ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61511-1— 2018

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 1

Термины, определения и технические требования

(IEC 61511-1:2016 + Corr:2016, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2018 г. № 466-ст

Настоящий стандарт идентичен международному стандарту МЭК 61511-1:2016 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования», включая техническую поправку (Поправка 1:2016) («Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements», IDT).

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

4 ВЗАМЕН ГОСТ Р МЭК 61511-1—2011

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартинформ, оформление, 2018

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 4
3 Термины, определения и сокращения . . . 4
3.1 Термины . . . 4
3.2 Термины и определения . . . 4
3.3 Сокращения . . . 20
4 Соответствие настоящему стандарту . . . 21
5 Управление функциональной безопасностью . . . 21
5.1 Цель . . . 21
5.2 Требования . . . 21
6 Требования к жизненному циклу системы безопасности . . . 26
6.1 Цели . . . 26
6.2 Требования . . . 26
6.3 Требования к жизненному циклу прикладной программы приборной системы безопасности . . . 27
7 Верификация . . . 31
7.1 Цель . . . 31
7.2 Требования . . . 31
8 Анализ опасностей и рисков процесса . . . 32
8.1 Цели . . . 32
8.2 Требования . . . 33
9 Распределение функций безопасности по слоям защиты . . . 34
9.1 Цели . . . 34
9.2 Требования к процессу распределения . . . 34
9.3 Требования к основной системе управления процессом как к слою защиты . . . 37
9.4 Требования к предотвращению отказов по общей причине, отказов общего типа и зависимых отказов . . . 38
10 Спецификация требований к безопасности приборной системы безопасности . . . 38
10.1 Цель . . . 38
10.2 Основные требования . . . 38
10.3 Требования к безопасности приборной системы безопасности . . . 38
11 Проектирование и разработка приборной системы безопасности . . . 41
11.1 Цель . . . 41
11.2 Основные требования . . . 41
11.3 Требования к поведению системы при обнаружении отказа . . . 42
11.4 Отказоустойчивость аппаратных средств . . . 43
11.5 Требования к выбору устройств . . . 44
11.6 Внешние устройства . . . 47
11.7 Интерфейсы . . . 47
11.8 Требования к проектированию обслуживания или испытаний . . . 48
11.9 Количественная оценка случайного отказа . . . 49
12 Требования к разработке прикладной программы приборной системы безопасности . . . 51
12.1 Цель . . . 51
12.2 Общие требования . . . 51
12.3 Проектирование прикладных программ . . . 52

12.4 Реализация прикладной программы . . . 53
12.5 Требования к верификации прикладной программы (проверка и тестирование) . . . 54
12.6 Требования к методологии и инструментальным средствам разработки прикладной программы . . . 54
13 Заводские приемочные испытания . . . 55
13.1 Цель . . . 55
13.2 Рекомендации . . . 55
14 Установка и ввод в действие приборной системы безопасности . . . 56
14.1 Цели . . . 56
14.2 Требования . . . 56
15 Подтверждение соответствия безопасности приборной системы безопасности . . . 57
15.1 Цель . . . 57
15.2 Требования . . . 57
16 Эксплуатация и техническое обслуживание приборной системы безопасности . . . 60
16.1 Цели . . . 60
16.2 Требования . . . 60
16.3 Контрольная проверка и осмотр . . . 62
17 Модификация приборной системы безопасности . . . 63
17.1 Цели . . . 63
17.2 Требования . . . 63
18 Снятие с эксплуатации приборной системы безопасности . . . 64
18.1 Цели . . . 64
18.2 Требования . . . 64
19 Требования к информации и документации . . . 64
19.1 Цели . . . 64
19.2 Требования . . . 65
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам . . . 66

Введение

Приборные системы безопасности (ПСБ) уже в течение многих лет используют для выполнения функций безопасности (ФБ ПСБ) в промышленных процессах. Для эффективного применения приборных систем безопасности при выполнении ФБ ПСБ необходимо, чтобы они соответствовали определенному минимальному уровню стандартизации.

Область применения комплекса стандартов МЭК 61511 — ПСБ, применяемые в промышленных процессах. Комплекс стандартов МЭК 61511 также рассматривает проведение анализа опасности и риска процесса для обеспечения формирования спецификации приборных систем безопасности. Вклад других систем безопасности учитывается только по отношению к требованиям к эффективности приборных систем безопасности. ПСБ включает все устройства, необходимые для выполнения каждой ФБ ПСБ, — от датчика(ов) до исполнительного(ых) элемента(ов).

В основе комплекса стандартов МЭК 61511 лежат две фундаментальные концепции, необходимые для ее применения: концепция жизненного цикла системы безопасности и концепция уровней полноты безопасности (УПБ).

Комплекс стандартов МЭК 61511 рассматривает ПСБ, использующие электрические/электронные/программируемые электронные технологии. Если для логических устройств используют другие принципы действия, то следует применять основные положения МЭК 61511, чтобы гарантировать выполнение требований к функциональной безопасности. Комплекс стандартов МЭК 61511 также рассматривает датчики и исполнительные элементы ПСБ независимо от принципа их действия. Комплекс стандартов МЭК 61511 является конкретизацией для промышленных процессов общего подхода к вопросам обеспечения безопасности, представленного в комплексе стандартов МЭК 61508.

Комплекс стандартов МЭК 61508 устанавливает подход, минимизирующий уровень стандартизации действий на всех стадиях жизненного цикла ПСБ. Этот подход был принят в целях реализации рациональной и последовательной технической политики.

В большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. Но при необходимости процесс может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск. Системы защиты могут быть основаны на применении различных технологий: химических, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных. Для облегчения применения такого подхода настоящий стандарт:

- устанавливает, чтобы выполнялся анализ опасностей и рисков для определения общих требований к безопасности;
- устанавливает, чтобы выполнялось распределение требований к безопасности в (по) приборной(ым) системе(ам) безопасности;
- реализует подход, который применим ко всем приборным мерам обеспечения функциональной безопасности;
- подробно рассматривает применение определенных действий по управлению безопасностью, которые могут быть применены ко всем методам обеспечения функциональной безопасности.

Комплекс стандартов МЭК 61511 по ПСБ для промышленных процессов:

- охватывает все стадии жизненного цикла ПСБ — от разработки первоначальной концепции, проектирования, внедрения, эксплуатации и технического обслуживания вплоть до утилизации;
- дает возможность, чтобы существующие или новые стандарты в разных странах, регламентирующие конкретные промышленные процессы, были гармонизированы с комплексом стандартов МЭК 61511.

Комплекс стандартов МЭК 61511 призван привести к высокому уровню согласованности (например, основных принципов, терминологии, информации) в рамках конкретных промышленных процессов. Это должно принести преимущества как в плане безопасности, так и в плане экономики. Ниже, на рисунке 1, показана общая структура комплекса стандартов МЭК 61511.

В пределах своей юрисдикции соответствующие регулирующие органы (например, национальные, федеральные, штата, провинции, округа, города) могут устанавливать такие правила к процессу проектирования системы безопасности, к процессу управления безопасностью или другие правила, которые могут превалировать над требованиями, определенными в комплексе стандартов МЭК 61511.

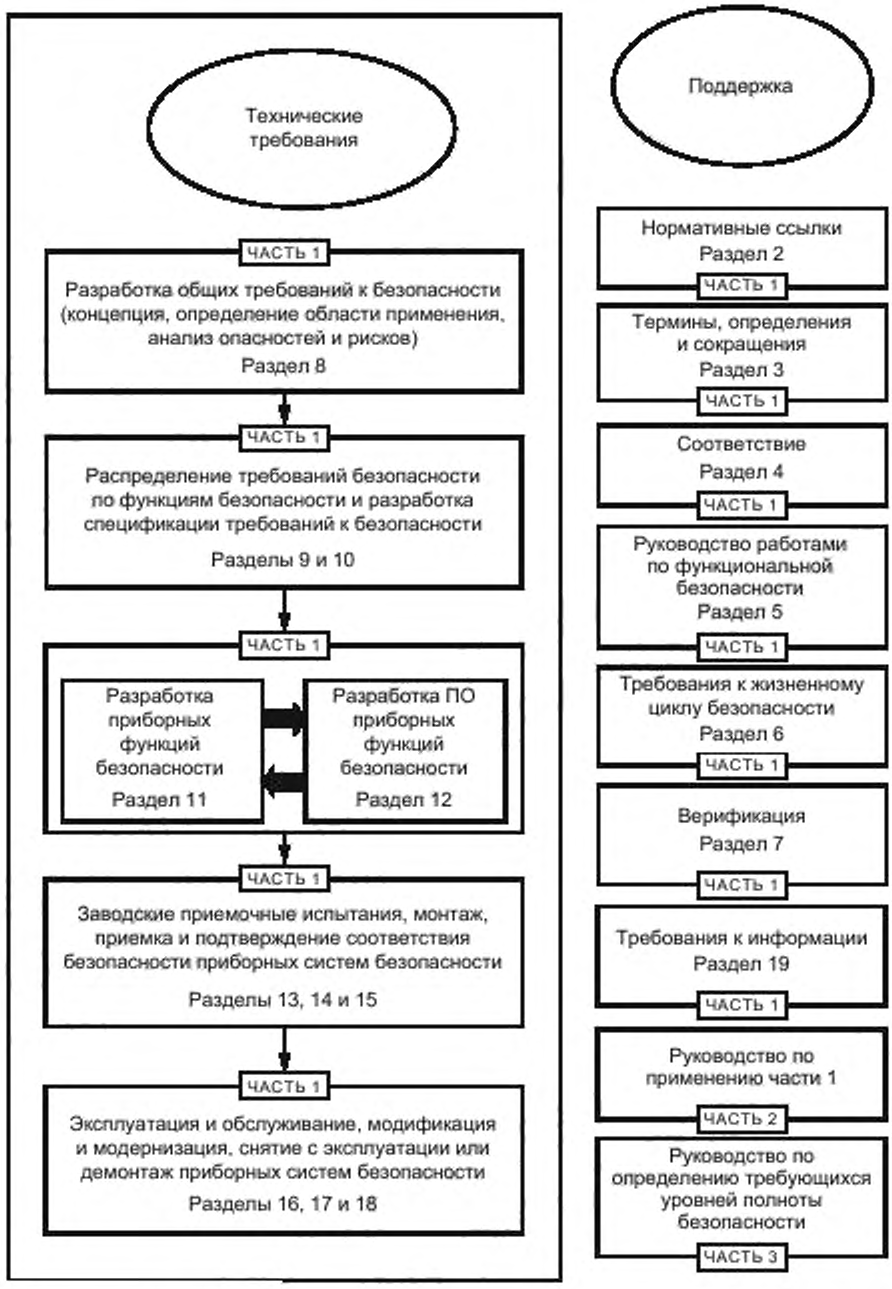


Рисунок 1 — Общая структура комплекса стандартов МЭК 61511

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 1

Термины, определения и технические требования

Functional safety. Safety instrumented systems for the process industry sector.
Part 1. Terms, definitions and technical requirements

Дата введения — 2019—07—01

1 Область применения

Настоящий стандарт определяет требования к спецификации, проектированию, монтажу, эксплуатации и техническому обслуживанию приборной системы безопасности (ПСБ) так, чтобы она могла надежно переводить и удерживать процесс в безопасном состоянии. Настоящий стандарт разработан для реализации МЭК 61508:2010 в области промышленных процессов.

В частности, настоящий стандарт:

a) определяет требования к достижению функциональной безопасности, но не определяет, кто отвечает за выполнение этих требований (проектировщики, поставщики, собственник, эксплуатирующая организация, подрядчик); такая ответственность будет возложена на различных участников согласно планированию безопасности, планированию и управлению проектом и национальному законодательству;

b) распространяется на случаи, когда устройства, удовлетворяющие требованиям МЭК 61508:2010 или настоящего стандарта, подраздел 11.5, применяются в общей системе управления промышленным процессом; но не распространяется на изготовителей, желающих заявить, что их устройства подходят для использования в ПСБ для промышленных процессов (см. МЭК 61508-2:2010 и МЭК 61508-3:2010);

c) определяет связь между МЭК 61511 и МЭК 61508 (см. рисунки 2 и 3);

d) применяется в тех случаях, когда прикладные программы разработаны для систем, использующих языки с ограниченной изменчивостью, или устройств, использующих фиксированные языки программирования, но не применяется к изготовителям, разработчикам ПСБ, интеграторам и пользователям, разрабатывающим встроенное (системное) программное обеспечение либо использующим языки с полной изменчивостью (см. МЭК 61508-3:2010);

e) распространяется на широкий набор промышленных процессов в различных отраслях промышленности, включая химическую, нефтеперерабатывающую, нефтегазодобывающую, целлюлозно-бумажное производство, фармацевтику, пищевые продукты и неядерную энергетику.

Примечание — Для некоторых промышленных процессов могут быть установлены дополнительные обязательные требования;

f) определяет отношение между ФБ ПСБ и другими функциями (см. рисунок 4);

g) определяет функциональные требования и требования к полноте безопасности для ФБ ПСБ, учитывая снижение риска, достигаемое другими методами;

h) определяет требования жизненного цикла для архитектуры системы и конфигурации ее технических средств, прикладного программирования и системной интеграции;

Издание официальное

i) определяет требования к прикладному программированию, предъявляемые к пользователям и интеграторам ПСБ;

j) применяется, когда функциональная безопасность (ФБ) обеспечивается с помощью одной или более ФБ ПСБ для защиты персонала, защиты населения или защиты окружающей среды;

k) может быть применен в случаях, не связанных с безопасностью, таких как защита имущества;

l) определяет требования для реализации ФБ ПСБ как части общей системы для достижения функциональной безопасности;

m) использует жизненный цикл ПСБ (см. рисунок 7) и определяет список действий, которые необходимы для определения функциональных требований и требований к полноте безопасности для ПСБ;

n) специфицирует выполнение анализа опасности и риска для каждой ФБ ПСБ для определения требований функциональной безопасности и уровня полноты безопасности (УПБ).

Примечание — На рисунке 9 представлен краткий обзор методов снижения риска;

o) устанавливает количественные целевые значения для средней вероятности отказа по запросу (в режиме работы по запросу) и средней частоты опасных отказов (в режиме по запросу или непрерывном режиме) для каждого УПБ;

p) определяет минимальные требования для отказоустойчивости аппаратных средств (ОАС);

q) определяет меры и методы, необходимые для достижения установленного УПБ;

r) определяет максимальное значение уровня функциональной безопасности (УПБ 4), который может быть достигнут для ФБ ПСБ, реализуемых в соответствии с МЭК 61511;

s) определяет минимальное значение уровня функциональной безопасности (УПБ 1), ниже которого настоящий стандарт не применяется;

t) является основой для установления УПБ, но не определяет УПБ для конкретных приложений (которые должны быть установлены на основании знаний о каждом конкретном приложении и общем целевом значении снижения риска);

u) определяет требования для всех элементов ПСБ — от датчика до исполнительного(ых) элемента(ов);

v) определяет информацию, необходимую в течение жизненного цикла ПСБ;

w) определяет, как проект ПСБ учитывает человеческий фактор;

x) не содержит каких-либо прямых требований к конкретному оператору или специалисту по обслуживанию.



Рисунок 2 — Связь между МЭК 61511 и МЭК 61508

Примечание — МЭК 61508 также используется проектировщиками, специалистами по интеграции и пользователями ПСБ там, где МЭК 61511 дает на это указания.



Рисунок 3 — Детализированная связь между МЭК 61511 и МЭК 61508

Примечание — Пункт 4.7.2.2 настоящего стандарта и пункт 4.7.2.2 МЭК 61511-2 содержат руководство по интеграции подсистем, соответствующих другим стандартам (например, для машинного оборудования, печи и т. п.).

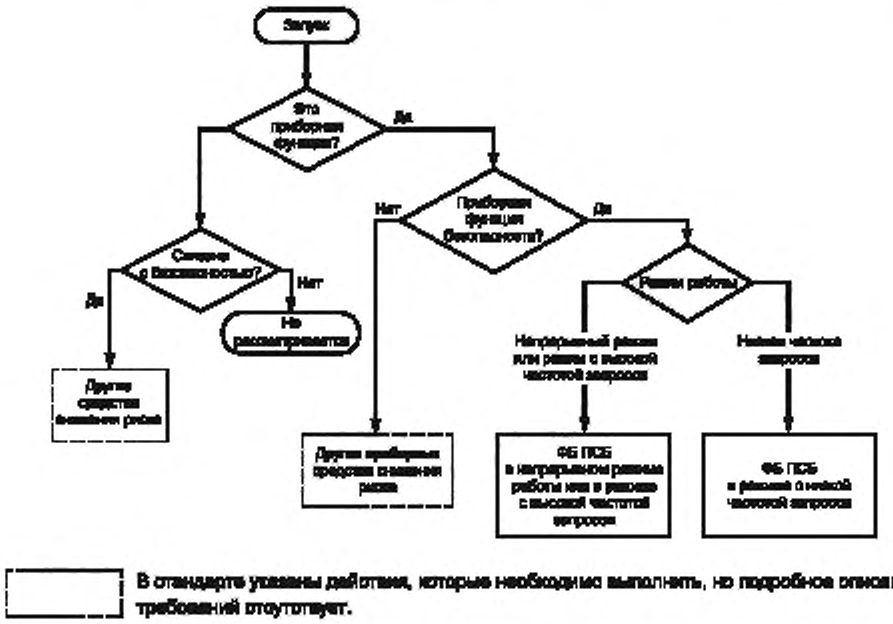


Рисунок 4 — Связь между приборными функциями безопасности и другими функциями

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты [для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения)]:

IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General Requirements (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 1. Общие требования)

IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 2. Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью)

IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 3. Требования к программному обеспечению)

3 Термины, определения и сокращения

3.1 Термины

Термины перечислены в алфавитном порядке в 3.2.

3.2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

В некоторых случаях эти определения отличаются от определений тех же самых терминов в МЭК 61508-4:2010. В некоторых случаях это связано с терминологией, используемой в промышленных процессах. В других случаях эти определения могут соответствовать другим значимыми ссылкам (например, МЭК 60050 Международный электротехнический словарь, ИСО/МЭК Руководство 51:2013). Тем не менее, если не указано иное, эти определения и определения тех же терминов в МЭК 61508-4:2010 с технической точки зрения не различаются.

3.2.1 **архитектура, конфигурация** (architecture, configuration): Определенная конфигурация компонентов аппаратных средств и программного обеспечения в системе.

Примечание — В комплексе стандартов МЭК 61511 это может означать, например, организацию подсистем ПСБ, внутреннюю структуру подсистемы ПСБ или внутреннюю структуру прикладных программ ПСБ.

3.2.2 **защита имущества** (asset protection): Функция, предусмотренная системой и спроектированная в целях предотвращения имущественных потерь или нанесения вреда имуществу.

3.2.3 **основная система управления процессом;** ОСУП (basic process control system; BPCS): Система, которая реагирует на входные сигналы, поступающие от процесса, от его соответствующего оборудования, от программируемых систем и/или от оператора и вырабатывает выходные сигналы, заставляющие процесс и его соответствующее оборудование действовать желательным образом, но которая не выполняет никаких ФБ ПСБ.

Примечания

1 ОСУП включает все устройства, необходимые для обеспечения выполнения процесса желательным образом.

2 ОСУП, как правило, может реализовывать различные функциональные слои защиты, такие как функции управления процессом, мониторинг, аварийная сигнализация или другие не связанные с ПСБ функциональные слои защиты.

3.2.4 **байпас** (bypass): Действие или средство для предотвращения выполнения функционала ПСБ целиком или частично.

Примечания

1 Примеры байпасов включают:

- входной сигнал, поступивший от системы аварийного отключения, заблокирован, но оператор все равно получает входные параметры и аварийный сигнал;

- выходной сигнал из системы аварийного отключения в исполнительный элемент удерживается в нормальном состоянии, предотвращая работу исполнительного элемента;
- физическую линию байпаса, которая устанавливается в обход исполнительного элемента;
- заранее выбранное состояние входа (например, выключенный/включенный вход) или набор таких состояний принудительно устанавливается с помощью инструментального приложения (например, в прикладной программе).

2 В качестве синонимов байпаса также используются другие термины, такие как отмена, обход, отключение, принуждение или запрещение или подавление.

3.2.5 **канал** (channel): Устройство или группа устройств, независимо выполняющее(ая) определенную функцию.

Примечания

1 Устройствами канала могут быть устройства ввода/вывода, логические решающие устройства, датчики, исполнительные устройства.

2 Дуальная (или двухканальная) конфигурация — это такая конфигурация, при которой два канала независимо выполняют одну и ту же функцию. Эти каналы могут быть идентичными или разными.

3 Термин может быть применен для описания как полной системы, так и ее части (например, для описания датчиков или исполнительных элементов).

4 Канал описывает архитектурные особенности аппаратных средств, часто используемые для выполнения требований отказоустойчивости.

3.2.6 **общая причина** (common cause)

3.2.6.1 **отказы по общей причине** (common cause failure): Одновременные отказы разных устройств, вызванные одним событием, в котором эти отказы не являются последствиями друг друга.

Примечания

1 Все отказы по общей причине не обязательно происходят одновременно, что позволяет успеть обнаружить возникновение общей причины перед тем, как произойдет сам отказ ФБ ПСБ.

2 Отказы по общей причине могут также привести к отказам общего типа.

3 Потенциальные отказы по общей причине снижают эффективность избыточности системы или ее отказоустойчивость (например, повышается вероятность отказа двух или нескольких каналов в многоканальной системе).

4 Отказы по общей причине являются зависимыми отказами. Они могут быть вызваны внешними событиями (например, температурой, влажностью, электрическим перенапряжением, пожаром или коррозией), систематическим сбоем (например, ошибкой в проекте, ошибками монтажа или установки, серьезными программными ошибками), ошибкой человека (например, некорректным использованием) и т. п.

5 В более широком смысле, согласно определению настоящего пункта, отказ по общей причине (в форме единичного отказа) является отказом, принадлежащим набору одновременных отказов (в форме множественного отказа).

3.2.6.2 **отказы общего типа** (common mode failures): Одновременные отказы разных устройств, которые можно охарактеризовать одинаковым типом отказа (т. е. идентичные сбои).

Примечания

1 Отказы общего типа могут иметь разные причины.

2 Отказы общего типа могут также быть результатом отказов по общей причине (см. 3.2.6.1).

3 Потенциальные отказы общего типа снижают эффективность избыточности системы или ее отказоустойчивость (например, два или несколько каналов отказывают одинаковым образом, приводя к одинаковым ошибочным результатам).

4 В более широком смысле, согласно определению настоящего пункта, отказ общего типа (в форме единичного отказа) является отказом, принадлежащим набору одновременных отказов (в форме множественного отказа).

3.2.7 **компенсирующие меры** (compensating measures): Временная реализация запланированных или документально оформленных методов управления рисками во время обслуживания или выполнения процесса, когда известно, что рабочие характеристики ПСБ ухудшаются.

3.2.8 **компонент** (component): Одна из частей системы, подсистемы ПСБ или устройства, выполняющая определенную функцию.

Примечание — Компонент может также включать программное обеспечение.

3.2.9 **управление конфигурацией** (configuration management): Порядок определения компонентов и их организации в развивающейся системе, обеспечивающий управление изменениями в этих компонентах, а также поддержку целостности системы и прослеживаемость любых изменений на протяжении всего ее жизненного цикла.

3.2.9.1 **консервативный подход** (conservative approach): Осторожный подход к выполнению анализа и вычислений.

Примечание — В области обеспечения безопасности, когда требуется выполнить анализ, определить допущения или провести вычисления (для моделей, входных данных, машинных расчетов и т. п.), такой подход может быть выбран для получения пессимистических результатов.

3.2.10 **система управления** (control system): Система, которая реагирует на входные сигналы, поступающие от процесса и/или от оператора, и вырабатывает выходные сигналы, формирующие процесс заданным способом.

Примечание — Система управления включает в себя датчики и исполнительные устройства и может быть либо ОСУП, либо ПСБ, либо их комбинацией.

3.2.11 **опасный отказ** (dangerous failure): Отказ, препятствующий или блокирующий выполнение заданного действия по обеспечению безопасности.

Примечания

1 Отказ является «опасным» только в отношении заданной ФБ ПСБ.

2 Если реализована отказоустойчивость, то опасный отказ может привести:

- к деградации ФБ ПСБ, в которой действие по обеспечению безопасности выполняется, но с более высоким значением PFD (в режиме по запросу) или с более высокой вероятностью возникновения опасного события (в режиме с высокой частотой запросов или в непрерывном режиме), либо
- к отключению ФБ ПСБ, в которой действие по обеспечению безопасности полностью блокируется (в режиме по запросу) или произошло опасное событие (в режиме с высокой частотой запросов или в непрерывном режиме).

3 Если не реализовано никакой отказоустойчивости, то все опасные отказы ведут к отключению ФБ ПСБ.

3.2.12 **зависимый отказ** (dependent failure): Отказ, вероятность которого не может быть выражена в виде простого произведения безусловных вероятностей отдельных событий, являющихся причиной отказа.

Примечания

1 Два события A и B будут зависимы только тогда, когда вероятность возникновения A и B, $P(A \text{ и } B)$ больше, чем $P(A) \cdot P(B)$.

2 В 9.4.2 и МЭК 61511-3:2016, приложение J, рассматриваются зависимые отказы между слоями защиты.

3 Зависимый отказ включает в себя отказ по общей причине.

3.2.13 **обнаруженный, раскрытый, наблюдаемый** (detected, revealed, overt): Виды отказов, связанные с отказами или сбоями аппаратных средств или программного обеспечения, которые не являются скрытыми, так как они заявляют о себе или обнаруживаются в ходе нормального функционирования или с помощью специальных методов обнаружения.

Примечания

1 Имеются определенные различия в использовании терминов:

- «наблюдаемый» применяется к отказам или сбоям, которые заявляют о себе, как только они случаются (например, через изменение состояния). Устранение последствий таких отказов можно начать, как только они произойдут;
- «обнаруженный» применяется к отказам или сбоям, которые не заявляют о себе на момент, когда они случаются, и остаются скрытыми до обнаружения какими-либо мерами (например, диагностическими испытаниями, контрольными проверками, вмешательством оператора, такими как физический осмотр или ручные испытания). Исправление таких отказов можно начать только после их раскрытия. О конкретном использовании данного термина в МЭК 61511 см. в примечании 2;
- «раскрытый» применяется к отказам или сбоям, которые становятся очевидными ввиду их наблюдаемости или в результате их обнаружения.

2 В МЭК 61511, за исключением случаев, когда контекст предполагает иное значение, термин «опасные обнаруженные отказы/сбои» связан с опасными отказами, обнаруженными в ходе диагностических проверок.

3 Если обнаружение осуществляется быстро (например, с помощью диагностических проверок), то обнаруженные отказы или сбои могут считаться наблюдаемыми отказами или сбоями.

Если быстро обнаружить отказы не удается (например, при контрольных проверках), то при рассмотрении уровней полноты безопасности обнаруженные отказы или сбои не могут считаться наблюдаемыми отказами или сбоями.

4 Опасный раскрытый отказ может считаться безопасным отказом, только если на достаточно коротком промежутке времени, на котором обеспечено поддержание безопасности процесса, были приняты эффективные меры для его поддержания (автоматически или вручную).

3.2.14 **устройство** (device): Аппаратные средства вместе с программным обеспечением или без него, способные выполнять определенную задачу.

Примечание — Примерами устройств являются датчики, логические решающие устройства, исполнительные элементы, средства интерфейса оператора и внешняя проводка.

3.2.14.1 **внешнее устройство** (field device): Устройство ПСБ или ОСУП, непосредственно подключенное к процессу или размещенное рядом с процессом.

Примечание — Примерами внешних устройств являются датчики, исполнительные элементы и ручные переключатели.

3.2.15 **диагностика** (diagnostics): Частая (относительно времени безопасности процесса) автоматическая проверка для выявления сбоев.

3.2.15.1 **охват диагностикой**, ОД (diagnostic coverage, DC): Доля опасных отказов, выявленная в ходе диагностики. Охват диагностикой не включает в себя никакие сбои, обнаруженные с помощью контрольных проверок.

Примечания

1 Охват диагностикой чаще применяется к устройствам или подсистемам ПСБ. Например, охват диагностикой обычно определяется для датчиков, исполнительных или логических устройств.

2 В случае приложений безопасности охват диагностикой, как правило, затрагивает опасные отказы ПСБ устройств и ПСБ подсистем. Например, охват диагностикой для опасных отказов устройства или подсистемы определяется как ОД = $\lambda_{DD}/\lambda_{DT}$ (λ_{DD} — интенсивность выявленных опасных отказов и λ_{DT} — общая интенсивность опасных отказов). Для подсистемы ПСБ, обладающей внутренней избыточностью, ОД зависит от времени: ОД(t) = $\lambda_{DD}(t)/\lambda_{DT}(t)$.

3 Если известны ОД и общая интенсивность всех отказов (λ_{DT}), то интенсивность обнаруженных (λ_{DD}) и необнаруженных (λ_{DU}) отказов вычисляются по формулам:

$$\lambda_{DD} = \text{ОД} \cdot \lambda_{DT},$$

$$\lambda_{DU} = (1 - \text{ОД}) \cdot \lambda_{DT}.$$

3.2.16 **разнообразие** (diversity): Различие имеющихся мер для выполнения требуемой функции.

Примечание — Разнообразие может быть достигнуто с помощью различных физических мер, различных методов программирования или различных проектных подходов.

3.2.17

ошибка (error): Расхождение между вычисленным, наблюдаемым или измеренным значением или условием и его истинным, проектным или теоретически правильным значением или условием.
[МЭК 60050-192:2015, 192-03-02]

3.2.18

отказ (failure): Потеря способности функционировать соответствующим образом.

Примечания

1 Отказ устройства — это событие, которое приводит к состоянию сбоя этого устройства.

2 Если потеря способности функционировать вызвана скрытым сбоем, то отказ происходит в условиях определенного набора обстоятельств.

3 Выполнение требуемых функций неизбежно исключает определенное поведение, а некоторые функции могут быть определены в терминах поведения, которого следует не допускать. Случаи такого поведения являются отказами.

4 Отказы могут быть случайными или систематическими (см. 3.2.59 и 3.2.81).

[МЭК 60050-192:2015, 192-03-01, модифицировано — изменены примечания]

3.2.18.1

вид отказа (failure mode): То, каким образом происходит отказ.
[МЭК 60050-192:2015, 192-03-17]

Примечание — Вид отказа может быть определен в результате потери функции или произошедшей смены состояния.

3.2.19

сбой (fault): Потеря способности выполнять требуемую функцию из-за внутреннего состояния.

[МЭК 60050-192:2015, 192-04-01, модифицировано — некоторые примечания были изменены, а другие удалены]

Примечания

1 Сбой происходит либо в результате отказа самого элемента, либо из-за дефектов на ранних стадиях жизненного цикла, таких как спецификация, проектирование, изготовление или обслуживание.

2 Сбой устройства приводит к отказу в условиях определенного набора обстоятельств.

3.2.20 **предотвращение сбоя** (fault avoidance): Использование методов и процедур, предназначенных для предотвращения возникновения сбоев во время любой стадии жизненного цикла ПСБ.

3.2.20.1 **исключение сбоев** (fault exclusion): Исключение из дальнейшего рассмотрения сбоев из-за малой вероятности вызываемых ими видов отказов.

Примечания

1 Дополнительная информация об исключении сбоев может быть найдена в ИСО 13849-1 и ИСО 13849-2. Кроме этих стандартов исключение сбоев может быть основано:

- на технической невероятности появления некоторых сбоев;
- общепринятом техническом опыте, не зависящем от рассматриваемого приложения;
- технических требованиях, связанных с приложением и конкретной опасностью.

2 Виды отказов, идентифицированные для устройств, выполняющих функцию безопасности, могут быть исключены, так как связанная с ними интенсивность отказов является очень низкой по сравнению с целевой мерой отказов для рассматриваемой функции безопасности. То есть сумма интенсивностей опасных отказов всех серийных устройств, для которых заявляется исключение сбоев, как правило, не может превышать 1 % целевой меры отказов.

3.2.21 **отказоустойчивость** (fault tolerance): Способность функционального элемента продолжать выполнять требуемую функцию при наличии сбоев или ошибок.

3.2.22 **исполнительный элемент** (final element): Часть ОСУП или ПСБ, которая выполняет физические действия, необходимые для достижения и поддержания безопасного состояния.

Примечание — Исполнительными элементами могут служить клапаны, переключатели, двигатели, включая их дополнительные элементы (например, соленоидный клапан и исполнительное устройство, используемые для управления клапаном).

3.2.23 **функциональная безопасность** (functional safety): Часть общей безопасности процесса и ОСУП, которая зависит от правильного функционирования ПСБ и других слоев защиты.

3.2.24 **оценка функциональной безопасности;** ОФБ (functional safety assessment; FSA): Изучение фактов, позволяющее судить о функциональной безопасности, достигаемой с помощью одного или более слоев защиты ПСБ или других слоев защиты.

Примечание — Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4.

3.2.25 **аудит функциональной безопасности** (functional safety audit): Систематическое и независимое исследование для определения, согласуются ли процедуры, характерные для требований к функциональной безопасности, с запланированными мероприятиями и насколько они пригодны для достижения поставленных целей.

Примечание — Аудит функциональной безопасности может быть выполнен как часть ОФБ.

3.2.26 **полнота безопасности аппаратных средств** (hardware safety integrity): Составляющая полноты безопасности ПСБ, связанная с такими случайными отказами аппаратных средств, которые относятся к виду опасных отказов.

Примечания

1 Двумя мерами отказов, важными для данного контекста, являются средняя интенсивность опасных отказов (в режиме с высокой частотой запросов или в непрерывном режиме) и средняя вероятность отказа при выполнении запроса (в режиме с низкой частотой запросов).

2 См. 3.2.82.

3 Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4:2010.

3.2.27

вред (harm): Повреждение или ущерб здоровью человека, или повреждение имущества, или ухудшение окружающей среды.
[ИСО/МЭК Руководство 51:2014, 3.1]

3.2.27.1 **вредоносное событие** (harmful event): Опасное событие, принесшее вред.

Примечание — Приносит опасное событие вред или нет, зависит от того, подвергаются ли люди, имущество или окружающая среда влиянию опасной ситуации, а в случае нанесения вреда людям зависит от того, могут ли подверженные опасности люди избежать последствий события сразу после его происшествия. Опасное событие, нанесшее вред, называется вредоносным событием.

3.2.28

опасность (hazard): Потенциальный источник вреда.
[ИСО/МЭК Руководство 51:2014, 3.2, модифицировано — добавлено примечание]

Примечание — Термин включает в себя опасности для людей, действующие в течение коротких промежутков времени (например, пожары и взрывы), а также опасности, имеющие долгосрочное влияние на здоровье людей (например, утечка токсических веществ или радиоактивное излучение).

3.2.28.1

опасное событие (hazardous event): Событие, способное принести вред.
[ИСО/МЭК Руководство 51:2014, 3.3, модифицировано, см. примечание]

Примечание — Приносит опасное событие вред или нет, зависит от того, подвергаются ли люди, имущество или окружающая среда влиянию опасной ситуации, а в случае нанесения вреда людям зависит от того, могут ли подверженные опасности люди избежать последствий события сразу после его происшествия.

3.2.28.2

опасная ситуация (hazardous situation): Обстоятельства, в которых люди, имущество или окружающая среда подвергаются влиянию одной или нескольких опасностей.
[ИСО/МЭК Руководство 51:2014, 3.4]

3.2.29 **ошибка человека** (human error): Преднамеренное или непреднамеренное действие или бездействие человека, которое может привести к непредусмотренному результату.

Примечания

1 Примерами человеческих ошибок могут быть просчеты, промахи и оплошности.

2 Это определение не включает злонамеренное действие.

3.2.30 **анализ влияния** (impact analysis): Действия по определению влияния, при котором изменение в функции или компоненте должно привести к изменению функций или компонентов в данной системе или в системах, с ней связанных.

3.2.31 **независимая организация** (independent organisation): Отдельная организация, обособленная в отношении руководства и ресурсов от организаций, ответственных за работы, выполняемые в течение определенной стадии жизненного цикла безопасности ПСБ, которая осуществляет оценку ФБ или подтверждение соответствия ФБ.

3.2.32 **независимое лицо** (independent person): Физическое лицо, которое отделено и обособлено от действий, осуществляемых на определенной стадии жизненного цикла безопасности ПСБ, не несет прямой ответственности за указанные действия и проводит работы по оценке ФБ или подтверждению соответствия ФБ.

3.2.33 **входная функция** (input function): Функция, состоящая в регулярном наблюдении за состоянием процесса и его соответствующего оборудования в целях обеспечения логического решающего устройства входной информацией.

Примечание — Входная функция может быть выполнена вручную.

3.2.34 **прибор** (instrument): Устройство, используемое для выполнения действия и обычно входящее в состав систем, оснащенных измерительными средствами (измерительной аппаратурой).

3.2.34.1 **приборная система** (instrumented system): Система, состоящая из датчиков (например, давления, расхода, температуры), логических решающих устройств (например, программируемых контроллеров, распределенных систем управления, дискретных контроллеров) и исполнительных элементов (например, управляющих клапанов, схем управления приводом).

Примечание — Приборные системы выполняют приборные функции, включая управление, мониторинг, аварийную сигнализацию и защитные функции. Приборными системами могут быть ПСБ (см. 3.2.67) или ОСУП (см. 3.2.3).

3.2.35 **логическая функция** (logic function): Функция, выполняющая преобразование между входной информацией, полученной от одной или нескольких входных функций, и выходной информацией, используемой одной или несколькими выходными функциями.

Примечания

1 Логические функции обеспечивают преобразование из одной или нескольких входных функций в одну или несколько выходных функций.

2 Дополнительные указания см. в МЭК 61131-3:2012 и МЭК 60617-12:1997.

3.2.36 **логическое решающее устройство** (logic solver): Часть ОСУП или ПСБ, выполняющая одну или более логических функций.

Примечания

1 В МЭК 61511 применены следующие термины для логических решающих устройств:

- электрические логические системы — для систем с электромеханическим принципом действия;
- электронные логические системы — для систем с электронными системами;
- ПЭ логические системы — для систем с программируемыми электронными системами.

2 Примеры логических решающих устройств: электрические системы, электронные системы, программируемые электронные системы, пневматические системы, гидравлические системы. Датчики и исполнительные элементы не являются частью логического решающего устройства.

3.2.36.1 **конфигурируемое ПЭ логическое решающее устройство системы безопасности** (safety configured PE logic solver): Промышленное ПЭ логическое решающее устройство общего назначения, которое специально сконфигурировано для применения в целях обеспечения безопасности.

Примечание — Дополнительное руководство см. в 11.5.

3.2.37 **эксплуатационный/инженерный интерфейс** (maintenance/engineering interface): Аппаратные средства и программное обеспечение, обеспечивающие возможность правильного обслуживания и модификации ПСБ.

Примечание — Эксплуатационный/инженерный интерфейс может включать в свой состав инструкции и диагностические средства, которые можно найти в составе ПО, терминалы для программирования с соответствующими протоколами связи, средства диагностики, индикаторы, устройства обхода (байпасы), приборы для тестирования и калибровочные устройства.

3.2.37.1 **среднее время ремонта;** MRT (mean repair time; MRT): Ожидаемое общее время ремонта.

Примечание — MRT включает в себя время (b), (c) и (d) из MTTR (см. 3.2.37.2).

3.2.37.2 **среднее время до восстановления;** MTTR (mean time to restoration; MTTR): Ожидаемое время, за которое будет достигнуто восстановление.

Примечание — MTTR включает:

- время обнаружения отказа (a);
- время, прошедшее до начала ремонта (b);
- минимальное время ремонта (c);
- время возвращения компонента в работу (d).

Начало интервала (b) является концом (a); начало интервала (c) — концом (b); начало интервала (d) — это конец (c).

3.2.37.3 **максимально допустимое время ремонта;** MPRT (maximum permitted repair time; MPRT): Максимально разрешенная продолжительность ремонта последствий сбоя после его обнаружения.

Примечания

1 MRT может использоваться в качестве MPRT, но MPRT может быть определено без учета MRT:

- для снижения вероятности опасного события значение MPRT может быть выбрано меньшее, чем MRT;
- если вероятность опасного события может быть уменьшена, то значение MPRT может быть выбрано большее, чем MRT.

2 Если MPRT было определено, то его можно использовать вместо MRT для вычисления вероятности случайных отказов аппаратных средств.

3.2.38 **ослабление** (mitigation): Действие, снижающее тяжесть последствия(й) опасного события.

Примечание — Например, аварийное снижение давления или закрытие вентиляционных клапанов при обнаружении или подтверждении возгорания или утечки газа или включение водяной завесы при обнаружении подтверждения возгорания.

3.2.39 **режим работы (ФБ ПСБ)** [mode of operation (of a SIF)]: Способ, в соответствии с которым выполняется ФБ ПСБ, т. е. режим с низкой частотой запросов, высокой частотой запросов или непрерывный режим.

a) Режим с низкой частотой запросов: режим работы, при котором ФБ ПСБ для того, чтобы перевести процесс в заданное безопасное состояние, выполняется только по запросу, а частота запросов не превышает одного раза в год.

b) Режим с высокой частотой запросов: режим работы, при котором ФБ ПСБ для того, чтобы перевести процесс в заданное безопасное состояние, выполняется только по запросу, а частота запросов выше чем один запрос в год.

c) Режим с высокой частотой запросов и непрерывный режим: режим работы, при котором ФБ ПСБ удерживает процесс в безопасном состоянии, что является частью нормального функционирования.

3.2.39.1 **режим работы ФБ ПСБ по запросу** (demand mode SIF): ФБ ПСБ реализует режим с низкой частотой запросов [3.2.39 a)] или режим с высокой частотой запросов [3.2.39 b)].

Примечания

1 При опасном отказе ФБ ПСБ опасное событие может возникнуть, только если:

- отказ не был обнаружен и запрос поступает перед следующей контрольной проверкой;
- отказ обнаружен в ходе диагностической проверки, но связанный с ним процесс перевода в безопасное состояние не был запущен, а связанное с ним оборудование не было переведено в безопасное состояние перед поступлением запроса.

2 В режиме с высокой частотой запросов обычно уместно использовать критерии непрерывного режима работы.

3 Уровни полноты безопасности ФБ ПСБ, функционирующей в режиме по запросу, определены в таблицах 4 и 5.

3.2.39.2 **непрерывный режим работы ФБ ПСБ** (continuous mode SIF): ФБ ПСБ реализует непрерывный режим или режим с высокой частотой запросов [3.2.39 c)].

Примечания

1 При опасном отказе ФБ ПСБ опасное событие возникает даже без последующих отказов, если за время безопасности процесса не предприняты меры по предотвращению опасности.

2 Непрерывный режим или режим с высокой частотой запросов характерен для тех ФБ ПСБ, которые реализуют непрерывное управление, обеспечивающее поддержку функциональной безопасности.

3 Уровни полноты безопасности для ФБ ПСБ, работающей в непрерывном режиме или режиме с высокой частотой запросов, определены в таблице 5.

3.2.40 **модуль** (module): Независимая часть прикладной программы ПСБ (может быть встроена в программу или быть набором программ), выполняющая установленную функцию (например, последовательность запуска/останова/испытания исполнительного элемента, последовательность, связанную с приложением, внутри ФБ ПСБ).

Примечания

1 В контексте МЭК 61131-3:2012 модуль программного обеспечения (ПО) является функцией или функциональным блоком.

2 Большинство модулей можно повторно использовать в рамках прикладной программы.

3.2.41 **MooN** (M из N): ПСБ или ее часть, выполненная из **N** независимых каналов, соединенных так, что **M** каналов достаточно для выполнения ФБ ПСБ.

3.2.42 **необходимое снижение риска** (necessary risk reduction): Уменьшение риска, которого необходимо достигнуть с помощью ПСБ и/или других слоев защиты, чтобы быть уверенным, что риск снижен до приемлемого уровня.

3.2.43 **непрограммируемая система;** НП-система (non-programmable; NP system): Система, основанная на некомпьютерных технологиях [т. е. система, принцип действия которой не основан на использовании программируемой электроники (ПЭ) или ПО].

Примечание — Примерами таких систем являются: аппаратные электрические или электронные системы, механические, гидравлические или пневматические системы.

3.2.44 **условия эксплуатации** (operating environment): Условия работы конкретного устройства, которые потенциально влияют на его функциональность и полноту безопасности, например:

- внешняя среда, например требования для подготовки к зимним условиям, классификация опасных зон;
- условия эксплуатации процесса, например экстремальные значения температуры, давления, вибраций;
- состав, для которого реализуется процесс, например твердые частицы, соли или корродирующие вещества;
- интерфейсы процесса;
- интеграция в рамках всего завода систем управления обслуживанием и эксплуатацией;
- пропускная способность коммуникаций, например электромагнитные помехи; и
- качество общеиспользуемых услуг, например электропитания, воздуха, гидравлических систем.

Примечание — Некоторые применения процесса обладают специальными требованиями к условиям эксплуатации, выполнение которых необходимо для выживания в условиях серьезной аварии. Например, некоторое оборудование нуждается в специальных корпусах, системах продува или огнезащиты.

3.2.45 **режим работы, технологический процесс** (operating mode, process operating mode): Любое запланированное состояние технологического процесса, включая такие режимы, как запуск после аварийного останова, нормальный запуск, работа и останов, временная эксплуатация, а также аварийный режим и останов.

3.2.46 **интерфейс оператора** (operator interface): Средство или совокупность средств, обеспечивающих обмен информацией между оператором-человеком и ПСБ (например, экранные интерфейсы, световые индикаторы, кнопки, сирены, устройства аварийной сигнализации).

Примечание — Интерфейс оператора иногда называют ЧМИ.

3.2.47 **выходная функция** (output function): Функция управления процессом и его соответствующим оборудованием в соответствии с выходной информацией, поступающей от логической функции.

3.2.48 **рабочая характеристика** (performance): Выполнение заданного действия или задачи в соответствии со спецификацией и серией стандартов МЭК 61511.

3.2.49 **стадия** (phase): Временной интервал в жизненном цикле ПСБ, в течение которого выполняются действия, описанные в МЭК 61511.

3.2.50 **предотвращение** (prevention): Действие, снижающее частоту появления опасных событий.

3.2.51 **предшествующее применение** (prior use): Документированная оценка предшествующего опыта применения в похожих на текущие условиях работы, которую пользователь выполняет для доказательства того, что устройство подходит для применения в ПСБ и способно выполнять необходимые требования к полноте безопасности и функциональности.

Примечания

1 Чтобы квалифицировать устройство ПСБ на основании предшествующего применения, пользователь может документально подтвердить факт того, что устройство достигает удовлетворительных рабочих характеристик в похожих условиях работы. Чтобы обеспечить высокую степень уверенности в том, что запланированные методы, используемые при проектировании, проверке, испытании, обслуживании и эксплуатации, являются достаточными, необходимо понимание того, как оборудование ведет себя в рабочей среде.

2 Проверка в эксплуатации основывается на характеристиках проектного решения (например, предельные температура, вибрация, коррозия, необходимая поддержка обслуживания) изготовителя данного устройства. Предшествующее применение касается рабочих характеристик установленных устройств в применении для промышленных процессов в конкретной рабочей среде, которая зачастую отличается от заданной изготовителем.

3.2.52 **риск процесса** (process risk): Риск, возникающий из состояний процесса, вызванных непредусмотренными событиями (включая неправильное функционирование ОСУП).

Примечания

1 Риск в данном контексте связан с конкретным опасным событием, в котором ПСБ используется для необходимого снижения риска (т. е. риск связан с функциональной безопасностью).

2 Анализ риска процесса описан в МЭК 61511-3:2016. Основной целью определения риска процесса является установление начального значения риска без учета слоев защиты.

3 Оценка такого риска включает в себя влияние соответствующих факторов человека.

4 Данный термин эквивалентен термину «риск УО», описанному в МЭК 61508-4:2010.

3.2.52.1 **время безопасности процесса** (process safety time): Период времени между отказом процесса или основой системы управления процессом (потенциально способным привести к опасному событию) и опасным событием в случае, если ФБ ПСБ не выполняется.

Примечание — Это свойство только процесса. ФБ ПСБ необходимо обнаружить отказ и выполнить свое действие настолько быстро, чтобы опасное событие было предотвращено с учетом любых запаздываний процесса (например, из-за охлаждения емкости).

3.2.53 **программируемая электроника;** ПЭ (programmable electronic; PE): Компонент, основанный на компьютерной технологии, который может состоять из аппаратных средств, ПО и модулей ввода или вывода.

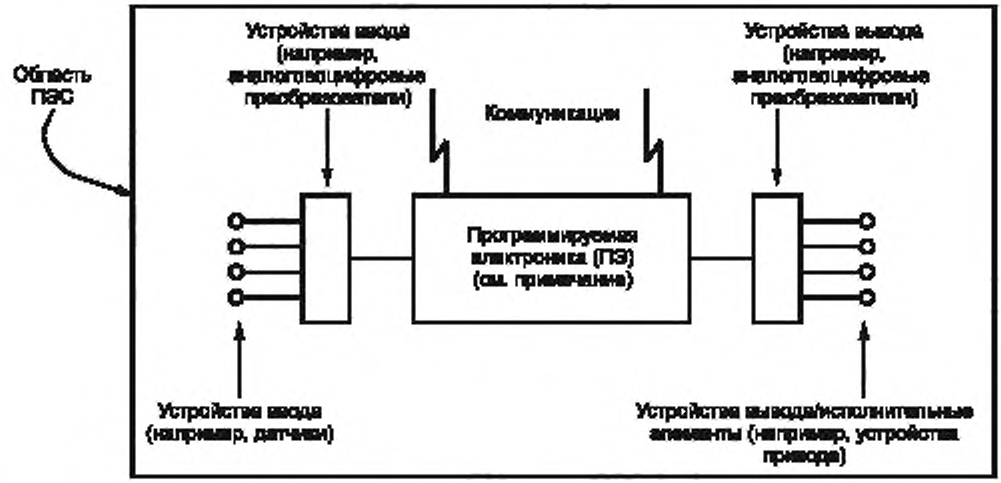
Примечания

1 Данный термин распространяется на микроэлектронные устройства с использованием одного или нескольких центральных процессоров (ЦП) с соответствующими устройствами памяти. Примерами программируемой электроники служат:

- интеллектуальные датчики и исполнительные элементы;
- программируемые электронные логические решающие устройства, включающие:
  - программируемые контроллеры;
  - программируемые логические контроллеры;
  - контроллеры цикла.

2 Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4.

3.2.54 **программируемая электронная система;** ПЭС (programmable electronic system; PES): Система для управления, защиты или контроля (мониторинга), основанная на применении одного или нескольких программируемых электронных устройств, включая все устройства системы, такие как источники питания, датчики и другие устройства ввода, шины данных и другие линии связи, исполнительные устройства и другие выходные устройства (см. рисунок 5).



Примечание — Программируемая электроника показана в центре, но она может присутствовать в нескольких местах ПЭС.

Рисунок 5 — Программируемая электронная система (ПЭС). Структура и терминология

3.2.55 **программирование** (programming, coding): Процесс проектирования, написания и тестирования набора инструкций для решения проблемы или обработки данных.

Примечание — В комплексе стандартов МЭК 61511 программирование обычно связано с ПЭ.

3.2.56 **контрольная проверка** (proof test): Периодическое испытание, проводимое для выявления скрытых опасных отказов в ПСБ, чтобы при необходимости систему можно было вернуть к ее начальному состоянию или к состоянию, максимально приближенному к начальному.

3.2.57 **слой защиты** (protection layer): Самостоятельный механизм, снижающий риск с помощью управления риском, его предотвращения или ослабления.

Примечание — Роль подобного механизма могут выполнять конструктивные решения процесса, такие как размеры емкостей, содержащих опасные химические вещества, механические устройства типа предохранительного клапана, ПСБ или организационные процедуры, такие как аварийный план действий при угрозе опасности. Их реагирование может быть автоматическим или инициироваться действиями человека (см. рисунок 9).

3.2.58 **качество** (quality): Совокупность характеристик сущности, которая отражает ее способность удовлетворять установленным и подразумеваемым потребностям.

Примечание — Более подробно см. в ИСО 9000.

3.2.59

случайный отказ аппаратных средств (random hardware failure): Отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик аппаратных средств.

[МЭК 61508-4:2010, 3.6.5, модифицировано — изменены примечания]

Примечания

1 Существует много механизмов ухудшения характеристик, действующих с различной интенсивностью в различных компонентах, и поскольку допуски изготовления приводят к тому, что компоненты в результате действия этих механизмов отказывают в разное время, отказы всего оборудования, составленного из большого числа компонентов, происходят с предсказуемой частотой, но в непредсказуемые (т. е. случайные) моменты времени.

2 Существует два основных различия между случайными отказами аппаратных средств и систематическими отказами:

- случайный отказ аппаратных средств связан только с самой системой, в то время как систематический отказ связан как с самой системой (сбой), так и с определенными условиями проявления этого сбоя (см. 3.2.81). Кроме того, случайный отказ аппаратных средств характеризуется одним параметром безотказности (интенсивностью отказов), в то время как систематический отказ характеризуется двумя параметрами безотказности (вероятностью уже существующего сбоя и частотой возникновения определенных условий возможной опасности от этого сбоя);
- систематический отказ может быть устранен после его обнаружения, в то время как случайные отказы аппаратных средств не могут быть устранены.

Это подразумевает, что параметры безотказности разных аппаратных отказов могут быть предварительно оценены на основе информации об эксплуатации, но в то же время очень сложно выполнить такую же оценку для систематических отказов. В случае систематических отказов предпочтительнее использовать качественный подход к оценке.

3.2.60

избыточность (redundancy): Наличие более одного средства для выполнения требующейся функции или для представления информации.

[МЭК 61508-4:2010, 3.4.6]

Примечания

1 Примерами избыточности являются дублирование устройств и добавление битов четности.

2 Избыточность используется в первую очередь для повышения безотказности или готовности.

3.2.61

риск (risk): Сочетание вероятности появления события причинения вреда и тяжести этого вреда.

[ИСО/МЭК Руководство 51:2014, 3.8]

Примечание — Вероятность возникновения включает в себя подверженность влиянию опасной ситуации, возникновение опасного события и вероятность того, что вреда можно будет избежать или ограничить его.

3.2.62 **безопасный отказ** (safe failure): Отказ, который не способен запустить заданное действие безопасности.

Примечания

1 Отказ является безопасным только по отношению к заданной функции безопасности.

2 Если реализована отказоустойчивость, то безопасный отказ может привести:

- к функционированию, при котором выполняются действия по безопасности, но обладает более высокой вероятностью успешное выполнение функции безопасности по запросу (режим работы по запросу) или более низкой вероятностью появление опасного события (непрерывный режим или режим работы с высокой интенсивностью запросов);
- ложному срабатыванию, в результате которого инициируется действие по безопасности.

3 Если отказоустойчивость не реализована, то безопасные отказы приводят к выполнению действия по безопасности независимо от условий процесса. Это также называют ложным срабатыванием.

4 Ложное срабатывание может быть безопасным по отношению к данной функции безопасности, но может быть опасным по отношению к другой функции безопасности.

5 Ложные срабатывания могут также негативно влиять на готовность процесса.

3.2.63 **безопасное состояние** (safe state): Состояние процесса, в котором достигается безопасность.

Примечания

1 Некоторые состояния безопаснее других, и при переходе от потенциально опасного состояния к конечному безопасному состоянию или при переходе от номинальных безопасных условий к опасным условиям процесс может проходить через несколько промежуточных безопасных состояний.

2 Для некоторых ситуаций безопасное состояние существует только до тех пор, пока процесс остается под непрерывным управлением. Такое непрерывное управление может продолжаться в течение короткого или неопределенно длительного периода времени.

3 Состояние, являющееся безопасным для одной заданной функции безопасности, может иметь высокую вероятность возникновения опасного события для другой заданной функции безопасности. В таком случае максимально допустимая средняя частота ложных срабатываний (см. 10.3.2) для первой функции может рассматриваться как возможное повышение риска, связанного с другой функцией.

4 Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4:2010.

3.2.64

безопасность (safety): Отсутствие неприемлемого риска.
[ИСО/МЭК Руководство 51:2014, 3.14, модифицировано — добавлено примечание]

Примечание — В соответствии с ИСО/МЭК Руководство 51 термины «допустимый риск» и «приемлемый риск» являются синонимами.

3.2.65 **функция безопасности** (safety function): Функция, реализуемая одним или несколькими защитными слоями, которая предназначена для достижения или поддержания безопасного состояния процесса применительно к определенному опасному событию.

3.2.66 **функция безопасности приборной системы безопасности**; ФБ ПСБ (safety instrumented function; SIF): Функция безопасности, которую будет реализовывать приборная система безопасности (ПСБ).

Примечание — ФБ ПСБ спроектирована для достижения требующегося УПБ, который определяется с учетом других слоев защиты, участвующих в снижении того же риска.

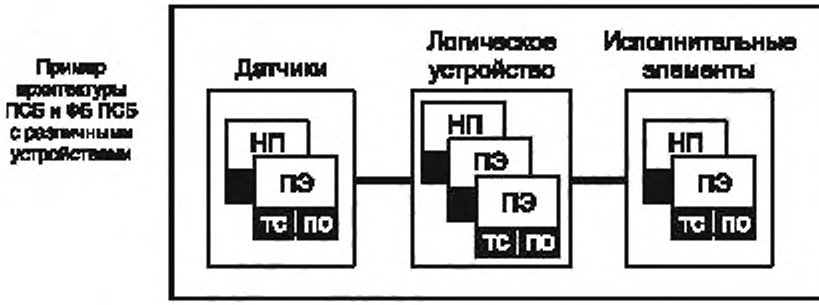
3.2.67 **приборная система безопасности**; ПСБ (safety instrumented system; SIS): Приборная система, которая используется для выполнения одной или нескольких функций безопасности.

Примечания

1 ПСБ может состоять из одного или нескольких датчиков, из одного или нескольких логических устройств и из одного или нескольких исполнительных элементов (пример см. на рисунке 6). Она также включает в себя средства коммуникации и вспомогательное оборудование (например, кабели, кабельные каналы, источники электропитания, импульсные линии и линии обогрева).

2 ПСБ может содержать в себе ПО.

3 ПСБ может включать в себя действия человека как часть ФБ ПСБ (см. ISA TR84.00.04:2015, часть 1).



ТС — технические средства; ПО — программное обеспечение

Рисунок 6 — Пример архитектуры ПСБ, включающей три подсистемы ПСБ

3.2.68 **полнота безопасности** (safety integrity): Способность ПСБ выполнять требующуюся ФБ ПСБ так, как это требуется и когда это требуется.

Примечания

1 Это определение эквивалентно функциональной надежности ПСБ при реализации требующейся ФБ ПСБ. Понятие функциональной надежности, чаще ассоциируемое скорее с экономикой, чем с концепцией безопасности, не используется во избежание путаницы.

2 Эта способность включает как функциональную реакцию (например, закрытие указанного клапана в течение установленного времени), так и вероятность того, что ПСБ будет действовать соответствующим образом.

3 При определении полноты безопасности следует учитывать все причины случайных отказов аппаратных средств и систематических отказов, которые приводят к небезопасному состоянию (например, отказы аппаратных средств, отказы, вызванные программным обеспечением, и отказы в электрических соединениях, вызванные наводками). Некоторые из таких типов отказов (например, случайные отказы аппаратных средств) могут быть описаны количественно с использованием таких параметров, как средняя частота опасных отказов или вероятность отказа при наличии запроса. Однако полнота безопасности ПСБ также зависит от многих систематических факторов, которые нельзя точно определить количественно, но которые часто рассматривают качественно на протяжении жизненного цикла. Вероятность того, что систематические отказы приводят к опасному отказу ПСБ, снижается за счет применения отказоустойчивых аппаратных средств (см. 11.4) или других методов и практических решений.

4 Полнота безопасности системы включает в себя полноту безопасности аппаратных средств (см. 3.2.26) и систематическую полноту безопасности (см. 3.2.82), но можно также рассматривать и сложные отказы, вызываемые взаимодействием случайных отказов аппаратных средств и систематических отказов.

3.2.69 **уровень полноты безопасности**; УПБ (safety integrity level; SIL): Дискретный уровень (принимающий одно из четырех возможных значений), назначаемый для ФБ ПСБ и определяющий требования к полноте безопасности, которая должна быть достигнута реализуемой ПСБ.

Примечания

1 Чем выше УПБ, тем ниже ожидаемый $ВОНЗ_{ср}$ для режима по запросу или тем ниже средняя частота возникновения опасных отказов, приводящих к опасному событию в режиме с высокой частотой запросов или с непрерывным запросом.

2 Связь между целевой мерой отказов и УПБ указана в таблицах 4 и 5.

3 УПБ 4 является самым высоким уровнем полноты безопасности; УБП 1 — самым низким.

4 Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4:2010.

3.2.69.1 **требования к полноте безопасности**; мн. ч. (safety integrity requirements, pl): Такой набор требований МЭК 61511, который должен быть выполнен ПСБ и который позволяет утверждать, что заданное значение УПБ для ФБ ПСБ реализовано данной ПСБ.

Примечание — Требования к полноте безопасности повышаются при увеличении связанного с ними УПБ.

3.2.70 **жизненный цикл ПСБ** (SIS safety lifecycle): Необходимые действия, относящиеся к реализации ФБ ПСБ, выполняемые в течение периода времени, который начинается со стадии разработки концепции проекта и заканчивается, когда все функции безопасности ПСБ уже не используются.

Примечания

1 Термин «жизненный цикл систем функциональной безопасности» является более строгим и точным, однако прилагательное «функциональной» не является обязательным в контексте комплекса стандартов МЭК 61511.

2 Модель жизненного цикла ПСБ, используемая в МЭК 61511, приведена на рисунке 7.

3.2.71 **руководство по безопасности, руководство по функциональной безопасности** (safety manual, functional safety manual): Руководство, определяющее, как для целей обеспечения безопасности могут быть применены устройства, подсистемы или системы ПСБ.

Примечания

1 Руководство по безопасности может включать в себя информацию как от изготовителя, так и от пользователя.

2 Для устройств, соответствующих МЭК 61508, руководством по безопасности является информация изготовителя.

3 Такое руководство может быть как общим самостоятельным документом, так и набором документов.

4 Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4:2010.

3.2.72

спецификация требований к безопасности; СТБ (safety requirements specification; SRS): Спецификация, содержащая функциональные требования к ФБ ПСБ и связанным с ними уровням полноты безопасности.

[МЭК 61508-4:2010, 3.5.11, модифицировано, соответствует терминологии МЭК 61511]

3.2.73 **датчик** (sensor): Часть ОСУП или ПСБ, выполняющая измерение и выявление условий протекания процесса.

Примечание — Например, передатчики, преобразователи, переключатели процессов, конечные выключатели.

3.2.74 **программное обеспечение**; ПО (software): Программы, процедуры, данные, правила и любая связанная с ними документация, относящаяся к функционированию системы обработки данных.

Примечания

1 Программное обеспечение является независимым от носителя записи, на котором оно записано.

2 Примеры различных типов ПО см. в 3.2.75 и 3.2.76.

3.2.75 **языки прикладного программирования** (application programming languages)

3.2.75.1 **фиксированный язык программирования**; ФЯП (fixed program language; FPL): Язык программирования, в котором пользователь ограничен выбором из набора нескольких заранее определенных и фиксированных параметров.

Примечание — Типичными примерами устройств с ФЯП являются интеллектуальный датчик (например, датчик давления без алгоритмов управления), интеллектуальный исполнительный элемент (например, клапан без алгоритмов управления), контроллер последовательности событий, уставки для цифрового блока аварийной сигнализации. Использование ФЯП часто называют «конфигурированием устройства».

3.2.75.2 **язык программирования с ограниченной изменчивостью**; ЯОИ (limited variability language; LVL): Язык программирования для коммерческих и промышленных программируемых электронных контроллеров, обладающий диапазоном возможностей, ограниченных применением этих возможностей, определенным в руководстве по безопасности для данных контроллеров. Нотация данного языка может быть текстовой или графической или же обладать характеристиками обоих типов.

Примечания

1 Данный язык программирования специально создан для того, чтобы его можно было легко понять пользователям, работающим с процессами, и позволяет объединить предварительно определенные, специфические для предметной области библиотечные функции для выполнения СТБ. ЯОИ позволяет обеспечить близкое функциональное соответствие с функциями, необходимыми для реализации данного применения.

2 МЭК 61511 предполагает, что ограничения, необходимые для обеспечения свойств безопасности, достигаются комбинацией положений руководства по безопасности, близостью нотаций языка к функциям, необходимым прикладному программисту для определения алгоритмов управления процессом, и проверкой времени компиляции и времени выполнения, которые провайдер логического решающего устройства закладывает в его системную программу и его среду разработки. Ограничения, идентифицированные в протоколе сертификации и руководстве по безопасности, могут гарантировать, что соответствующие требования МЭК 61508-3:2010 удовлетворены.

3 Наиболее распространенное применение ЯОИ — это «прикладные программы» в комплексе стандартов МЭК 61511.

3.2.75.3 **язык программирования с полной изменчивостью**; ЯПИ (full variability language; FVL): Язык, специально созданный для программистов и позволяющий реализовать широкий диапазон функций и прикладных задач.

Примечания

1 Типичными примерами систем, использующих ЯПИ, являются компьютеры общего назначения.

2 В области работы с процессами ЯПИ используется во встроенном программном обеспечении и реже — в прикладном.

3 Примерами ЯПИ являются Ada, C, Pascal, Список инструкций, языки ассемблера, C++, Java, SQL.

3.2.76 **Типы ПО и программ** (software & program type)

3.2.76.1 **прикладная программа** (application program): Специальная программа для приложений пользователей, содержащая в общем случае последовательности логических операций, настроенные значения программируемого устройства, ограничения и выражения, управляющие вводом, выводом, вычислениями и решениями, необходимыми для выполнения функциональных требований ПСБ.

3.2.76.2 **встроенное программное обеспечение** (embedded software): Являющееся частью системы программное обеспечение, которое поставляется производителем и запрещено модифицировать конечным пользователям.

Примечание — Встроенное программное обеспечение называют также аппаратнореализованным или системным программным обеспечением. См. 3.2.75.3, язык программирования с полной изменчивостью.

3.2.76.3 **сервисное программное обеспечение** (utility software): Инструментальные программные средства для создания, модификации и документирования прикладных программ.

Примечание — Такие инструментальные программные средства для работы ПСБ не требуются.

3.2.77 **жизненный цикл прикладной программы** (application program lifecycle): Деятельность, происходящая в течение периода времени, который начинается с появления общей концепции прикладной программы и заканчивается, когда прикладная программа окончательно перестает эксплуатироваться.

Примечания

1 Обычно жизненный цикл прикладной программы включает в себя стадии: разработки требований, разработки прикладной программы, тестирования, интеграции, установки, а также проведение модификаций.

2 Программное обеспечение, включающее прикладную программу, не может подвергаться обслуживанию, скорее, оно подлежит модификации.

3.2.78 **подсистема ПСБ** (SIS subsystem): Независимая часть ПСБ, предотвращение ведущего к аварии отказа в которой приводит к предотвращению ведущего к аварии отказа в ПСБ.

Примечания

1 На рисунке 6 показана ПСБ из трех подсистем ПСБ.

2 С точки зрения подхода, основанного на сечении (см. МЭК 61025), минимальное сечение подсистемы ПСБ является минимальным сечением всей ПСБ. Поэтому ФБ ПСБ, реализованные в ПСБ, целиком зависят от подсистем ПСБ этой ПСБ (т. е. при отказе подсистемы ПСБ связанные с ней ФБ ПСБ также выдают отказ).

3.2.79 **система** (system): Совокупность устройств, которые взаимодействуют в соответствии со спецификацией.

Примечания

1 Человек может быть частью системы.

2 Чтобы отразить отличия в терминологии, используемой при описании технологических процессов, определение данного термина отличается от его определения в МЭК 61508-4.

3.2.80 **стойкость к систематическим отказам** (systematic capability, SC): Мера (выраженная шкалой от SC 1 до SC 4) уверенности в том, что систематическая полнота безопасности устройства соответствует требованиям указанного УПБ для указанной функции безопасности, если устройство применяется в соответствии с инструкциями, указанными в руководстве по безопасности.

Примечания

1 Стойкость к систематическим отказам определяется с учетом требований к предотвращению и управлению систематическими сбоями в МЭК 61508-2:2010 и МЭК 61508-3:2010.

2 Механизм систематического отказа зависит от характера устройства. В случае устройства, состоящего только из аппаратных средств, будут рассматриваться только механизмы отказов аппаратных средств. В случае устройства, состоящего как из аппаратных средств, так и из ПО, необходимо рассмотреть взаимодействия между механизмами отказов аппаратных средств и ПО.

3 Стойкость к систематическим отказам SC *N* устройства означает, что систематическая полнота безопасности устройства с SC *N* удовлетворяет техническим требованиям, если это устройство применяется в соответствии с инструкциями, указанными для SC *N* в его руководстве по безопасности.

3.2.81 **систематический отказ** (systematic failure): Отказ, связанный с уже существовавшим сбоем, который постоянно происходит при определенных условиях и который может быть устранен только путем модификации проекта, процесса производства, рабочих операций, процедур, документации или других соответствующих факторов.

Примечания

1 Причины систематических отказов ПО могут называться «дефектами».

2 Внеплановое техобслуживание без модификации обычно не устраняет причину отказа, которая приводит к отказу при определенных условиях.

3 Систематический отказ может быть воспроизведен преднамеренной имитацией условий, при которых он уже произошел, однако не все воспроизводимые отказы являются систематическими.

4 Примерами источников систематических отказов являются ошибки человека, внесенные:

- в СТБ;
- при проектировании, изготовлении, установке, эксплуатации или обслуживании аппаратных средств;
- при проектировании или реализации ПО (включая прикладные программы).

5 Похожие устройства, спроектированные, установленные, управляемые, реализованные или обслуживаемые одинаково, вероятнее всего, будут содержать похожие сбои. Поэтому они рассматриваются как отказы по общей причине в случае, если возникают определенные условия.

3.2.82 **систематическая полнота безопасности** (systematic safety integrity): Составляющая полноты безопасности ПСБ, связанная с систематическими отказами в случае опасных отказов.

Примечания

1 Обычно систематическую полноту безопасности нельзя описать количественно (в отличие от полноты безопасности технических средств).

2 См. также 3.2.26.

3.2.83 **целевая мера отказов** (target failure measure): Рабочая характеристика, требующаяся от ФБ ПСБ и определенная либо как средняя вероятность отказа при выполнении ФБ ПСБ при наличии запроса для режима работы по запросу, либо как средняя частота опасных отказов для непрерывного режима или режима с высокой частотой запросов.

Примечание — Связь между целевой мерой отказа и УПБ дана в таблицах 4 и 5.

3.2.84

приемлемый риск (tolerable risk): Уровень риска, который приемлем при данных обстоятельствах на основании существующих в текущий период времени ценностей в обществе.

[ИСО/МЭК Руководство 51:2014, 3.15]

Примечание — См. МЭК 61511-3:2016, приложение А.

3.2.85 **необнаруженный, нераскрытый, ненаблюдаемый** (undetected, unrevealed, covert): Необнаруженный, или нераскрытый, или ненаблюдаемый отказ.

Примечание — В МЭК 61511 и за исключением случаев, когда контекст подразумевает другое значение, термин «опасные необнаруженные отказы/сбои» связан с опасными отказами/сбоями, не обнаруженными с помощью диагностических проверок.

3.2.86 **подтверждение соответствия** (validation): Подтверждение с помощью исследования и предоставления объективных свидетельств того, что определенные требования к конкретному предназначенному использованию были выполнены.

Примечание — В комплексе стандартов МЭК 61511 это означает демонстрацию того, что ФБ ПСБ и ПСБ соответствуют СТБ во всех отношениях сразу после установки.

3.2.87 **верификация** (verification): Подтверждение с помощью исследования и предоставления объективных свидетельств того, что требования были выполнены.

Примечания

1 В комплексе стандартов МЭК 61511 это действия, демонстрирующие для каждой стадии соответствующего жизненного цикла ПСБ путем анализа и/или тестирования, что при определенных входных данных выходные данные удовлетворяют во всех отношениях целям и требованиям соответствующей стадии.

2 Пример действий по верификации включает в себя:

- просмотр выходных данных (документов, относящихся ко всем стадиям жизненного цикла) для того, чтобы убедиться в соответствии целям и требованиям соответствующей стадии с учетом конкретных входных данных для этой стадии;
- проверку проектов;
- тестирование разработанных изделий для того, чтобы убедиться, что они выполнены в соответствии с их спецификациями;
- испытания интеграции, при которых различные части системы последовательно объединяются в единую систему, и испытания на воздействие окружающей среды для того, чтобы убедиться в том, что все части работают вместе в соответствии со спецификацией.

3.2.88 **сторожевое устройство** (watchdog): Совокупность диагностирующих и выходных (обычно переключающих) устройств, осуществляющих наблюдение за правильностью функционирования программируемых электронных (ПЭ) устройств и срабатывающих при обнаружении неправильной работы.

Примечания

1 Сторожевое устройство подтверждает, что система ПО работает корректно, путем регулярной установки в исходное состояние внешнего устройства (например, аппаратного электронного таймера сторожевого устройства) с помощью программно-управляемого выходного устройства.

2 Сторожевое устройство может быть использовано для обесточивания группы выходов системы безопасности при обнаружении опасных отказов для перевода процесса и удержания его в безопасном состоянии в случае опасного события. Сторожевое устройство используется для увеличения охвата диагностикой ПЭ логического решающего устройства в реальном времени (см. 3.2.13 и 3.2.15).

3.3 Сокращения

Сокращения, используемые в МЭК 61511, представлены в таблице 1. Кроме этого, были включены некоторые сокращения, связанные с функциональной безопасностью процесса.

Таблица 1 — Сокращения, используемые в МЭК 61511

Сокращение (англ.)	Сокращение (рус.)	Полное название
AC/DC	—	Постоянный ток/переменный ток
ALARP	—	Настолько низкий, насколько это практически осуществимо (As low as reasonable practicable)
AIChE	—	Американский институт инженеров-химиков (American Institute of Chemical Engineers)
ANSI	—	Американский национальный институт стандартов
AP	ППО	Прикладное программное обеспечение (программа)
BPCS	ОСУП	Основная система управления процессом
CCPS	—	Центр обеспечения безопасности химического процесса [Centre for Chemical Process Safety (AIChE)]
DC	ОД	Охват диагностикой
E/E/PE	Э/Э/ПЭ	Электрическая, или электронная, или программируемая электронная
EMC	ЭМС	Электромагнитная совместимость
FAT	ЗПИ	Заводские приемочные испытания
FPL	ФЯП	Фиксированный язык программирования
FSA	ОФБ	Оценка функциональной безопасности
FSMS	СУФБ	Система управления функциональной безопасностью
FTA	АДО	Анализ дерева ошибок
FVL	ЯПИ	Язык программирования с полной изменчивостью
H&RA	АОР	Анализ опасности и риска
HFT	—	Отказоустойчивость аппаратных средств
HMI	ЧМИ	Человеко-машинный интерфейс
IEC	МЭК	Международная электротехническая комиссия
ISA	—	Международное общество автоматизации (International Society of Automation)
ISO	ИСО	Международная организация по стандартизации

Окончание таблицы 1

Сокращение (англ.)	Сокращение (рус.)	Полное название
LVL	ЯОИ	Язык программирования с ограниченной изменчивостью
MooN	М из N	М из N (см. 3.2.45)
MPRT	—	Максимальное допустимое время ремонта
MRT	—	Среднее время на ремонт
MTTR	—	Среднее время до восстановления
NFPA	—	Национальная ассоциация пожарной безопасности США [National Fire Protection Association (US)]
NP	НП	Непрограммируемый(ая, ое)
OEM	—	Производитель оригинального оборудования (Original Equipment Manufacturer)
PE	ПЭ	Программируемая электроника
PES	ПЭС	Программируемая электронная система
PFD	ВОНЗ	Вероятность отказа при наличии запроса
PFD_{avg}	$ВОНЗ_{ср}$	Средняя вероятность отказа при наличии запроса
PFH	ВОЧ	Вероятность (средняя частота опасных отказов) отказа в час
pl	мн. ч.	Множественное число
PLC	ПЛК	Программируемый логический контроллер
S/W	ПО	Программное обеспечение
SAT	ПИО	Приемочные испытания на объекте
SC	—	Стойкость к систематическим отказам
SFF	ДБО	Доля безопасных отказов
SIF	ФБ ПСБ	Функция безопасности приборной системы безопасности
SIL	УПБ	Уровень полноты безопасности
SIS	ПСБ	Приборная система безопасности
SRS	СТБ	Спецификация требований по безопасности

4 Соответствие настоящему стандарту

Для достижения соответствия настоящему стандарту необходимо выполнять требования, представленные в разделах 5—19, по отношению к заданным указанным критериям и, следовательно, выполнять все требования каждого раздела и подраздела.

5 Управление функциональной безопасностью

5.1 Цель

Целью требований раздела 5 является определение перечня таких руководящих действий, которые необходимы для достижения требуемой функциональной безопасности.

Примечание — Раздел 5 исключительно ориентирован на достижение и поддержку функциональной безопасности ПСБ и не касается общих мер охраны здоровья и безопасности на рабочих местах.

5.2 Требования

5.2.1 Общие положения

Политику и стратегию обеспечения безопасности следует определять совместно с методами для оценки их достижимости и уведомлять организацию об их наличии.

5.2.2 Организация и ресурсы

5.2.2.1 Должны быть определены отдельные лица, подразделения, организации и другие структуры, ответственные за выполнение и проверку каждой из стадий жизненного цикла ПСБ, и необходимо проинформировать их о возложенной на них ответственности.

5.2.2.2 Отдельные лица, подразделения или организации, участвующие в реализации жизненного цикла ПСБ, должны быть компетентны в выполнении тех действий, за которые они отвечают.

При рассмотрении компетенции лиц, подразделений, организаций и других структур, участвующих в реализации жизненного цикла ПСБ, следует проверить следующие позиции:

a) технические знания, навыки и опыт, соответствующие области применения процесса;

b) технические знания, навыки и опыт работ в области применяемых технологий (например, электрических, электронных или программируемых электронных устройств);

c) технические знания, навыки и опыт работы с соответствующими датчиками и исполнительными элементами;

d) знание методов обеспечения безопасности (например, анализа безопасности процесса);

e) знание правовых и нормативных требований функциональной безопасности;

f) соответствие управленческих и лидерских навыков, их роли в действиях в течение жизненного цикла ПСБ;

g) понимание потенциально возможных последствий события;

h) УПБ ПСБ;

i) новизну и сложность данного случая применения и используемых технологий.

5.2.2.3 Должна быть утверждена процедура для управления компетентностью всех, кто вовлечен в жизненный цикл ПСБ. Для документирования компетентности отдельных лиц по отношению к выполняемой ими деятельности и при замене лица, занимающего роль, следует периодически проводить их оценку.

5.2.3 Оценка и управление рисками

Следует определить опасности, оценить риски и определить необходимое снижение риска в соответствии с указаниями, приведенными в разделе 8.

Примечание — По экономическим причинам может оказаться полезным рассмотреть также возможные капитальные затраты.

5.2.4 Планирование системы безопасности

Чтобы определить действия, которые необходимо выполнить, а также лиц, подразделения, организации или другие структуры, ответственные за выполнение этих действий, следует составить план для системы безопасности. При необходимости такой план следует обновлять в процессе всего жизненный цикл ПСБ (см. раздел 6) и выполнять его на уровне отдельных действий в соответствии с ролью, которую в жизненном цикле ПСБ выполняет лицо или организация.

Примечание — Результаты планирования системы безопасности могут быть оформлены:

- как раздел в плане качества, озаглавленный «План жизненного цикла ПСБ», или
- как отдельный документ, озаглавленный «План жизненного цикла ПСБ», или
- в виде нескольких документов, каждый из которых может устанавливать принятые в компании процедуры или правила работ.

5.2.5 Реализация и мониторинг

5.2.5.1 Следует установить процедуры, обеспечивающие быстрое и точное выполнение операций, относящихся к ПСБ и являющихся результатами следующих действий:

a) анализа опасностей и оценки рисков;

b) действий по подтверждению достоверности;

c) действий по верификации;

d) действий по подтверждению соответствия;

e) действий по оценке функциональной безопасности;

f) аудитов функциональной безопасности;

g) действий после инцидентов и несчастных случаев.

5.2.5.2 Любой поставщик изделий или услуг для организации, несущей общую ответственность за одну или более стадий полного жизненного цикла ПСБ, должен передавать изделия или услуги как специально предназначенные для этой организации и иметь систему управления качеством. При этом следует установить процедуры, чтобы продемонстрировать адекватность такой системы.

Если поставщик делает какие-либо заявления о функциональной безопасности для своего изделия или услуги, которые используются организацией для демонстрации соответствия требованиям настоящего стандарта, то поставщик должен иметь систему управления функциональной безопасностью. При этом следует установить процедуры, чтобы продемонстрировать адекватность такой системы.

Система управления функциональной безопасностью должна соответствовать требованиям базового стандарта по функциональной безопасности МЭК 61508:2010, раздел 6, или требованиям к управлению функциональной безопасностью стандарта, созданного на основе МЭК 61508, которому функциональная безопасность должна соответствовать согласно заявлениям.

5.2.5.3 Должны быть реализованы процедуры, предназначенные для оценки рабочих характеристик ПСБ ее требованиям безопасности, включая процедуры:

- для обнаружения и предотвращения систематических отказов, которые могут нарушить безопасность;
- контроля и оценки соответствия параметров безотказности ПСБ параметрам, принятым при проектировании;
- определения необходимых корректирующих действий, принимаемых в случае, если интенсивность отказов выше той, что была принята во время проектирования;
- сравнения интенсивности запросов к ФБ ПСБ во время функционирования с тем, что было принято во время оценки риска, когда определялись требования к УПБ.

5.2.5.4 Если существующая ПСБ была спроектирована и сконструирована в соответствии с кодом, стандартами или практиками, предшествующими изданию данного стандарта, то пользователь должен определить, осуществляются ли проектирование, обслуживание, осмотр, испытание и управление оборудованием безопасным образом.

5.2.6 Оценка, аудит и проверки

5.2.6.1 Оценка функциональной безопасности (ОФБ)

5.2.6.1.1 Следует определить и выполнить такую процедуру ОФБ, которая позволяет судить, достигла ли каждая ФБ ПСБ системы ПСБ необходимой функциональной безопасности и уровня полноты безопасности. Эта процедура должна требовать, чтобы была назначена команда специалистов, которая проводит ОФБ, включая техническую, прикладную и эксплуатационную экспертизу, необходимую для конкретного приложения.

5.2.6.1.2 В состав команды специалистов, проводящих ОФБ, должен входить по крайней мере один старший компетентный специалист, не участвовавший в проектировании (для этапов 1, 2 и 3), или специалист, не учувствовавший в эксплуатации и обслуживании ПСБ (для этапов 4 и 5).

5.2.6.1.3 При планировании ОФБ необходимо рассмотреть:

- область применения ОФБ;
- кто должен участвовать в ОФБ;
- навыки, ответственность и авторитетность команды специалистов, проводящих ОФБ;
- информацию, которая будет получена в результате ОФБ;
- подлинность любого другого органа, участвующего в оценивании;
- ресурсы, необходимые для выполнения действий по ОФБ;
- уровень независимости команды специалистов, проводящих оценку;
- способы, с помощью которых ОФБ будет проверяться после внесения изменений.

Примечание — Если команда специалистов, проводящих ОФБ, велика, то следует рассмотреть вопрос о привлечении в ее состав более чем одного старшего компетентного специалиста, не зависящего от проектной команды.

5.2.6.1.4 Команда по проведению ОФБ должна провести анализ работы, выполненной на всех этапах жизненного цикла системы безопасности до оцениваемой стадии, которая еще не рассматривалась в предыдущих ОФБ. Если предыдущие ОФБ были выполнены, то команда по ОФБ должна рассмотреть заключения и рекомендации предыдущих оценок. Стадии жизненного цикла ПСБ, на которых должны проводиться ОФБ, должны быть идентифицированы во время планирования ПСБ.

Примечания

1 Если после модификации или периодически в процессе функционирования будут выявлены новые источники опасности, то могут быть включены дополнительные действия по ОФБ.

2 Действия по ОФБ должны быть выполнены на следующих стадиях жизненного цикла ПСБ (см. рисунок 7):

- стадия 1. После выполнения анализа опасностей и рисков следует определить необходимые слои защиты и разработать СТБ;
- стадия 2. После проведения разработки проекта ПСБ;
- стадия 3. После того как выполнена установка и проведены предварительная сдача в эксплуатацию и заключительное подтверждение соответствия ПСБ, а также разработаны процедуры эксплуатации и технического обслуживания;
- стадия 4. После получения опыта эксплуатации и обслуживания;
- стадия 5. После проведения изменений и перед снятием ПСБ с эксплуатации.

3 Число, объем и область применения всех действий по ОФБ могут зависеть от конкретных обстоятельств. Факторы, влияющие на эти решения, обычно включают в себя:

- объем проекта;
- уровень его сложности;
- УПБ;

- продолжительность проекта;
- последствия в случае отказа;
- уровень стандартизации проектных решений;
- нормативные требования безопасности;
- предшествующий опыт выполнения подобных проектов;
- учет значимых факторов, таких как:
  - время эксплуатации,
  - число и область применения изменений в эксплуатации,
  - частота проведения контрольных проверок.

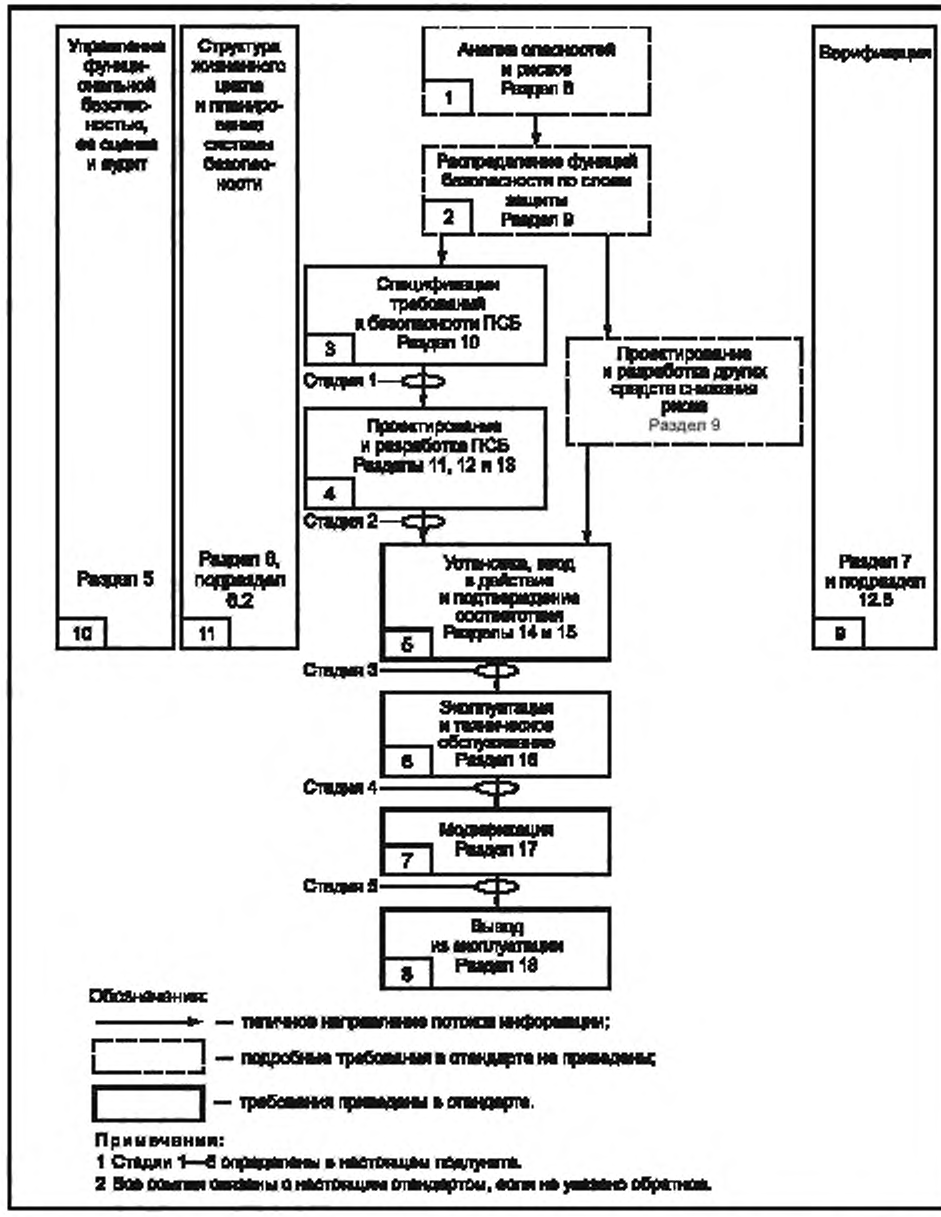


Рисунок 7 — Этапы жизненного цикла и стадии оценки функциональной безопасности ПСБ

5.2.6.1.5 Команда специалистов, проводящих ОФБ, до возникновения выявленных опасностей должна выполнить оценку(и) функциональной безопасности и подтвердить, что:

- анализ опасностей и рисков выполнен (см. 8.1);
- рекомендации, являющиеся результатом анализа опасностей и рисков, относящиеся к ПСБ, были реализованы или учтены;
- процедуры проведения изменений проектных решений существуют и были должным образом реализованы;
- рекомендации, возникшие в результате предыдущей ОФБ, выполнены;
- ПСБ спроектирована, создана и установлена в соответствии с СТБ, а любые отклонения от них определены и обоснованы;
- процедуры обеспечения безопасности, функционирования, обслуживания и действий в чрезвычайных обстоятельствах, относящиеся к ПСБ, установлены;
- планирование подтверждения соответствия ПСБ выполнено правильно, и действия по подтверждению соответствия были реализованы;
- обучение персонала было выполнено, и вся необходимая информация о ПСБ обслуживающему и оперативному персоналу предоставлена;
- планы или стратегии проведения последующих работ по ОФБ имеются.

5.2.6.1.6 Инструментальные средства проектирования, разработки и изготовления, используемые для любого действия, выполняемого на любой стадии жизненного цикла ПСБ, сами должны быть подвергнуты оценке, демонстрирующей, что они не оказывают никакого негативного влияния на ПСБ, в противном случае выходные данные инструментальных средств должны подтверждаться с помощью процедур верификации.

Примечания

1 Глубина оценивания таких средств должна зависеть от их влияния на достигаемый уровень риска.

2 Примерами инструментальных средств разработки и изготовления являются: средства имитации и моделирования, измерительное оборудование, испытательное оборудование, оборудование, используемое в действиях по обслуживанию, а также средства управления конфигурацией.

3 Контроль качества инструментальных средств включает в себя, но не ограничивается, проверку прослеживаемости до калибровочных эталонов, историю эксплуатации и журнал дефектов.

5.2.6.1.7 Результаты ОФБ должны быть доступными вместе с любыми рекомендациями, вытекающими из этой оценки.

5.2.6.1.8 Участники команды специалистов, проводящих ОФБ, должны иметь доступ по их запросу ко всей информации, относящейся к этой работе.

5.2.6.1.9 Если ОФБ выполняется в случае модификации, то в оценке должен учитываться анализ влияния модификации, выполненный для предложенной модификации и подтвердивший, что работа по модификации соответствует требованиям МЭК 61511.

Примечание — Требования к жизненному циклу ПСБ (включая ОФБ), связанные с ее модификацией, можно найти в 17.2.3.

5.2.6.1.10 ОФБ должна также периодически выполняться во время этапа эксплуатации и обслуживания, чтобы обеспечить выполнение эксплуатации и обслуживания в соответствии с положениями, принятыми во время проектирования, а также обеспечить выполнение требований МЭК 61511 по управлению безопасностью и верификации.

5.2.6.2 Аудит и проверка функциональной безопасности

5.2.6.2.1 Целью аудита является проверка информационных документов и записей для подтверждения наличия системы управления функциональной безопасностью (СУФБ), ее соответствия современным требованиям и строгого ее выполнения. Если обнаруживаются несоответствия, то указываются рекомендации по их устранению.

5.2.6.2.2 Все процедуры, определенные как необходимые и сформированные из всех действий на жизненном цикле ПСБ, должны подвергаться аудиту функциональной безопасности.

5.2.6.2.3 Аудит функциональной безопасности должен выполняться независимым лицом, не участвующим в работе над ПСБ, которая подвергается аудиту. Должны быть определены и выполнены процедуры для аудита, соответствующие требованиям, которые включают:

- частоту выполнения аудита функциональной безопасности;

- степень независимости между людьми, подразделениями, организациями и другими структурными единицами, выполняющими работу, а также теми, кто занимается аудитом функциональной безопасности;
- регистрацию и контроль результатов действий.

5.2.6.2.4 Должны быть утверждены процедуры управления изменениями, чтобы инициировать, документально оформлять, проверять, реализовывать и принимать изменения, вносимые в ПСБ, но не являющиеся равнозначной заменой (т. е. идентичной или точной копией заменяемого элемента или принятой заменой, которая не требует модификации ПСБ на момент монтажа).

5.2.6.2.5 Должны быть утверждены процедуры управления изменениями, идентифицирующие изменения, влияющие на требования к ПСБ (например, изменение проекта ОСУП, изменение в обеспечении персоналом на определенных участках).

5.2.7 Управление конфигурацией ПСБ

5.2.7.1 Должны быть установлены процедуры управления конфигурацией ПСБ, выполняемые в течение всех этапов жизненного цикла ПСБ.

Примечание — В частности, должны быть определены:
- стадии, на которых следует проводить формальное управление конфигурацией;
- процедуры, применяемые для однозначного определения всех компонент ПСБ или подсистем ПСБ (например, ее устройств, прикладных программ);
- процедуры для предотвращения использования несанкционированных устройств.

5.2.7.2 ПО, аппаратные средства и процедуры ПСБ, используемые для разработки и выполнения прикладной программы, должны быть обеспечены управлением конфигурации и управлением версиями.

Примечание — ПО ПСБ включает в себя прикладные программы (например, в логических решающих устройствах); встроенное ПО (например, датчики, логические решающие устройства, исполнительные элементы); сервисное ПО (инструментальные средства).

6 Требования к жизненному циклу системы безопасности

6.1 Цели

Цели данного раздела следующие:
- определить этапы и установить требования к действиям на жизненном цикле ПСБ;
- определить и организовать технические действия на жизненном цикле ПСБ;
- убедиться, что существует (или разрабатывается) адекватный план, который дает уверенность в том, что ПСБ отвечает требованиям безопасности.

Примечания

1 Общий подход, принятый в настоящем стандарте, показан на рисунке 7. Следует подчеркнуть, что этот подход приведен для иллюстрации и служит только для того, чтобы показать типичные действия на всем жизненном цикле ПСБ, от появления начального замысла до вывода из эксплуатации.

2 Чтобы отразить процесс контроля инцидентов и отказов, а также проверить инженерные предположения, информация на рисунке 7 может протекать в обратном направлении, от этапов эксплуатации и обслуживания к ранним этапам жизненного цикла.

6.2 Требования

6.2.1 Жизненный цикл ПСБ, предусмотренный требованиями комплекса стандартов МЭК 61511, должен быть определен в процессе планирования работ по безопасности. Жизненный цикл системы безопасности также должен охватывать и прикладное программирование (см. 6.3.1).

6.2.2 Для каждого этапа жизненного цикла ПСБ должны быть определены входы, выходы, а также действия по верификации правильности его выполнения (см. таблицу 2).

6.2.3 Для всех этапов жизненного цикла ПСБ необходимо выполнять планирование мероприятий по безопасности для определения действий, критериев, способов, показателей, процедур и ответственных организаций/людей, чтобы:
- обеспечить выполнение требований к ПСБ (и к функциям, и к полноте безопасности) для всех соответствующих состояний процесса;

- обеспечить надлежащую установку и ввод в действие ПСБ;
- обеспечить полноту безопасности ФБ ПСБ после ее ввода в действие;
- поддерживать полноту безопасности в процессе функционирования ПСБ (например, проверочные испытания, анализ отказов);
- управлять опасностями процесса в ходе технического обслуживания ПСБ.

6.2.4 Если на каком-либо этапе жизненного цикла ПСБ требуется выполнить изменения, касающиеся более раннего этапа ее жизненного цикла, то в таком случае более ранний этап жизненного цикла ПСБ и все ее последующие этапы жизненного цикла следует повторно проверить, а также внести в них соответствующие изменения и повторно верифицировать.

6.3 Требования к жизненному циклу прикладной программы приборной системы безопасности

6.3.1 Для каждого этапа жизненного цикла прикладной программы (см. рисунок 8) должны быть определены основные действия, цели, необходимая входная информация, выходные результаты, а также требования к верификации (см. таблицу 3).

6.3.2 Методы, методики и инструментальные средства должны применяться в каждом этапе жизненного цикла в соответствии с 12.6.2.

6.3.3 Каждый этап жизненного цикла ПСБ, для которого было выполнено планирование безопасности, должен быть верифицирован (см. раздел 7), а результаты должны быть представлены так, как это описано в разделе 19.

Таблица 2 — Обзор жизненного цикла ПСБ

Этап жизненного цикла ПСБ или действие		Цель	Требование. Номер раздела, подраздела	Вход	Выход
Номер блока на рисунке 7	Название				
1	Анализ опасностей и рисков (H&RA)	Определить опасности и опасные события процесса и связанного с ним оборудования, последовательности событий, приводящих к опасным событиям, риски процесса, связанные с опасным событием, требования по снижению риска и к функциям безопасности для достижения необходимого сокращения риска	Раздел 8	Проект процесса, его размещение, состав персонала, цели безопасности	Описания опасностей, требуемых функций безопасности и соответствующего снижения риска
2	Распределение функций безопасности по слоям защиты	Распределить функции безопасности по уровням защиты и для каждой ФБ ПСБ, назначить УПБ	Раздел 9	Описание необходимой ФБ ПСБ и соответствующих требований к полноте безопасности	Описание распределения требований к безопасности
3	Спецификация требований безопасности ПСБ	Установить для каждой ПСБ требования в терминах, требуемых ФБ ПСБ, и их значений полноты безопасности, необходимых для достижения требуемой функциональной безопасности	Раздел 10	Описание распределения требований к безопасности	Требования к безопасности ПСБ, требования к безопасности прикладных программ

Окончание таблицы 2

Этап жизненного цикла ПСБ или действие		Цель	Требование. Номер раздела, подраздела	Вход	Выход
Номер блока на рисунке 7	Название				
4	Проектирование и разработка ПСБ	Спроектировать ПСБ, отвечающую требованиям к ФБ ПСБ и к полноте безопасности	Разделы 11, 12	Требования к безопасности ПСБ. Требования к безопасности для прикладных программ	Проект аппаратных средств ПСБ и прикладных программ ПСБ, отвечающий требованиям к безопасности ПСБ. План тестирования интеграции ПСБ
5	Установка, ввод в действие и подверждение соответствия	Собрать и испытать ПСБ. Подтвердить соответствие ПСБ во всех отношениях требованиям безопасности в терминах, требуемых ФБ ПСБ, и их значений полноты безопасности	Разделы 14, 15	Проект ПСБ. План тестирования интеграции ПСБ. Требования к безопасности ПСБ. План подтверждения соответствия безопасности ПСБ	Полное функционирование ПСБ в соответствии с требованиями к безопасности ПСБ. Результаты тестирования интеграции ПСБ. Результаты установки, ввода в действие и подтверждения соответствия
6	Эксплуатация и техническое обслуживание ПСБ	Обеспечить поддержание функциональной безопасности ПСБ в процессе эксплуатации и технического обслуживания	Раздел 16	Требования к ПСБ. Проект ПСБ. План эксплуатации и технического обслуживания ПСБ	Результаты деятельности по эксплуатации и техническому обслуживанию ПСБ
7	Модификация ПСБ	Провести изменения, улучшения и настройку ПСБ, обеспечивающие достижение и поддержание требуемого УПБ	Раздел 17	Скорректированные требования к безопасности ПСБ	Результаты модификации ПСБ
8	Снятие с эксплуатации	Обеспечить правильную проверку, организацию работ и сохранность ПСБ	Раздел 18	Информация о технологическом процессе и требованиях к его безопасности	ПСБ, выведенная из обслуживания
9	Верификация ПСБ	Провести испытания и оценить результаты конкретного этапа, чтобы гарантировать их правильность и соответствие изделиям и стандартам на входе этого этапа	Разделы 7, 12.5	План верификации ПСБ на каждом этапе	Результаты верификации ПСБ на каждом этапе
10	ОФБ ПСБ	Обследовать ПСБ и дать заключение о достигнутой функциональной безопасности	Раздел 5	Планирование ОФБ ПСБ. Требования к безопасности ПСБ	Результаты ОФБ ПСБ
11	Структура и планирование жизненного цикла ПСБ	Установить способы выполнения этапов жизненного цикла	6.2	Не применимы	План обеспечения безопасности

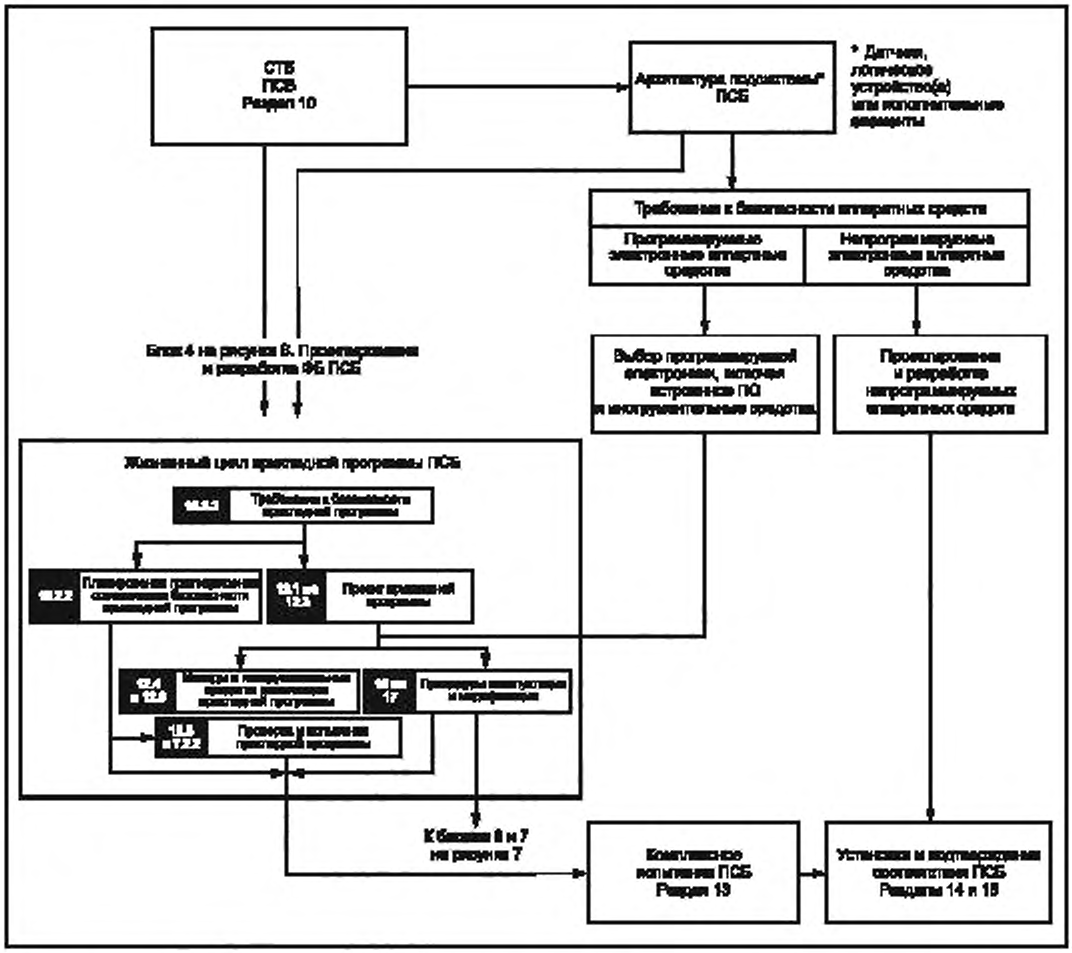


Рисунок 8 — Жизненный цикл прикладной программы ПСБ и его связь с жизненным циклом ПСБ

Таблица 3 — Жизненный цикл прикладной программы ПСБ. Обзор

Этап жизненного цикла ПСБ		Цель	Требование. Номер раздела, подраздела	Вход	Выход
Номер блока на рисунке 8	Название				
10.3.2	Требования к безопасности прикладных программ	Определить требования к безопасности прикладной программы для каждой ПСБ, необходимые для реализации требующейся ФБ ПСБ. Указать требования к прикладной программе для каждой ФБ ПСБ, назначенной этой ПСБ	10.3, 11.5	Требования к безопасности ПСБ. Руководства по безопасности для выбранной ПСБ. Архитектура ПСБ	Спецификация требования к безопасности прикладной программы ПСБ. Информация по верификации

Продолжение таблицы 3

Этап жизненного цикла ПСБ		Цель	Требование. Номер раздела, подраздела	Вход	Выход
Номер блока на рисунке 8	Название				
15.2.2	Планирование подтверждения соответствия прикладной программы	Разработать план для подтверждения соответствия прикладной программы	15.2.2, 15.2.5	Требования к безопасности прикладной программы ПСБ	Планирование подтверждения соответствия безопасности ПСБ. Информация по верификации
12.1—12.3	Разработка прикладной программы	Архитектура. Создать архитектуру прикладной программы, выполняющую указанные требования к безопасности прикладной программы. Провести проверку и оценивание требований, предъявленных к прикладной программе со стороны архитектуры аппаратных средств ПСБ. Определить процедуры для разработки прикладной программы	12.1 (также 10.3, 12.2)	Требования к безопасности прикладной программы ПСБ Ограничения проекта архитектуры аппаратных средств ПСБ	Описание проекта архитектуры, например разделение прикладной программы в подсистеме соответствующего процесса и УПБ, например выявление общих модулей прикладной программы, таких как последовательности работы насосов или клапанов. Требования к комплексному тестированию архитектуры прикладной программы и подсистемы. Информация по верификации
	Проетирование прикладной программы	Разработать проект прикладной программы. Идентифицировать подходящий набор инструментальных средств конфигурирования, управления библиотеками, управления и моделирования, используемых на протяжении жизненного цикла прикладной программы системы безопасности	12.3	Требования к безопасности прикладной программы ПСБ. Описание проекта архитектуры. Руководства по ПСБ. Руководство по безопасности для выбранного логического устройства ПСБ	Проект прикладной программы. Используемые процедуры во время программирования. Описание используемых стандартных (от производителей) библиотечных функций. Информация по верификации
12.4, 12.6	Реализация прикладной программы	Разработка приложения и его модулей. Реализовать прикладную программу, выполняющую указанные требования к безопасности приложения. Использовать подходящие инструменты поддержки и языки программирования	12.4, 12.3.4, 12.6	Описание проекта. Список руководств и процедур для выбранного логического устройства, которое будет использоваться вместе с прикладной программой	Прикладная программа (например, диаграммы функциональных блоков, многоступенчатая логика). Моделирование и комплексное испытание прикладной программы. Требования к безопасности прикладной программы специального назначения

Окончание таблицы 3

Этап жизненного цикла ПСБ		Цель	Требование. Номер раздела, подраздела	Вход	Выход
Номер блока на рисунке 8	Название				
12.5, 7.2.2	Верификация прикладной программы	Провести верификацию выполнения требований к безопасности прикладной программы. Продемонстрировать, что все прикладные программы ПСБ взаимодействуют корректно и тем самым могут выполнять предназначенные им функции (и не выполнять непредназначенные для них функции)	12.5, 7.2.2	Требования к моделированию и комплексному испытанию прикладной программы (тестирование на основе структуры). Требования к комплексному испытанию архитектуры прикладной программы	Результаты тестирования прикладной программы. Система прикладной программы, прошедшая верификацию и тестирование. Информация по верификации
13	Комплексное испытание (тестирование интеграции) ПСБ	Провести интеграцию прикладной программы в целевое логическое устройство, включая взаимодействие с опытной установкой внешних устройств и/или моделирование	Раздел 13	Требования к тестированию интеграции прикладной программы и логического устройства	Результаты тестирования интеграции прикладной программы и логического устройства

7 Верификация

7.1 Цель

Цель настоящего раздела состоит в том, чтобы продемонстрировать с помощью рассмотрения, анализа и/или испытаний, что требуемые выходные результаты соответствующих этапов (см. рисунок 7) жизненного цикла ПСБ удовлетворяют установленным требованиям, определенным с помощью планирования верификации.

7.2 Требования

7.2.1 Планирование верификации должно выполняться на протяжении всех этапов жизненного цикла ПСБ, и в плане должны быть определены все действия, необходимые для каждого этапа (см. рисунок 7) жизненного цикла ПСБ, включая стадии прикладной программы. План верификации должен соответствовать комплексу стандартов МЭК 61511, включая следующие требования:

- действия по верификации;
- процедуры, меры и способы, которые будут использованы для верификации, включая реализацию и утверждение итоговых рекомендаций;
- время выполнения указанных действий;
- определение лиц, подразделений и организаций, несущих ответственность за выполнение этих действий, включая уровни их независимости;
- определение объектов, подлежащих верификации;
- определение информации, используемой при выполнении верификации;
- определение адекватности выходных данных путем сравнения их с требованиями к данному этапу;
- определение корректности данных;
- способы преодоления несоответствий;
- инструментальные средства и анализ поддержки;

- компетентность реализации ПСБ и прослеживаемость требований;
- удобочитаемость и контролируемость документации;
- тестируемость проекта.

7.2.2 Если верификация включает в себя тестирование, то при планировании верификации должно также учитываться следующее:

- стратегия интеграции прикладной программы, аппаратных средств и внешних устройств, включая интеграцию подсистем, которые должны соответствовать другим стандартам (например, машинное оборудование или печи);
- окружение тестирования (описывает установку и настройку тестирования и какой тип тестирования будет выполняться, включая аппаратные средства, прикладное программное обеспечение и программирующие устройства, которые будут использованы);
- тестовые сценарии и результаты испытаний (т. е. конкретные сценарии со связанными с ними данными);
- типы проводимых испытаний;
- окружающие условия, включая инструментальные средства, аппаратные средства, все ПО и требующуюся конфигурацию при испытаниях;
- критерии (например, критерии прохождения/непрохождения теста), по которым оценивается результат испытаний;
- процедуры для корректирующих действий в случае отказа во время испытания;
- физические условия (например, заводские или стендовые);
- зависимости от внешних функций;
- надлежащий персонал;
- управление изменениями;
- несоответствия.

7.2.3 Функции, не связанные с безопасностью, интегрированные вместе с функциями безопасности, должны подвергаться верификации, чтобы избежать их вмешательства в выполнение функций безопасности.

7.2.4 Верификация должна выполняться в соответствии с планом верификации.

7.2.5 Во время тестирования любые модификации должны подвергаться анализу, который должен определить все компоненты ПСБ, на которые повлияли эти модификации, а также должны выполняться необходимые действия повторной верификации.

7.2.6 Результаты процесса верификации должны быть доступны (см. раздел 19), включая информацию о достижении целей и критериев тестирования.

Примечания

1 Выбор способов и мер выполнения процесса верификации и степени независимости ее исполнителей зависит от ряда факторов, включая степень сложности, новизну проекта, новизну технологии, требуемый УПБ.

2 Примерами некоторых действий по верификации являются: анализ проекта, применение инструментальных средств и способов верификации, включая средства верификации программного обеспечения и средства анализа результатов автоматизированного проектирования.

8 Анализ опасностей и рисков процесса

8.1 Цели

Цели требований настоящего раздела:

- определить опасности и опасные события процесса, свойственные данному процессу и соответствующему оборудованию;
- выявить последствия событий, приводящих к опасному событию;
- определить риски процесса, связанные с опасными событиями;
- установить любые требования по снижению риска;
- определить функции безопасности, необходимые для достижения требуемого снижения риска;
- установить, являются ли функции безопасности ФБ ПСБ (см. раздел 9).

Примечания

1 Настоящий раздел предназначен инженерам-технологам процесса, специалистам по анализу опасностей и рисков, руководителям работ по безопасности, а также инженерам по контрольно-измерительным приборам. Его задача — раскрыть междисциплинарный подход, который обычно требуется для установления ФБ ПСБ.

2 Если это практически достижимо, то процессы следует проектировать с внутренне присущими свойствами безопасности. В тех случаях, когда это невозможно, могут потребоваться другие слои защиты (см. рисунок 9). Для некоторых приложений промышленные стандарты устанавливают необходимость использования определенных слоев защиты.

3 Для снижения риска можно использовать несколько слоев защиты при условии, что такие слои являются независимыми, достаточными, зависимыми и проверяемыми аудитом.

8.2 Требования

8.2.1 Для материалов, процесса и связанного с ним оборудования следует провести анализ опасностей и риска, в результате выполнения которого:

- должны быть получены описания каждого определенного опасного события и влияющих на него факторов;
- должно быть выполнено описание вероятности и последствий каждого опасного события;
- должны быть рассмотрены режимы работы процесса, такие как нормальная работа, запуск, останов, обслуживание, нарушение режима, аварийный останов;
- должны быть установлены требования по дополнительному снижению риска, необходимому для достижения требуемой функциональной безопасности;
- должно быть выполнено описание (или даны соответствующие ссылки) мероприятий, предпринимаемых для снижения или устранения опасностей и риска;
- должны быть подробно описаны допущения, сделанные в ходе анализа рисков, включая интенсивности запросов к слоям защиты, и средняя частота опасных отказов, связанных с инициирующими источниками, а также любые сведения об ограничениях условий работы или вмешательстве человека;
- должны быть определены те функции безопасности, которые реализуются как ФБ ПСБ.

Примечания

1 При определении требований к полноте безопасности следует учесть влияние общих причин на системы, которые генерируют запросы, и слои защиты, разработанные, чтобы реагировать на эти запросы. Например, запросы могут возникнуть в результате отказа в ОСУП, а оборудование, используемое в слоях защиты, аналогично или идентично оборудованию, используемому в ОСУП. В таких случаях на запрос, вызванный отказом оборудования ОСУП, нельзя ответить эффективно, так как общая причина повлияла на подобное оборудование в системе защиты и сделала ее неработоспособной. Не всегда возможно выявить все проблемы появления общей причины в ходе начального определения опасностей и анализа рисков, потому что на такой ранней стадии разработка слоев защиты еще не будет выполнена. В подобных случаях может быть необходимым пересмотреть требования к полноте безопасности и ФБ ПСБ после завершения проектирования ПСБ и других слоев защиты. Однако при определении соответствия проекта процесса и слоев защиты требованиям необходимо рассмотреть отказы по общей причине.

2 Примеры способов, с помощью которых можно определить необходимые значения УПБ для ФБ ПСБ, продемонстрированы в МЭК 61511-3:2016.

8.2.2 Среднюю частоту опасных отказов функции ОСУП как инициирующего источника опасного события не следует принимать больше чем 10^{-5} в час.

8.2.3 Анализ опасностей и рисков должен фиксироваться так, чтобы отношения между вышеупомянутыми позициями были понятными и прослеживаемыми.

Примечания

1 Перечисленные выше требования не означают, что требования к полноте безопасности должны быть определены как числовые значения. Допустимо также применение качественных или полуколичественных подходов [см. МЭК 61511-3:2016 (приложения C, D и E)].

2 Требования к полноте безопасности зависят от особенностей применения и требований национального законодательства. Во многих странах принят следующий принцип: дополнительные меры по сокращению риска можно применять, пока их стоимость не становится непропорциональной достигнутой полноте безопасности.

8.2.4 Для идентификации уязвимых мест в защите ПСБ необходимо провести оценку рисков, связанных с защитой, результатом которой должно быть:

- описание устройств, охватываемых этой оценкой рисков (например, ПСБ, ОСУП или какое-либо другое устройство, подключенное к ПСБ);

- описание идентифицированных угроз, которые могут использовать уязвимости защиты и привести к событиям защиты (включая преднамеренные атаки на аппаратные средства, прикладные программы и связанное с ними ПО, а также непреднамеренные события, являющиеся результатом человеческих ошибок);
- рассмотрение различных этапов, таких как проектирование, реализация, запуск в эксплуатацию, эксплуатация и обслуживание;
- определение требований к дополнительному снижению риска;
- описание или ссылки на информацию по мерам, принятым для сокращения или удаления угроз.

Примечания

1 Руководство, связанное с защитой ПСБ, предоставлено в ISA TR84.00.09, ИСО/МЭК 27001:2013 и МЭК 62443-2-1:2010.

2 Информацию о граничных условиях и по управлению этими условиями, необходимую для оценки риска, связанного с защитой, как правило, можно получить у владельца/компании-производителя, но не у поставщика. В таких случаях владелец/компания-производитель может принять на себя ответственность за соблюдение соответствия требованиям настоящего пункта.

3 Оценка риска, связанного с защитой ПСБ, может выполняться как для отдельной ФБ ПСБ, так и для всех ПСБ в компании.

9 Распределение функций безопасности по слоям защиты

9.1 Цели

Цели требований настоящего раздела следующие:
- распределить функции безопасности по слоям защиты;
- определить необходимые ФБ ПСБ;
- определить для каждой ФБ ПСБ соответствующий уровень полноты безопасности.

Примечания

1 В процессе размещения следует учитывать другие отраслевые стандарты или нормы.

2 Требования к полноте безопасности для каждой ФБ ПСБ могут включать в себя соответствующее сокращение риска, ВОНЗ, ВОЧ или УПБ.

9.2 Требования к процессу распределения

9.2.1 Процесс распределения должен обеспечить:
- распределение функций безопасности, необходимых для достижения требующегося сокращения риска, по определенным слоям защиты;
- распределение сокращения риска или средней частоты опасных отказов для каждой ФБ ПСБ.

Примечание — Процесс распределения может зависеть от требований законодательства или других отраслевых норм.

9.2.2 Требуемый УПБ ФБ ПСБ должен быть определен с учетом требуемых ВОНЗ и ВОЧ, которые должны быть достигнуты с помощью этой ФБ ПСБ.

Примечание — Дополнительное руководство см. в МЭК 61511-3:3026.

9.2.3 Для каждой ФБ ПСБ, выполняемой в режиме по запросу, требуемый УПБ следует установить в соответствии с таблицами 4 или 5.

Таблица 4 — Требования к полноте безопасности: $ВОНЗ_{ср}$

Режим работы по запросу		
Уровень полноты безопасности (УБП)	$ВОНЗ_{ср}$	Целевое сокращение риска
4	$\geq 10^{-5} — < 10^{-4}$	> 10 000 — ≤ 100 000
3	$\geq 10^{-4} — < 10^{-3}$	> 1000 — ≤ 10 000
2	$\geq 10^{-3} — < 10^{-2}$	> 100 — ≤ 1000
1	$\geq 10^{-2} — < 10^{-1}$	> 10 — ≤ 100

Таблица 5 — Требования к полноте безопасности: средняя частота опасных отказов ФБ ПСБ

Непрерывный режим работы или режим работы с высокой частотой запросов	
Уровень полноты безопасности (УБП)	Средняя частота опасных отказов (в час)
4	$\geq 10^{-9} — < 10^{-8}$
3	$\geq 10^{-8} — < 10^{-7}$
2	$\geq 10^{-7} — < 10^{-6}$
1	$\geq 10^{-6} — < 10^{-5}$

Примечания

1 См. дополнительные пояснения по режимам работы в 3.2.39.

2 УПБ определен в числовой форме, чтобы обеспечить объективное сравнение альтернативных проектов и решений. Однако признается, что при современном состоянии знаний многие систематические причины отказов могут быть оценены только качественно.

3 Требуемая целевая частота опасных отказов для ФБ ПСБ в режиме непрерывной работы или в режиме с высокой частотой запросов определяется путем рассмотрения риска, вызванного отказом ФБ ПСБ, работающей в непрерывном режиме или в режиме с высокой частотой запросов, совместно с отказами других устройств, которые приводят к такому же риску, с учетом вкладов в сокращения риска от других слоев защиты.

9.2.4 Для каждой ФБ ПСБ, выполняемой в непрерывном режиме или в режиме с высокой частотой запросов, требуемый УПБ следует установить в соответствии с таблицей 5.

9.2.5 Если процесс распределения приводит к требованию снижения риска до более 10 000 или средней частоты опасных отказов менее 10^{-8} в час для одиночной ПСБ, или нескольких ПСБ, или ПСБ вместе с защитным слоем ОСУП, то необходимо пересмотреть применение (например, процесса, других защитных слоев) с целью установления возможности модификации каких-либо параметров риска так, чтобы избежать снижение риска до более 10 000 или средней частоты опасных отказов менее 10^{-8} в час. Следует рассмотреть:

- возможность модификации процесса или резервуаров/трубопровода с целью устранения или снижения опасностей, возникающих в первоисточнике;
- возможность применения дополнительных систем, связанных с безопасностью, или других мер снижения риска, не основанных на приборных средствах;
- возможность снижения степени тяжести последствий, например сокращения количества опасных материалов;
- возможность снижения вероятности заданной последовательности, например за счет снижения вероятности инициирующего источника опасного события.

Примечание — Применения, в которых требуется использование одиночной ФБ ПСБ с целевым снижением риска до более 10 000 или средней частотой опасных отказов менее 10^{-8} в час, необходимо избегать, потому что достигнуть такого высокого уровня рабочих характеристик и поддерживать их на протяжении всего жизненного цикла ПСБ достаточно сложно. Снижение риска до более 10 000 или средней частоты опасных отказов менее 10^{-8} в час может потребовать высокого уровня компетентности и высокого уровня охвата всех приемочных заводских испытаний, контрольных проверок, действий по верификации и подтверждению соответствия.

9.2.6 Если при дальнейшем рассмотрении все еще подтверждается необходимость достижения снижения риска до более 10 000 или средней частотой опасных отказов менее 10^{-8} в час, то следует рассмотреть возможности выполнения требований к полноте безопасности с помощью увеличения числа слоев защиты (например, ПСБ или ОСУП) с требованиями к снижению риска на меньшие значения. Если снижение риска распределено между несколькими слоями защиты, то такие слои защиты должны быть независимыми друг от друга или же неполную независимость следует оценить и показать, что она достаточно низка по сравнению с требованиями к снижению риска. При оценке следует учитывать следующие факторы:

- общую причину отказа ПСБ и поступления запроса.

Примечания

1 Распространенность общей причины может быть оценена за счет рассмотрения разнообразия всех устройств, отказ в которых мог повлечь за собой запрос, а также всех устройств слоя защиты ОСУП и/или ПСБ, используемых для снижения риска.

2 Примером общей причины между ПСБ и поступлением запроса может быть потеря управления процессом из-за сбоя или отказа датчика, которая может повлечь за собой запрос, в то время как датчик, используемый для управления, имеет тот же тип, что и датчик, используемый для ПСБ;

- общую причину отказов с другими слоями защиты, обеспечивающими снижение риска.

Примечания

1 Распространенность общей причины может быть оценена за счет рассмотрения разнообразия всех устройств слоя защиты ОСУП и/или ПСБ, используемых для выполнения требований к снижению риска.

2 Примером общей причины между системами ПСБ, обеспечивающими снижение риска, может быть случай, когда две отдельные и независимые ПСБ, выполняющие различные измерения, имеющие различные логические устройства, используют оконечные исполнительные устройства, которые являются двумя запорными клапанами одного типа, или имеется один запорный клапан, используемый обеими ПСБ;

- любые зависимости, которые могут возникнуть в ходе общих действий в процессе эксплуатации, обслуживания, осмотра или испытаний или из-за общих процедур контрольных проверок и общей периодичности контрольных проверок.

Примечания

1 Даже если слои защиты являются различными, то синхронные контрольные проверки уменьшат общее достигнутое снижение риска, что может быть существенным фактором, затрудняющим достижение необходимого снижения риска возникновения опасного события.

2 Если необходимы высокие уровни снижения риска и контрольные проверки не проводятся синхронно (в соответствии с примечанием 1), то главным фактором, как правило, является отказ по общей причине, даже если для снижения риска используется множество независимых слоев защиты. Зависимости внутри и между слоями защиты, обеспечивающими снижение риска возникновения некоторого опасного события, могут быть оценены, чтобы показать, что они достаточно малы.

9.2.7 Если необходимо выполнить требование по снижению риска до значения более 10 000 или средней частотой опасных отказов менее 10^{-8} в час (независимо от того, распределено ли это снижение на одну ПСБ, несколько ПСБ или на ПСБ совместно с защитным слоем ОСУП), то необходимо выполнить дополнительную оценку риска с помощью количественной методологии для подтверждения выполнения требований к полноте безопасности. В такой методологии должны учитываться зависимость и отказы по общей причине между ПСБ и:

- любым другим слоем защиты, отказ которого приведет к запросу к этой ПСБ;
- любой другой ПСБ, снижающей вероятность возникновения опасного события;
- любыми другими средствами снижения риска, которые уменьшают вероятность возникновения опасного события (например, аварийные сигналы).

9.2.8 Если снижение риска, требуемое для опасного события, распределено по нескольким ФБ ПСБ в одной ПСБ, то эта ПСБ должна удовлетворять требованию общего снижения риска.

9.2.9 Результаты процесса распределения должны быть записаны таким образом, чтобы ФБ ПСБ описывались в контексте функциональных потребностей процесса, например с указанием действий, которые необходимо предпринять, уставок, скоростей реакции, задержек активации, обработки сбоев, требований к закрытию клапанов, а также с учетом требований к снижению риска.

Примечание — Это описание может иметь точную логическую форму, а может являться ссылкой на спецификацию требований к процессу или описанием системы безопасности. Такое описание может прояснить намерения распределения и используемый подход к распределению. Спецификация требований к процессу используется в качестве входной информации для СТБ, рассмотренной в разделе 10, и она может представляться достаточно подробно, чтобы обеспечить адекватную спецификацию ПСБ и ее устройств. Например, описание может включать требования к уставкам для датчиков, ко времени безопасности процесса, доступному для реакции, и к закрытию клапанов.

9.3 Требования к основной системе управления процессом как к слою защиты

9.3.1 Основная система управления процессом может считаться слоем защиты (см. рисунок 9).



Рисунок 9 — Типовые слои защиты и средства снижения риска

9.3.2 Коэффициент снижения риска для слоя защиты ОСУП должен быть не более 10.

Примечание — Следует учитывать, что ОСУП может также являться инициатором запроса к слою защиты.

9.3.3 Если коэффициент снижения риска с помощью слоя защиты ОСУП оказывается более 10, то ОСУП следует разрабатывать в соответствии с требованиями комплекса стандартов МЭК 61511.

9.3.4 Если не предполагается, что ОСУП должна соответствовать комплексу стандартов МЭК 61511, то:

- для одной и той же последовательности событий, ведущей к появлению опасного события, если ОСУП является инициатором запроса к слою защиты, должно требоваться не более одного слоя защиты ОСУП или
- для одной и той же последовательности событий, ведущей к появлению опасного события, если ОСУП не является инициатором запроса, должно требоваться не более двух слоев защиты ОСУП.

Примечание — Идентифицированный слой защиты ОСУП может состоять из одной ОСУП, являющейся инициатором запроса (см. 8.2.2), и второго независимого слоя защиты ОСУП (см. 9.3.2 и 9.3.3) или из максимально двух независимых слоев защиты ОСУП, когда инициатор запроса, не связан с отказом ОСУП.

9.3.5 Если применим 9.3.4, то каждый слой защиты ОСУП должен быть независимым и отделен как от источника, инициирующего запрос, так и от других слоев защиты ОСУП так, чтобы ничто не могло повлиять на требуемое снижение риска слоя защиты ОСУП.

Примечания

1 Оценка разделения и независимости может позволить установить, что необходимо для достижения снижения риска, например центральные процессоры (ЦП), модули ввода/вывода, реле, внешние устройства, прикладное программное обеспечение, сети, базы данных, инструментальные средства разработки, человеко-машинный интерфейс, средства байпаса и другие устройства.

2 Контроллер оперативного резервирования не предполагается независимым от основного контроллера, так как он подвержен отказам по общей причине (например, у контроллеров оперативного резервирования имеются компоненты, которые есть как у основного контроллера, так и у контроллера резервирования, например системная плата, встроенное ПО, средства диагностики, механизмы передачи данных и необнаруженные опасные отказы).

9.4 Требования к предотвращению отказов по общей причине, отказов общего типа и зависимых отказов

9.4.1 Должен быть проанализирован проект слоев защиты для того, чтобы гарантировать, что вероятность появления отказов по общей причине, отказов общего вида и зависимых отказов между:

- слоями защиты,
- слоями защиты и ОСУП

была достаточно низкой по сравнению с общим уровнем требований к полноте безопасности слоев защиты. Оценка может быть дана в количественном или качественном виде, если не применяется 9.2.7.

Примечание — Определение зависимого отказа см. в 3.2.12.

9.4.2 При оценке должны быть рассмотрены:

- независимость слоев защиты между собой;
- разнообразие слоев защиты;
- физическое разделение между различными слоями защиты;
- отказы по общей причине между слоями защиты и между слоями защиты и ОСУП.

Примечания

1 Могут быть рассмотрены общие причины, связанные с процессом. Закупоривание предохранительного клапана может вызвать такие же проблемы, что и засорение датчика в ПСБ.

2 Можно рассмотреть независимость и физическое разделение. Человеко-машинный интерфейс, присоединения к сети ПСБ/ОСУП или средства байпаса могут приводить к отказу по общей причине.

10 Спецификация требований к безопасности приборной системы безопасности

10.1 Цель

Целью настоящего раздела является спецификация требований для ПСБ, включая любые прикладные программы и архитектуру ПСБ.

10.2 Основные требования

Требования безопасности должны быть установлены в результате распределения ФБ ПСБ и определены в ходе анализа опасностей и рисков. Требования, предъявляемые к ПСБ, должны быть выражены и структурированы так, чтобы они были:

- ясными, точными, поддающимися проверке, поддерживаемыми и реализуемыми;
- написаны так, чтобы помочь пониманию и упростить интерпретацию тем, кто обычно пользуется ими на любой стадии жизненного цикла.

10.3 Требования к безопасности приборной системы безопасности

10.3.1 Цель настоящего подраздела — рассмотреть проблемы, которые необходимо учитывать при разработке требований к безопасности ПСБ.

10.3.2 Эти требования, исходя из реальной ситуации, должны быть достаточны для проектирования ПСБ и должны включать описание намерений и подхода, применяемого при разработке требований к безопасности ПСБ, а именно:

- описание всех функций безопасности ПСБ, необходимых для достижения требуемой функциональной безопасности (например, используя причинно-следственные диаграммы, логическое описание);

- список устройств ввода и вывода на объекте, связанных с каждой ФБ ПСБ, которые четко идентифицированы с помощью средств идентификации оборудования на объекте (например, с помощью списка меток используемых устройств);

- требования для определения и учета отказов по общей причине;

- определение безопасного состояния процесса для каждой определенной ФБ ПСБ, такого, в котором достигается стабильное состояние и удается предотвратить или в достаточной мере смягчить опасное событие;

- определение любых таких по отдельности безопасных состояний процесса, которые, если совпадают во времени, создают опасность (например, переполнение аварийной памяти, система множественного сброса в факел);

- принятые источники запросов и интенсивность запросов на срабатывание для каждой ФБ ПСБ;

- требования, связанные с интервалами времени контрольных испытаний;

- требования, связанные с реализацией контрольных испытаний;

- требования ко времени отклика для каждой ФБ ПСБ, необходимому для перевода процесса в безопасное состояние за время безопасности процесса.

Примечание — Дальнейшее обсуждение времени безопасности процесса см. в МЭК 61511-2:2016;

- требуемый УПБ и режим выполнения (по запросу/непрерывный) для каждой ФБ ПСБ;

- описание измерений параметров процесса, их диапазона и точности в ПСБ и ее точки срабатывания;

- описание выходных действий, выполняемых ФБ ПСБ, и критериев их успешного выполнения (например, интенсивность утечки клапанов);

- функциональную связь между входами и выходами процесса, используя логику, математические функции и любые необходимые настроенные значения программируемого устройства для каждой ФБ ПСБ;

- требования для останова в ручном режиме для каждой ФБ ПСБ;

- требования, связанные со срабатыванием при включении или выключении питания, для каждой ФБ ПСБ;

- требования к установке каждой ФБ ПСБ в исходное состояние после ее останова (например, требования для ручной, полуавтоматической или автоматической установки в исходное состояние исполнительных элементов после срабатываний);

- максимально допустимую интенсивность ложных срабатываний для каждой ФБ ПСБ;

- режимы отказов каждой ФБ ПСБ и желательную реакцию на них ПСБ (например, аварийный сигнал, автоматическое завершение);

- любые особые требования, связанные с процедурами запуска и перезапуска ПСБ;

- все интерфейсы между ПСБ и любой другой системой (включая ОСУП и операторов);

- описание режимов работы установки и требований, связанных с работой ФБ ПСБ в каждом из режимов;

- требования к прикладной программе системы безопасности в соответствии с 10.3.3;

- требования к байпасам, включая прописанные процедуры, которые применяются во время состояния байпаса и описывают, как должно осуществляться административное управление байпаса и его последующее удаление;

- спецификацию любого действия, необходимого для достижения или поддержки безопасного состояния процесса в случае сбоя(ев), обнаруженных в ПСБ, с учетом всех соответствующих человеческих факторов;

- среднее время ремонта, достижимое для данной ПСБ, с учетом времени прибытия, обнаружения, получения запасных частей, обслуживания, а также ограничений внешней среды;

- идентификацию опасных комбинаций выходных состояний ПСБ, которых необходимо избегать;

- идентификацию предельных значений всех условий окружающей среды, с которыми может столкнуться ПСБ во время доставки, хранения, установки и эксплуатации. Это может потребовать рассмотрения следующих параметров: температуры, влажности, загрязненности, заземления, электромагнитных и радиочастотных помех (ЭМП/РЧП), ударов/вибрации, электростатических разрядов, классификации электрических зон, наводнения, молний и других факторов;

- установление нормальных и аномальных режимов работы как для объекта в целом (например, пуск установки), так и для отдельных эксплуатационных процедур объекта (например, обслуживание

оборудования, калибровка и/или ремонт датчика). Для поддержки этих режимов работы могут потребоваться дополнительные ФБ ПСБ;

- определение требований, предъявляемых к любой ФБ ПСБ, необходимой для того, чтобы перенести наиболее крупные инциденты (например, требуемое время сохранения работоспособности клапана в случае пожара).

10.3.3 Перечень требований безопасности, предъявляемых к прикладной программе, следует устанавливать, исходя из СТБ и выбранной архитектуры (организации и внутренней структуры) ПСБ. Требования к безопасности прикладной программы могут быть в СТБ или в отдельном документе (например, спецификации требований к прикладной программе). Входные данные для требований к безопасности прикладной программы для каждой подсистемы ПСБ должны включать:

a) установленные требования к безопасности каждой ФБ ПСБ, включая голосование датчиков и т. п.;

b) требования, вытекающие из архитектуры ПСБ и руководства по безопасности, такие как предельные значения и ограничения аппаратных средств и встроенного ПО;

c) любые требования по планированию безопасности, выходящие из 5.2.4.

10.3.4 Требования к безопасности прикладной программы должны быть указаны для каждого программируемого устройства ПСБ, необходимого для реализации требуемой ФБ ПСБ, в соответствии с архитектурой ПСБ.

10.3.5 Спецификация требований к безопасности прикладной программы должна быть достаточно подробной, чтобы проектирование и реализация могли достигнуть требующейся функциональной безопасности и выполнение оценки функциональной безопасности стало бы возможным. Необходимо учитывать следующее:

- ФБ ПСБ, поддерживаемые прикладной программой, и их УПБ;
- значение рабочих характеристик реального времени такие, как емкость ЦП, пропускная способность сети, допустимые рабочие характеристики реального времени в случае сбоев, а также то, что все сигналы срабатываний принимаются в рамках установленного периода времени;
- установление последовательности выполнения программ и задержки по времени, если применимы;
- интерфейсы с оборудованием и оператором и их удобство использования;
- все соответствующие режимы работы процесса, установленные в СТБ;
- действия, предпринимаемые при получении сигналов о нежелательных значениях переменных процесса, таких как значение сигнала датчика вне рабочего диапазона, излишний диапазон изменений, не меняющееся значение, обнаруженный разрыв цепи, обнаруженное короткое замыкание;
- функции, позволяющие проверочные и автоматические диагностические испытания внешних устройств (например, датчиков и исполнительных элементов), выполняемые в прикладной программе;
- самоконтроль прикладной программы (например, проверки программно-управляемых сторожевых устройства и диапазона данных);
- мониторинг других устройств в ПСБ (например, датчиков и исполнительных элементов);
- любые требования, связанные с проведением периодических проверок ФБ ПСБ без останова процесса;
- ссылки на входные документы (например, на спецификацию ФБ ПСБ, конфигурацию или архитектуру ПСБ, требования к полноте безопасности аппаратных средств ПСБ);
- требования к коммуникационным интерфейсам, включая меры по ограничению их использования, и к подтверждению соответствия как принимаемых, так и передаваемых по ним данных и команд;
- опасные состояния процесса (например, одновременное закрытие двух отсечных газовых клапанов, которое может повлечь за собой флуктуации давления и тем самым привести к опасному состоянию), создаваемые прикладной программой, необходимо идентифицировать и предотвращать;
- определения критериев подтверждения соответствия переменных процесса для каждой ФБ ПСБ.

10.3.6 Спецификация требований к безопасности прикладной программы должна быть выражена и структурирована таким образом, чтобы:

- она описывала намерения и подход, лежащий в основе требований к безопасности прикладной программы;
- была ясно выраженной и понятной для тех, кто будет использовать документ на любой стадии жизненного цикла ПСБ, что подразумевает использование четкой и понятной для всех пользователей

терминологии и описаний (например, для операторов на объекте, обслуживающего персонала, прикладных программистов);

- ее можно было бы верифицировать, проверить и модифицировать;
- она являлась прослеживаемой через всю выпускаемую документацию, включая документацию детального проектирования, СТБ, а также анализ опасностей и рисков, идентифицирующий требующиеся ФБ ПСБ и УПБ.

11 Проектирование и разработка приборной системы безопасности

11.1 Цель

Целью требований настоящего раздела является проектирование одной или нескольких ПСБ, выполняющей(их) ФБ ПСБ и удовлетворяющей(их) заданным требованиям полноты безопасности (например, УПБ, соответствующему снижению риска, ВОНЗ и/или ВОЧ).

11.2 Основные требования

11.2.1 Проект ПСБ должен соответствовать спецификации требований безопасности ПСБ с учетом всех требований настоящего раздела.

11.2.2 Если ПСБ должна осуществлять и ФБ ПСБ, и функции, не связанные с безопасностью, то все аппаратные средства, встроенное ПО и прикладные программы, которые могут негативно повлиять на любую ФБ ПСБ при нормальных условиях и в случае сбоя, должны рассматриваться как часть ПСБ и быть выполнены в соответствии с требованиями самого высокого УПБ среди всех ФБ ПСБ, на которые оно может повлиять.

11.2.3 Если ПСБ должна выполнять ФБ ПСБ с различными УПБ, тогда общедоступные или общие аппаратные средства, встроенное ПО и прикладные программы должны соответствовать самому высокому УПБ.

Примечание — Встроенное ПО или прикладные программы с разными УПБ могут сосуществовать в одном устройстве, если можно продемонстрировать, что ФБ ПСБ с более низким УПБ не может негативно влиять на ФБ ПСБ с более высоким УПБ.

11.2.4 Если не предполагается квалифицировать ОСУП как удовлетворяющую комплексу стандартов МЭК 61511, то ПСБ должна быть спроектирована так, чтобы ОСУП была отделена и независима до такой степени, чтобы не нарушалась полнота безопасности ПСБ.

Примечания

1 Обмен операционной информацией может быть реализован, но он не должен влиять на функциональную безопасности ПСБ.

2 Для выполнения функций ОСУП могут быть также использованы технические средства ПСБ, если можно показать, что отказ ОСУП не ухудшает выполнения ФБ ПСБ системы ПСБ.

11.2.5 В процессе проектирования ПСБ должны быть реализованы требования по оперативности, обслуживаемости, диагностике, осмотру и проверяемости, чтобы понизить вероятность возникновения опасных отказов.

11.2.6 Проект ПСБ должен учитывать возможности и ограничения человека и задачи, поручаемые операторам и обслуживающему персоналу. Проект интерфейсов оператора должен следовать устоявшейся практике учета человеческого фактора и должен быть приспособлен к уровню подготовки, который должны освоить операторы.

Примечание — Например, если для работы регулярно необходим ввод данных об ограничениях или другой вводимой оператором информации, то может быть необходимо выполнение исследований человеческого фактора.

11.2.7 ПСБ должна быть спроектирована так, чтобы как только она перевела процесс в безопасное состояние, процесс должен оставаться в безопасном состоянии до тех пор, пока не будет инициирована его установка в исходное состояние, или до другого события, установленного в СТБ.

11.2.8 Независимо от логического управляющего устройства должны существовать ручные средства (например, кнопка аварийного останова), чтобы воздействовать на процесс через исполнительные элементы ПСБ или другие средства, установленные в СТБ.

11.2.9 Проект ПСБ должен учитывать все аспекты зависимости и независимости между ПСБ и ОСУП, а также между ПСБ и другими слоями защиты.

11.2.10 Любое устройство, используемое ОСУП, не должно использоваться ПСБ в тех случаях, если отказ этого устройства может привести как к запросу к ФБ ПСБ, так и к опасному отказу этой ФБ ПСБ, если только не был проведен анализ, подтверждающий, что общий риск остается приемлемым.

Примечание — Если часть ПСБ также используется для целей управления и опасный отказ общего оборудования приводит к запросу функции, выполняемой ПСБ, то появляется новый риск. Величина дополнительного риска зависит от интенсивности опасных отказов общего устройства, так как если в общем устройстве происходит сбой, то немедленно создается запрос к ПСБ, на который она, возможно, не готова ответить. Поэтому в таких случаях необходимо провести дополнительный анализ, чтобы убедиться, что интенсивность опасных отказов совместно используемых устройств достаточно низка. В качестве примеров такого оборудования, общего с ОСУП, часто рассматривают датчики и клапаны.

11.2.11 Если любое устройство ПСБ, которое при потере функциональности (например, в случае отключения электропитания или подачи воздуха, гидравлического или пневматического давления), не способно перейти в безопасное состояние, то такие потери функциональности, а также нарушения целостности цепей ПСБ должны выявляться и приводить к формированию аварийных сигналов (например, с помощью мониторинга линии питания, измерения питающего давления, мониторинга гидравлического или пневматического давления), а также к выполнению действий в соответствии с 11.3.

Примечания

1 Полнота функциональности может быть улучшена с помощью дополнительного источника питания (например, аварийного аккумуляторного питания, бесперебойных источников питания, резервуара для воздуха, гидравