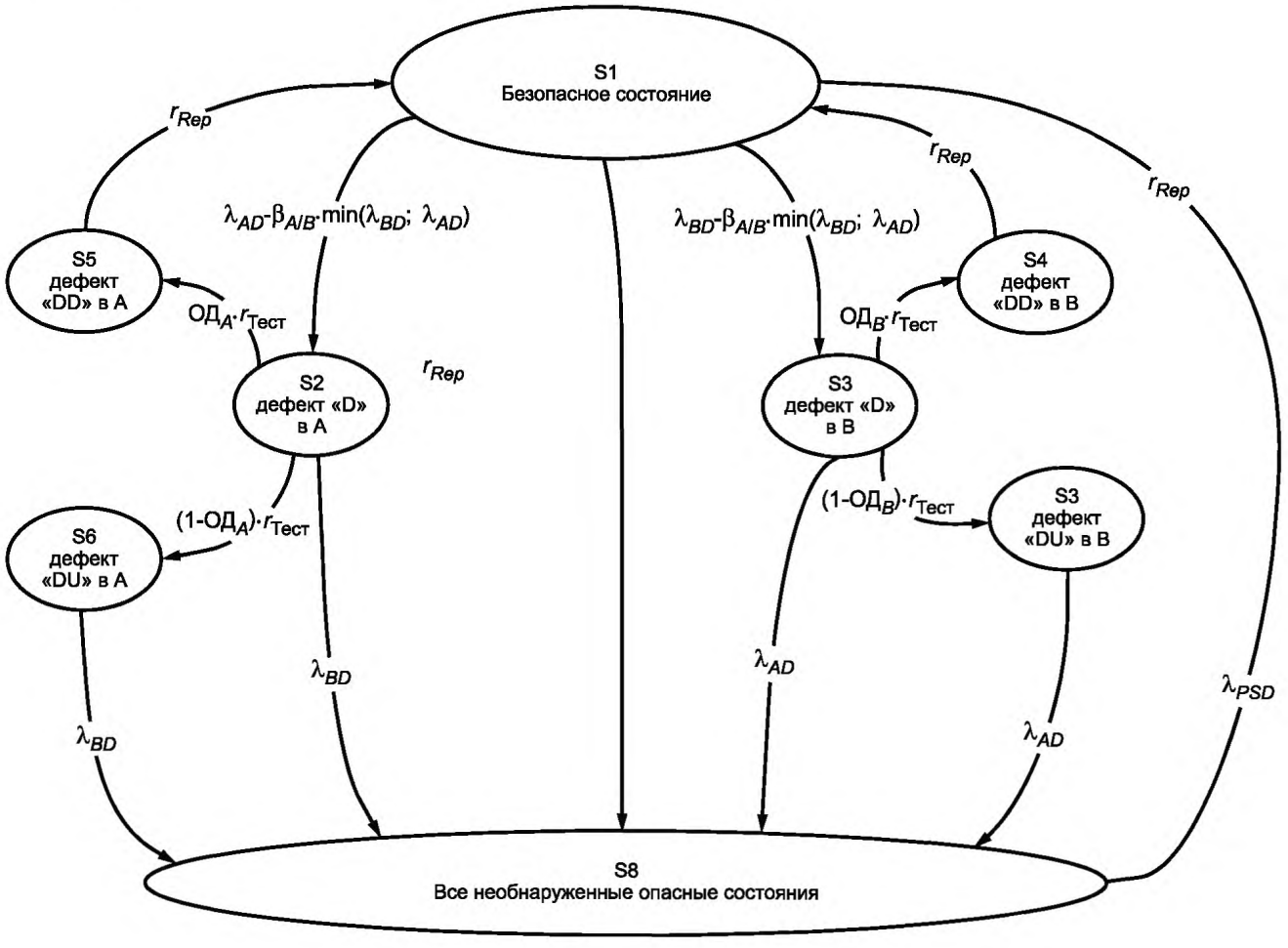


Рисунок B.4 — Модель надежности (Маркова) подсистемы A/B

Примечания

1 Вышеупомянутая модель Маркова должна рассматриваться как приближение, поскольку процессы перехода, соответствующие диагностическим тестам, и событие, инициирующее восстановления вследствие их природы, строго математически не соответствуют необходимым условиям для метода Маркова.

2 Модель, представленная на рисунке B.4, достаточно подробно показывает включение диагностических тестов. Так как величины интенсивностей отказов и частоты тестирования известны, модель может быть упрощена. Обычно не так важно, равен период тестирования 1/8 ч или 1/168 ч (см. таблицу B.2).

3 На рисунке B.4 min(λ_{BD}; λ_{AD}) означает наименьшее значение из λ_{BD} и λ_{AD}.

Модель не учитывает «безопасные» отказы, потому что они не оказывают существенного влияния на значение *PFH*. Модель предполагает, что СЭРС (СБ) отключается и восстанавливается после обнаружения отказа.

Интенсивность *отказов по общей причине* определяется $\beta_{A/B}$ фактором и минимальным значением среди интенсивностей опасных отказов функциональных блоков A и B (см. примечание 3).

Примечание — Интенсивность одновременных отказов обоих блоков никогда не может быть больше, чем наименьшая интенсивность отказов среди обоих блоков.

В состоянии S2 функциональный блок А перестал работать, и возникла опасная ситуация. В результате работы диагностического теста может быть выполнен переход в одно из следующих трех состояний.

- В состояние S5, если диагностический тест обнаруживает отказ, и функциональный блок восстанавливается.
- В состояние S6, если диагностический тест не обнаруживает отказ.
- В состояние S8, если функциональный блок В перестал работать, прежде чем диагностический тест обнаруживает отказ в функциональном блоке А.

В состоянии S6 функциональный блок А перестал работать из-за не обнаруживаемого опасного отказа. В состоянии S8 блок В опасно отказал.

Состояние S8 представляет опасную ситуацию, где функция безопасности больше недоступна, и никакой тест больше неэффективен. Вследствие непрерывного режима работы, принятого для СЭРС (СБ), состояние S8 также является «опасным событием», так как запрос на функцию безопасности выполняется к опасно отказавшей СЭРС (СБ).

B.3.1.6 Вычисление значения *PFH*

Значения λ, ОД и β-факторов получены в B.3.1.3 и B.3.1.4.

Дополнительные определения:

r_{Test} = 1/8 ч, 1/24 ч, 1/168 ч (частота диагностического теста);

r_{Rep} = 1/8 h (частота ремонтов);

T_M = 10 лет или 20 лет (заданная продолжительность работы).

Чтобы определить значение *PFH*, должны быть вычислены зависимые от времени вероятности перехода $[p_i(t)]$ для каждого состояния $[C_i]$ модели Маркова. Начальное значение вероятности всех состояний, кроме состояния S1, равно нулю. Начальное значение вероятности состояния S1 равно единице. Вычисления должны быть выполнены на заданной продолжительности работы T_M.

$$PFH_{A/B} = \frac{1}{T_M}\int_1^{T_M} \beta_{A/B} \cdot \min(\lambda_{AD}, \lambda_{BD}) \cdot p_1(t) + \lambda_{BD} \cdot p_2(t) + \lambda_{AD} \cdot p_3(t) + \lambda_{BD} \cdot p_6(t) + \lambda_{AD} \cdot p_7(t)]dt.$$

Результаты вычислений для различных значений параметров $\beta_{A/B}$, r_{Rep}, r_{Test} и T_M представлены в таблице B.2.

Таблица B.2 — Результаты вычислений значений *PFH* для подсистемы A/B

$\beta_{A/B}$	r_{Rep}	r_{Test}	T_M (годы)	$PFH_{A/B}$
2 %	1/8 ч	1/8 ч	10	$6{,}84 \cdot 10^{-10}$/ч
2 %	1/8 ч	**1/24 ч**	10	$6{,}84 \cdot 10^{-10}$/ч
2 %	1/8 ч	**1/168 ч**	10	$6{,}86 \cdot 10^{-10}$/ч
2 %	1/8 ч	**1/672 ч**	10	$6{,}91 \cdot 10^{-10}$/ч
2 %	1/8 ч	**1/8760 ч**	10	$7{,}72 \cdot 10^{-10}$/ч
2 %	**1/8760 ч**	1/8 ч	10	$6{,}83 \cdot 10^{-10}$/ч
2 %	1/8 ч	1/8 ч	**20**	$7{,}38 \cdot 10^{-10}$/ч
2 %	1/8 ч	**1/672 ч**	20	$7{,}46 \cdot 10^{-10}$/ч
3 %	1/8 ч	1/8 ч	20	$1{,}05 \cdot 10^{-9}$/ч
5 %	1/8 ч	1/8 ч	20	$1{,}68 \cdot 10^{-9}$/ч

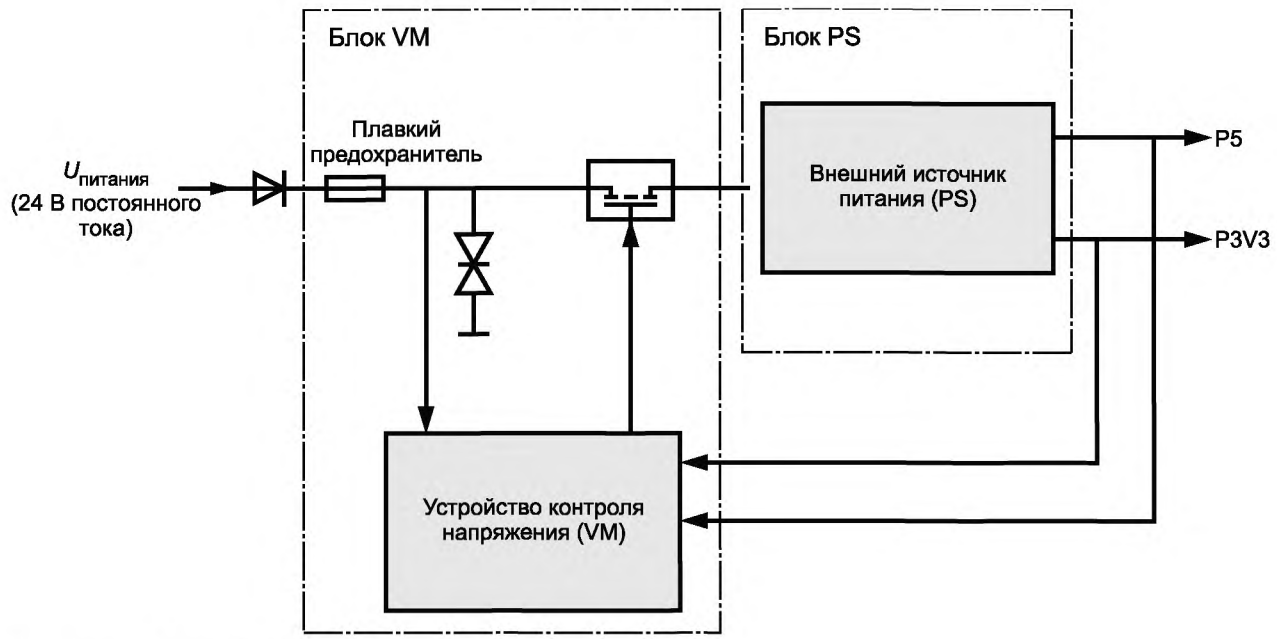
Примечание — Значения, выделенные полужирным текстом, дают значения, отличные от предыдущей строки.

Результаты в таблице B.2 показывают влияние частоты тестирования, заданной продолжительности работы и фактора, связанного с отказами по общей причине, на значение *PFH*. Чтобы показать влияние каждого параметра на значение PFH, даны различные значения параметров.

В.3.2 Подсистема PS/VM

В.3.2.1 Деление на функциональные блоки

Для реализации функции безопасности STO используется одноканальная подсистема PS/VM, включающая специально предназначенную для нее систему контроля. На рисунке В.5 представлена подсистема PS/VM, которая включает два функциональных блока: отдельный внутренний источник питания (PS) и схему контроля напряжения (VM).



P5 – источник питания 5 В;
P3V3 – источник питания 3 В

Рисунок В.5 — Функциональные блоки подсистемы PS/VM

В.3.2.2 Интенсивность отказов функциональных блоков

Интенсивность отказов каждого функционального блока определяется с помощью метода, используемого в В.3.1.2.

В.3.2.3 Доля безопасных отказов

Используя упрощенный метод, используемый в В.3.1.2.3, интенсивности отказов функциональных блоков определены следующим образом:

часть безопасных отказов в схемах печатной платы составляет 50 % (см. примечание).

Примечание — В таком случае часть *опасных отказов* в схемах печатной платы также составляет 50 %.

Охват диагностической (ОД) может быть оценен при помощи таблиц МЭК 61508-2:2000, приложение А.

ОД для функционального блока PS равен 99 % (см. таблицу В.3).

Таблица В.3 — Определение значения ОД для подсистемы PS/VM

Метод (МЭК 61598-2)	Уровень ОД	Метод реализации
Таблица А.9. Контроль напряжения (дополнительно) или отключение питания с системой аварийного отключения или с системой подключения ко второму источнику питания	Высокий	Блок контроля напряжения отключает питание PDS(SR)

ОД для функционального блока VM равен 0 % (никакой контроль блока контроля напряжения не предусмотрен).

Интенсивность отказов схем функциональных блоков PS и VM (в примере используются реальные значения).

Блочная PS		
λ_{PS} (общая интенсивность отказов)		250 FIT
λ_{PSS} (доля безопасных отказов)	0,5·250 FIT	125 FIT
λ_{PSD} (доля опасных отказов)	0,5·250 FIT	125 FIT
$\lambda_{PSDD} = ОД_{PS} \cdot \lambda_{PSD}$	0,99·125 FIT	123,75 FIT
$\lambda_{PSDU} = (1 - ОД_{PS}) \cdot \lambda_{PSD}$	(1 – 0,99)· 125 FIT	1,25 FIT
Блок VM		
λ_{VM} (общая интенсивность отказов)		250 FIT
λ_{VMS} (доля безопасных отказов)	0,5·250 FIT	125 FIT
λ_{VMD} (доля *опасных отказов*)	0,5·250 FIT	125 FIT

Доля безопасных отказов (ДБО) подсистемы PS/VM вычисляется согласно МЭК 61508-2:2000, подраздел С.1, перечисление g). См. примечание.

$ДБО_{PS/VM} = [\lambda_{PSS} + (ОД_{PS} \cdot \lambda_{PSD})] / \lambda_{PS} = [125 + (0,99 \cdot 125)]$ FIT/250 FIT.

$ДБО_{PS/VM} = 99,5$ %.

Примечание — Блок контроля напряжения не вносит вклад в ДБО.

B.3.2.4 $\beta_{PS/VM}$ фактор *отказа по общей причине*

$\beta_{PS/VM}$ фактор *отказа по общей причине* оценивается с помощью таблицы D.4 приложения D МЭК 61508-6:2000.

$\beta_{PS/VM} = 2$ %.

B.3.2.5 Модель надежности (Маркова)

Модель надежности подсистемы PS/VM реализована как модель Маркова в виде графа состояний и показана на рисунке B.6.

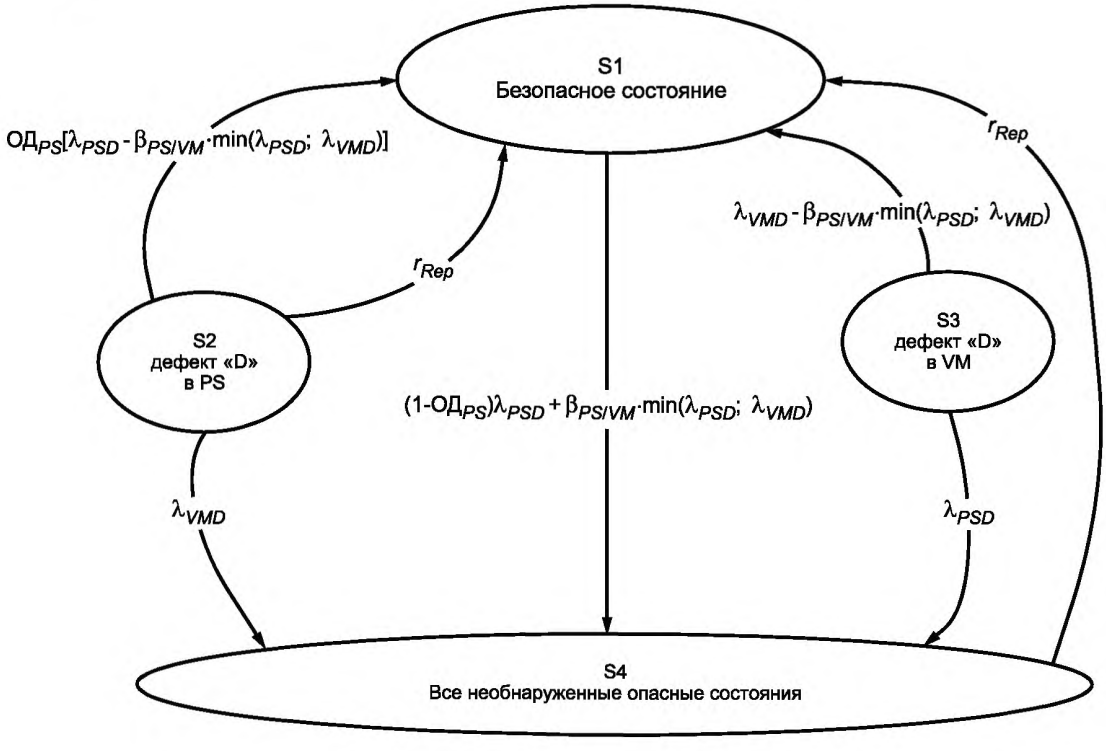


Рисунок B.6 — Модель надежности (Маркова) подсистемы PS/VM

Примечания

1 Вышеупомянутая модель Маркова должна рассматриваться как приближение, поскольку процессы перехода, соответствующие диагностическим тестам и событие, инициирующее восстановления, вследствие их природы, строго математически не соответствуют необходимым условиям для метода Маркова.

2 Блок контроля напряжения обеспечивает непрерывный контроль схемы источника питания. Поэтому частота тестирования в модели не появляется. Так как величины интенсивностей отказов и частоты тестирования известны, модель может быть упрощена. Изображенная версия предназначена для ясности.

В модели представлены возможные опасные состояния и не показаны безопасные состояния, которые не оказывают существенного влияния на значение *PFH*, но увеличили бы сложность модели. Модель предполагает, что СЭРС (СБ) отключается и восстанавливается после обнаружения отказа.

Интенсивность *отказов по общей причине* определяется $\beta_{PS/VM}$ фактором и минимальным значением среди интенсивностей *опасных отказов* функциональных блоков PS и VM (см. примечание).

Примечание — Так как *отказ по общей причине* представляет собой одновременный отказ блоков PS и VM, у которых различная интенсивность отказов, то интенсивность *отказов по общей причине* никогда не может быть больше, чем наименьшая интенсивность отказов среди обоих блоков.

В состоянии S2 функциональный блок PS перестал работать, и возникла опасная ситуация. Если функциональный блок VM перестал работать, прежде чем будет восстановлен блок PS, то выполняется переход в состояние S4.

В состоянии S3 функциональный блок VM отказал, но эта опасная ситуация не была замечена из-за отсутствия какого-либо контроля для этого функционального блока. И если функциональный блок PS опасно отказал, то выполняется переход в состояние S4.

Если функциональный блок PS перестал работать из-за необнаруживаемого опасного отказа или оба функциональных блока отказали одновременно, то выполняется переход в состояние S4 и функция безопасности более недоступна.

Состояние S4 представляет собой опасную ситуацию, где функция безопасности больше недоступна, и никакой тест больше неэффективен. Вследствие непрерывного режима работы, принятого для СЭРС (СБ), состояние S4 также является «опасным событием», так как запрос на функцию безопасности выполняется к опасно отказавшей СЭРС (СБ).

B.3.2.6 Вычисление значения *PFH*

Значения λ, ОД и β-факторов получены в B.3.2.3 и B.3.2.4.

Дополнительные определения:

r_{Rep} = 1/8 года (частота ремонтов);

T_M = 10 лет или 20 лет (заданная продолжительность работы).

Чтобы определить значение *PFH*, должны быть вычислены зависимые от времени вероятности перехода для каждого состояния модели Маркова. Начальное значение вероятности всех состояний, кроме состояния S1, равно нулю. Начальное значение вероятности состояния S1 равно единице. Вычисления должны быть выполнены на заданной продолжительности работы T_M.

$$PFH_{PS/VM} = \frac{1}{T_M}\int_0^{T_M} [((1 - ОД_{PS}) \cdot \lambda_{PSD} + \beta_{PS/VM} \cdot \min(\lambda_{PSD}, \lambda_{VMD})) \cdot p_1(t) + \lambda_{VMD} \cdot p_2(t) + \lambda_{PSD} \cdot p_3(t)]dt.$$

Результаты вычислений для различных значений параметров $\beta_{PS/VM}$, r_{Rep} и T_M представлены в таблице B.4.

Таблица B.4 — Результаты вычислений значений *PFH* для подсистемы PS/VM

$\beta_{PS/VM}$	r_{Rep}	T_M (годы)	$PFH_{PS/VM}$
2 %	1/8 ч	10	$4{,}39 \cdot 10^{-9}$/ч
2 %	1/8 ч	**20**	$5{,}03 \cdot 10^{-9}$/ч
3 %	1/8 ч	20	$6{,}25 \cdot 10^{-9}$/ч
5 %	1/8 ч	20	$8{,}70 \cdot 10^{-9}$/ч
Примечание — Значения, выделенные полужирным текстом, дают значения, отличные от предыдущей строки.			

B.3.3 Значение *PFH* функции безопасности STO для СЭРС (СБ)

Значения *PFH* в примере для r_{Rep} = 1/8 h и различных значений параметра T_M:

$PFH_{\text{STO/СЭРС (СБ)}} = PFH_{A/B} + PFH_{PS/VM}$ (значения из таблицы B.2 и таблицы B.4);

$PFH_{\text{STO/СЭРС (СБ)}}$ (T_M = 10 лет) = $(6{,}84 \cdot 10^{-10}$/год + $4{,}39 \cdot 10^{-9}$/год) = $5{,}074 \cdot 10^{-9}$/год;

$PFH_{\text{STO/СЭРС (СБ)}}$ (T_M = 20 лет) = $(7{,}38 \cdot 10^{-10}$/год + $5{,}03 \cdot 10^{-9}$/год) = $5{,}768 \cdot 10^{-9}$/год.

Приложение С
(справочное)

Доступные базы данных интенсивностей отказов

С.1 Базы данных

Представленный ниже список не является исчерпывающим, он не упорядочен и включает источники данных интенсивностей отказов для электронных и неэлектронных компонентов. Необходимо отметить, что эти источники не всегда согласуются друг с другом, и поэтому необходимо быть внимательным при применении данных.

IEC/TR 62380, Reliability data handbook — Universal model for reliability prediction of electronics components, PCBs and equipment, Union Technique de l'Electricité et de la Communication (gost.e-ecolog.ru ntical to RDF 2000/Reliability Data Handbook, UTEC 80-810.

Siemens Standard SN 29500, Failure rates of components, (parts 1 to 14); Siemens AG, CT SR SI, Otto-Hahn-Ring 6, D-81739, Munich.

Reliability Prediction of Electronic Equipment, MIL-HDBK-217E, Department of Defense, Washington DC, 1982.

Prediction Procedure for Electronic Equipment, Telcordia SR-332, Issue 01: May 2001, Reliability, (telecom-info. telcordia.com), (Bellcore TR-332, Issue 06).

EPRD (RAC-STD-6100) — Electronic Parts Reliability Data, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440 (rac.alionscience.com).

NNPRD-95 (RAC-STD-6200) — Non-electronic Parts Reliability Data, Reliability Analysis Center, 201 Mill Street, Rome, NY 13440.

HRD5, British Handbook for Reliability Data for Components used in Telecommunication Systems, British Telecom.

Chinese Military/Commercial Standard GJB/z 299B, Electronic Reliability Prediction, (gost.e-ecolog.ru).

AT&T reliability manual — Klinger, David J., Yoshinao Nakada, and Maria A. Menendez, Editors, AT&T Reliability Manual, Van Nostrand Reinhold, 1990, ISBN:0442318480.

FIDES (January, 2004) — это новое руководство по данным о надежности, разработанное консорциумом французских промышленных предприятий под управлением французского DoD DGA). FIDES доступно по запросу fides@ innovation.net.

Золотая книга IEEE (IEEE Gold book) — Золотая книга IEEE представляет рекомендуемый IEEE практический опыт для проектирования надежных, промышленных и коммерческих систем энергопитания и содержит данные по надежности оборудования, используемого в промышленных и коммерческих системах распределения энергопитания. IEEE Customer Service, 445 Hoes Lane, PO Box 1331, Piscataway, NJ, 08855-1331, U.S.A., Phone: +1 800 678 (IEEE в США и Канаде) +1 732 981 0060 (за пределами США и Канады), FAX: +1 732 981 9667 e-mail: gost.e-ecolog.ru .

IRPH ITALTEL, Руководство по прогнозу надежности является версией CNET RDF итальянских телекоммуникационных компаний. В этих стандартах используются одни и те же наборы данных, но разные процедуры и факторы. Итальянское руководство IRPH доступно по запросу от доктора. G Turconi, Direzione Qualita, Italtel Sit, CC1/2 Cascina Castelletto, 20019 Settimo Milanese Mi., Italy.

PRISM (RAC / EPRD) — Программное обеспечение PRISM доступно по нижеуказанному адресу или включено в несколько коммерчески доступных пакетов программного обеспечения надежности: The Reliability Analysis Center, 201 Mill Street, Rome, NY 13440-6916, U.S.A.

С.2 Полезные стандарты, связанные с отказами компонентов

IEC 60300-3-2, Dependability management — Part 3-2: Application guide — Collection of dependability data from the field.

IEC 60300-3-5, Dependability management — Part 3-5: Application guide — Reliability test conditions and statistical test principles.

IEC 60319, Presentation and specification of reliability data for electronic components.

IEC 60706-3, Maintainability of equipment — Part 3: Verification and collection, analysis and presentation of data.

IEC 60721-1, Classification of environmental conditions — Part 1: Environmental parameters and their severities.

IEC 61709, Electronic components — Reliability — Reference conditions for failure rates and stress models for conversion.

Приложение D
(справочное)

Список сбоев и методы их предотвращения

D.1 Общие положения

Список, представленный в таблицах D.1—D.16, содержит описание моделей сбоев, методы их предотвращения, а также обоснование методов.

В целях подтверждения соответствия следует рассматривать как постоянные, так и непостоянные сбои.

Точный момент времени, когда происходит сбой, может иметь очень большое значение. Следует провести теоретический анализ и, при необходимости, испытания для определения наихудшего варианта развития событий, например в неподвижном состоянии системы, во время запуска системы или же во время ее работы.

D.2 Замечания о методах предотвращения сбоев

D.2.1 Подтверждение соответствия методов предотвращения сбоев

Соответствие всех методов предотвращения сбоев может быть подтверждено, только если составляющие детали функционируют в пределах установленных для них номинальных параметров.

D.2.2 Рост усов олова

Если применяются процессы и изделия без примеси свинца, то возможно возникновение коротких замыканий в цепи, вызванных усами олова (см. примечание 1). Следует оценивать (см. примечание 2) и учитывать риск, связанный с усами олова при применении методов предотвращения сбоя «короткое замыкание...» для любого компонента (см. примечания 3 и 4).

Примечания

1 Рост оловянного уса представляет собой явление, которое чаще всего связано с появлением при пайке чистых ярких оловянных окончаний. Похожие на иголки выступы могут вырастать до нескольких сотен мкм и могут вызывать короткие замыкания. Преобладающая теория утверждает, что усы олова появляются в результате растущих сжимающих напряжений в процессе перехода олова из жидкого в твердое состояние.

2 Приведенные ниже издания могут быть полезны при выполнении оценки:

Test Method for Measuring Whisker Growth on Tin and Tin Alloy Surface Finishes, JESD22A121.01, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, gost.e-ecolog.ru

Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Tin Alloy Surface Finishes, JESD201, JEDEC Solid State Technology Association, 2500 Wilson Boulevard Arlington, VA 22201-3834, gost.e-ecolog.ru

3 Например, если предполагается высокий риск роста усов, то применение метода предотвращения сбоев «короткое замыкание резистора» является бесполезным, так как необходимо рассматривать короткое замыкание между контактами этого компонента.

4 Случаи возникновения усов олова на печатных платах еще не наблюдались. Монтажные соединения, как правило, состоят из меди и не имеют оловянного покрытия. Контактные площадки могут быть покрыты оловянным сплавом, но производственный процесс, похоже, не способствует росту усов.

D.2.3 Короткие замыкания деталей, смонтированных на печатные платы

Короткие замыкания деталей, смонтированных на печатную плату, можно устранить, если только метод предотвращения сбоев «короткое замыкание между двумя смежными монтажными соединениями / контактными площадками» выполнен так, как описано в таблице D.2.

D.3 Модели сбоев

Таблица D.1 — Проводники/кабели

Рассматриваемый сбой	Предотвращается	Замечание
Короткое замыкание между двумя любыми проводниками	Короткие замыкания между проводниками: - постоянным (фиксированным) подключением и защитой от внешних повреждений, например, с помощью защитного короба или оплетки для кабелей; или - изолированием многожильных кабелей; или - размещением внутри электрического корпуса (см. замечание 1); или - индивидуальным экранированием с заземлением	1 Применимо, если и проводники и корпус соответствуют требованиям МЭК 60204-1
Разрыв любого проводника	Нет	
Короткое замыкание любого проводника на оголенную проводящую деталь или на землю, или на защитную оплетку провода	Короткие замыкания между двумя проводниками, размещением внутри электрического корпуса (см. замечание 1)	

Таблица D.2 — Печатные платы/сборки

Рассматриваемый сбой	Предотвращается	Замечание
Короткое замыкание между двумя смежными монтажными соединениями/ контактными площадками	Короткие замыкания между смежными проводниками, с учетом замечаний 1—3	1 Материал печатной платы соответствует требованиям МЭК 61800-5-1. 2 Длины путей утечки и воздушные зазоры имеют размеры соответствующие, как минимум, МЭК 60664-1, со степенью загрязнения 2 / категорией перенапряжения (категорией импульсных выдерживаемых напряжений) III. Если оба соединения на плате питаются от источника безопасного или защитного сверхнизкого напряжения, то применяются степень загрязнения 2 / категория перенапряжения II при минимальном воздушном зазоре в 0,1 мм. 3 Сборка монтируется в кожух, защищающий от электропроводных загрязнителей, например в кожух со степенью защиты, как минимум, IP54, и сторона(ы) печатного проводника покрыта лаком с защитой от старения или защитным слоем, покрывающим все токоведущие пути. Примечания 1 Опыт показал, что паяльная маска является достаточным средством защиты. 2 Дополнительное покрытие защитным слоем, согласно МЭК 60664-3, может снизить размеры путей утечки и воздушных зазоров
Разрыв любого монтажного соединения	Нет	—

Таблица D.3 — Контактная колодка

Рассматриваемый сбой	Предотвращается	Замечание
Короткое замыкание между смежными клеммами	Короткое замыкание между смежными клеммами с учетом замечаний 1—2	1 Используемые клеммы и соединения соответствуют требованиям МЭК 61800-5-1. 2 Предусмотренное проектом, например, формирование термоусаживаемых трубок на местах соединений
Разрыв отдельных клемм	Нет	—

Таблица D.4 — Многоштырьковый разъем

Рассматриваемый сбой	Предотвращается	Замечание
Короткое замыкание между любыми двумя смежными контактными штырьками	Короткое замыкание между смежными контактными штырьками с учетом замечания 1. Замечание 2 также применимо, если разъем смонтирован на печатной плате	1 Используются наконечники или другие подходящие средства для многожильных проводов. Длины путей утечки и воздушные зазоры, а также все промежутки должны иметь размеры, соответствующие, как минимум, МЭК 60664-1 с категорией перенапряжения III. 2 Сборка должна быть смонтирована в кожух с минимальной степенью защиты IP54 (см. EN 60529), а сторона(ы) печатного проводника покрыта лаком с защитой от старения или защитным слоем, покрывающим все токоведущие пути в соответствии с МЭК 60664-3
Замененный или неправильно вставленный разъем, в случаях, когда это не предотвращается механическими средствами	Нет	—
Короткое замыкание любого проводника (см. замечание 3) на землю, токопроводящую часть или защитную оплетку	Нет	3 Центральная жила кабеля рассматривается как часть многоштырькового разъема
Разрыв в отдельных контактах разъема	Нет	—

Таблица D.5 — Электромеханические устройства (например, реле, контакторные реле)

Рассматриваемый сбой	Предотвращается	Замечание
Все контакты остаются в позиции «под напряжением», когда катушка обесточивается (например, по причине механического сбоя)	Нет	—
Все контакты остаются в позиции «без напряжения», когда подается питание (например, по причине механического сбоя, обрыва в катушке)	Нет	
Контакт не размыкается	Нет	
Контакт не замыкается	Нет	
Одновременное короткое замыкание между тремя клеммами переключающего контакта	Одновременное короткое замыкание может быть предотвращено, если выполнены требования замечаний 1 и 2	1 Длины путей утечки и воздушные зазоры, а также все промежутки должны иметь размеры, соответствующие, как минимум, МЭК 60664-1:1992, со степенью загрязнения 2/ категорией перенапряжения III. 2 Токопроводящие части, которые плохо закреплены, не могут обеспечить изоляцию между контактами и катушкой
Короткое замыкание между двумя парами контактов и/или между контактами и клеммой катушки	Короткое замыкание может быть предотвращено, если выполнены требования замечаний 1 и 2	
Одновременное замыкание нормально разомкнутого и нормально замкнутого контактов	Одновременное замыкание контактов может быть предотвращено, если выполнены требования замечания 3	3 Используются контакты с принудительным замыканием и размыканием (или механически связанные контакты)

Таблица D.6 — Трансформаторы

Рассматриваемый сбой	Предотвращается	Замечание
Обрыв в отдельной обмотке	Нет	–
Короткое замыкание между разными обмотками	Короткие замыкания между разными обмотками могут быть предотвращены, если выполнены требования замечаний 1 и 2	1 Должны быть соблюдены требования соответствующих частей МЭК 61558. 2 Между разными обмотками применяется двойная или усиленная изоляция или защитный экран. Применяется испытание, проведенное в соответствии с МЭК 61558, раздел 18. Подходящие тестовые значения напряжений представлены в МЭК 61558-1, таблица 8а. Короткие замыкания в катушках и обмотках следует избегать, выполняя соответствующие шаги, такие как: пропитывание катушки таким образом, чтобы заполнить все пустоты между отдельными витками и корпусом катушки и сердечником; эксплуатация проводников обмотки при значениях характеристик изоляции и температуры внутри диапазона их номинальных значений, причем находящихся достаточно далеко от этих номинальных значений. 3 В случае короткого замыкания во вторичной обмотке не должно происходить перегревания выше установленной температуры эксплуатации
Короткое замыкание в одной обмотке	Короткое замыкание в одной обмотке может быть предотвращено, если выполнено требование замечания 1	
Изменение эффективного коэффициента трансформации	Изменение эффективного коэффициента трансформации может быть предотвращено, если выполнено требование замечания 1. См. также указание в замечании 3	

Таблица D.7 — Индуктивность

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв	Нет	—
Замыкание	Короткое замыкание может быть предотвращено, если выполнены требования замечания 1	1 Катушка намотана отдельными слоями, покрытыми специальной эмалью или залитыми, с осевыми соединениями проводов и осевой конструкцией
Случайное изменение значения $0{,}5 \cdot L_N < L < L_N$ + допустимое отклонение, где L_N — это номинальное значение индуктивности (см. замечание 2)	Нет	2 В зависимости от типа конструкции, могут быть рассмотрены другие диапазоны значений индуктивности

Таблица D.8 — Резисторы

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв	Нет	—
Замыкание	Короткое замыкание может быть предотвращено, если выполнены требования замечания 1 или 2	1 Используются пленочные резисторы или в виде обмотки с защитой от разматывания проволоки в случае повреждения, с осевыми соединениями проводов, осевой конструкцией и покрыты лаком. 2 Резисторы в технологии поверхностного монтажа должны быть выполнены из тонкой металлической пленки в корпусах типа MELF, miniMELF или μMELF

Окончание таблицы D.8

Рассматриваемый сбой	Предотвращается	Замечание
Произвольное изменение значения $0,5 \cdot R_N < R < 2 \cdot R_N$, где R_N — это номинальное значение сопротивления (см. замечание 3)	Нет	3 В зависимости от типа конструкции, могут быть рассмотрены другие диапазоны значений резисторов

Таблица D.9 — Резисторные схемы

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв	Нет	—
Короткое замыкание между любыми двумя соединениями	Нет	
Короткое замыкание между любыми соединениями	Нет	
Произвольное изменение значения $0,5 \cdot R_N < R < 2 \cdot R_N$, где R_N — это номинальное значение сопротивления (см. замечание 1)	Нет	1 В зависимости от типа конструкции, могут быть рассмотрены другие диапазоны значений резисторов

Таблица D.10 — Потенциометры

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв отдельных соединений	Нет	—
Короткое замыкание между всеми соединения	Нет	
Короткое замыкание между любыми двумя соединениями	Нет	
Произвольное изменение значения $0,5 \cdot R_N < R < 2 \cdot R_N$, где R_N — это номинальное значение сопротивления (см. замечание 1)	Нет	1 В зависимости от типа конструкции, могут быть рассмотрены другие диапазоны значений потенциометров

Таблица D.11 — Конденсаторы

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв	Нет	—
Замыкание	Нет	
Произвольное изменение значения $0,5 \cdot C_N < C < C_N$ + допустимое отклонение, где C_N — это номинальное значение емкости (см. замечание 1)	Нет	1 В зависимости от типа конструкции, могут быть рассмотрены другие диапазоны значений емкостей
Изменение значения tg δ	Нет	—

Таблица D.12 — Дискретные полупроводниковые приборы (например, диоды, диоды Зенера, транзисторы, симисторы, запираемые тиристоры, биполярные транзисторы с изолированным затвором, регуляторы напряжения, кварцевые кристаллы, фототранзисторы, светоизлучающие диоды)

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв любого соединения	Нет	—
Короткое замыкание между любыми двумя соединениями	Нет	
Короткое замыкание между всеми соединениями	Нет	
Изменение характеристик	Нет	
Взрыв корпуса устройства	Может быть предотвращено, если выполнены требования замечания 1	1 Мощность короткого замыкания шины питания ограничена предельной прочностью корпуса устройства

Таблица D.13 — Оптроны

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв отдельного соединения	Нет	—
Короткое замыкание между любыми двумя входными соединениями	Нет	
Короткое замыкание между любыми двумя выходными соединениями	Нет	
Короткое замыкание между любыми двумя соединениями входа и выхода	Короткое замыкание между входом и выходом может быть предотвращено, если выполнены требования замечаний 1 и 2	1 Фотоэлемент строится в соответствии с категорией перенапряжения III согласно МЭК 61800-5-1 и МЭК 60664-1:1992, таблица 1. Если используется источник питания безопасного или защитного сверхнизкого напряжения, то применяется степень загрязнения 2/ категория перенапряжения II. 2 Принимаются меры для обеспечения защиты от избыточного повышения температуры изоляционного материала в результате внутреннего отказа

Таблица D.14 — Непрограммируемые интегральные схемы (ИС)

Рассматриваемый сбой	Предотвращается	Замечание
Разрыв каждого отдельного соединения	Нет	—
Короткое замыкание между любыми двумя соединениями	Нет	
Константный сбой (т. е. короткое замыкание, приводящее к 1 и 0 на гальванически развязанном входе или отключенном выходе). Сигнал статического «0» и «1» появляется на всех входах и выходах — либо отдельно на каждом, либо одновременно	Нет	
Паразитные колебания на выходах	Нет	
Изменение значений (например, входного/выходного напряжения аналоговых устройств)	Нет	
Примечание — В настоящем стандарте ИС с менее чем 1000 элементами, и/или с менее чем 24 выводами, операционные усилители, регистры сдвига, гибридные модули считаются несложными. Это определение субъективно.		

Таблица D.15 — Программируемые и/или сложные интегральные схемы

Рассматриваемый сбой	Предотвращается	Замечание
Сбои всех или части функций	Нет	—
Разрыв каждого отдельного соединения	Нет	
Константный сбой (т. е. короткое замыкание, приводящее к 1 и 0 на гальванически развязанном входе или отключенном выходе). Сигнал статического «0» и «1» появляется на всех входах и выходах — либо отдельно на каждом, либо одновременно	Нет	
Паразитные колебания на выходах	Нет	
Изменение значений (например, входного/выходного напряжения аналоговых устройств)	Нет	
Не обнаруживаемые сбои в аппаратных средствах, которые остаются незамеченными из-за сложности интегральной схемы	Нет	
Примечание — В настоящем стандарте ИС считается сложной, если она состоит из более чем 1000 элементов и/или имеет не менее чем 24 вывода. Это определение субъективно. В результате анализа должны быть идентифицированы дополнительные сбои, которые следует учитывать, если они влияют на выполнение функции безопасности.		

Таблица D.16 — Датчики обратной связи движения и положения

Рассматриваемый сбой	Предотвращается	Замечание
Общие		
Короткое замыкание между любыми двумя проводниками соединительного кабеля	Применима таблица D.1	—
Разрыв любого проводника соединительного кабеля	Нет	
Входное или выходное константное значение «0» или «1» на одном или на нескольких входах/выходах одновременно	Нет	
Разрыв или состояние высокого сопротивления на одном или на нескольких входах/выходах одновременно	Нет	
Увеличение или уменьшение амплитуды выходного сигнала	Нет	
Колебания на одном или нескольких выходах[a)]	Нет	Считается, что колебания на нескольких выходах выполняются в фазе
Изменение сдвига фаз между выходными сигналами[a)]	Нет	Например, из-за загрязнения диска устройства кодирования

Продолжение таблицы D.16

Рассматриваемый сбой	Предотвращается	Замечание
Общие		
Потеря крепления во время неподвижного состояния: - между корпусом датчика и рамой двигателя; - между валом датчика и валом двигателя	Подготовка FMEA и доказательство долгосрочной стойкости механических креплений	Выходной сигнал равносилен неподвижному состоянию. Если заявлена способность предотвратить сбой, то это значит, что монтаж корпуса датчика на корпус двигателя и вала датчика на вал двигателя, как правило, может выдержать превышение допустимого напряжения приблизительно в 20 раз. Также должна быть предоставлена специальная информация о техническом обслуживании
Потеря или ослабление крепления во время движения: - между корпусом датчика и рамой двигателя; - между валом датчика и валом двигателя	Подготовка FMEA и доказательство долгосрочной стойкости механических креплений	Возможные эффекты: - статическое смещение вала датчика; - динамическое сползание вала датчика; - неправильный выходной сигнал / сигнал нулевой скорости. Если заявлена способность предотвратить сбой, то это значит, что монтаж корпуса датчика на корпус двигателя и вала датчика на вал двигателя, как правило, может выдержать превышение допустимого напряжения приблизительно в 20 раз. Также должна быть предоставлена специальная информация о техническом обслуживании
Ослабление твердой меры[a)] (например, диска оптического датчика положения)	Нет	Выходной сигнал указывает на неправильное положение
Диод не светится	Нет	—
Дополнительно для датчиков вращения с синусоидальными и косинусоидальными выходными сигналами, генерация аналоговых сигналов		
Статическое значение входного и выходного сигнала, для одного отдельного или для нескольких сигналов, переменная составляющая в напряжении источника питания	Нет	—
Изменение формы сигнала	Нет	Например, отсутствие синусоидального и косинусоидального сигнала, смещение сигнала
Замена синусоидального и косинусоидального выходного сигнала	Предотвращение сбоя возможно, если для выбора выходного сигнала из нескольких источников не применяются электронные компоненты	—

Продолжение таблицы D.16

Рассматриваемый сбой	Предотвращается	Замечание
Дополнительно для инкрементного датчика вращения с прямоугольными выходными сигналами		
Колебания на выходе	Нет	—
Остановки выходного сигнала	Нет	Например, из-за царапин на диске
Нулевой импульс не срабатывает, слишком короткий, слишком длинный или повторный	Нет	Например, из-за механических повреждений
Дополнительно для устройства кодирования с инкрементным и абсолютным сигналами		
Неправильная смена положения при одновременно поданных инкрементном и абсолютном сигналах	Сбой может быть предотвращен, если инкрементные и абсолютные данные будут генерироваться независимо друг от друга	Например, применимо к синусоидальному или косинусоидальному датчику положения, обладающему дополнительными выходами для абсолютного положения и/или коммуникаций
Дополнительно для датчиков вращения с интерфейсом, основанным на процессоре		
Сбои коммуникаций: - повторение; - потеря; - вставка; - неправильный порядок; - неверные данные; - задержка	Нет	Равнозначно модели сбоев для коммуникационных шин
Дополнительно для датчиков вращения, многооборотность		
Неправильное число оборотов	Нет	Может не влиять на одиночные сигналы поворота
Дополнительно для датчиков вращения с синтезированными выходными сигналами		
Неправильный выходной сигнал по причине отказа синтезирующего устройства	Нет	—
Дополнительно для датчиков вращения, в которых значение положения формируется счетчиком		
Неправильное положение из-за ошибки подсчета	Нет	
Дополнительно для линейных датчиков		
Разбито крепление датчика чтения	Подготовка FMEA и доказательство долгосрочной стойкости механических креплений	Если заявлена способность предотвратить сбой, то это значит, что конструкция крепления датчика может выдерживать перенапряжения. Также должна быть предоставлена специальная информация о техническом обслуживании
Статическое смещение постоянной меры (например, полосы для оптического датчика положения)	Нет	—

Окончание таблицы D.16

Рассматриваемый сбой	Предотвращается	Замечание
Повреждение постоянной меры (например, полосы для оптического датчика положения)	Нет	Форма импульсов изменяется, импульсы вызывают отказ инкрементных датчиков
Дополнительно для кругового датчика положения с обработкой сигнала / генератором опорного напряжения		
Перекрестные помехи генератора опорного напряжения	Нет	—
- Сбои центрального датчика времени; - На аналогово-цифровом преобразователе не начинается преобразование; - Неправильная синхронизация Выборки и Записи	Нет	
Аналогово-цифровой преобразователь генерирует ошибочные значения	Нет	
Аналогово-цифровой преобразователь не генерирует значения	Нет	Например, из-за перемодуляции, вызванной слишком высоким опорным напряжением или электромагнитным воздействием
Нет частоты на генераторе опорного напряжения	Нет	—
Неправильная частота на генераторе опорного напряжения	Нет	
От генератора опорного напряжения не поступает периодический сигнал	Нет	
Ошибка в коэффициенте усиления или колебания при обработке сигналов (Ref, Sin, Cos)	Нет	
Воздействие магнитного поля на место установки	Надлежащее экранирование в месте установки	Например, из-за электромагнитного поля электромагнитного тормоза
[a] Нет в круговом датчике положения.		
Примечание — Настоящая таблица была сформирована, предполагая использование оптических датчиков. Если используются другие датчики (например, индуктивные), то применимы соответствующие сбои.		

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60204-1	IDT	ГОСТ Р МЭК 60204-1—2007 «Безопасность машин. Электрооборудование машин и механизмов. Часть 1. Общие требования»
МЭК 61508 (все части)	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Части 1– 7»
МЭК 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
МЭК 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
МЭК 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
МЭК 61508-5:2010	IDT	ГОСТ Р МЭК 61508-5—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
МЭК 61508-6:2010	IDT	ГОСТ Р МЭК 61508-6— 2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3
МЭК 61508-7:2010	IDT	ГОСТ Р МЭК 61508-7— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
МЭК 61800-1	IDT	ГОСТ Р МЭК 61800-1—2012 «Системы силовых электроприводов с регулируемой скоростью. Часть 1. Общие требования. Номинальные технические характеристики низковольтных систем электроприводов постоянного тока с регулируемой скоростью»
МЭК 61800-2	IDT	ГОСТ Р МЭК 61800-2—2012 «Системы силовых электроприводов с регулируемой скоростью. Часть 2. Общие требования. Номинальные технические характеристики низковольтных систем силовых электроприводов переменного тока с регулируемой частотой»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 61800-3	IDT	ГОСТ Р 51524—2012 (МЭК 61800-3:2012) «Совместимость технических средств электромагнитная. Системы электрического привода с регулируемой скоростью. Часть 3. Требования ЭМС и специальные методы испытаний»
МЭК 61800-4	IDT	ГОСТ Р МЭК 61800-4—2012 «Системы силовых электроприводов с регулируемой скоростью. Часть 4. Общие требования. Номинальные технические характеристики систем силовых приводов переменного тока свыше 1000 В и не более 35 кВ»
МЭК 61800-5-1	—	*
МЭК 62280	—	*

*Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] IEC 60050-191:1990, International Electrotechnical Vocabulary — Chapter 191: Dependability and quality of service

[2] IEC 60300-3-1, Application guide — Analysis techniques for dependability: Guide on methodology

[3] IEC 60664-1:1992, Insulation coordination for equipment within low-voltage systems — Part 1:Principles, requirements and tests

[4] IEC 60664-3, Insulation coordination for equipment within low-voltage systems — Part 3: Use of coating, potting or moulding for protection against pollution

[5] IEC 61025, Fault tree analysis (FTA)

[6] IEC 61078, Analysis techniques for dependability — Reliability block diagram and boolean methods

[7] IEC 61165, Application of Markov techniques

[8] IEC 61508-4:1998, Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 4: Definitions and abbreviations

[9] IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector

[10] IEC 61511-1, Functional safety — Safety instrumented systems for the process industry sector Part 1: Framework, definitions, system, hardware and software requirements

[11] IEC 61513, Nuclear power plants — Instrumentation and control for systems important to safety — General requirements for systems

[12] IEC 61558 (all parts), Safety of power transformers, power supplies, reactors and similar products

[13] IEC 61558-1:2005, Safety of power transformers, power supplies, reactors and similar products — Part 1: General requirements and tests

[14] IEC 62061, Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

[15] IEC 62280-1, Railway applications — Communication, signalling and processing systems — Part 1: Safety-related communication in closed transmission systems

[16] IEC 62280-2, Railway applications — Communication, signalling and processing systems — Part 2: Safety-related communication in open transmission systems

[17] ISO 13849-1, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

[18] ISO 13849-2, Safety of machinery — Safety-related parts of control systems — Part 2: Validation

[19] ENV 50129, Railway applications — Safety-related electronic systems for signalling

[20] ISO/IEC Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards

УДК 62-783:614.8:331.454:006.354

ОКС 13.110
29.200

Ключевые слова: силовые электроприводы, системы силовых электроприводов, силовые электроприводы с регулируемой скоростью, функциональная безопасность; требования

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *К.Л. Чубанова*

Сдано в набор 21.04.2016. Подписано в печать 20.05.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 5,21. Тираж 32 экз. Зак. 1312.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru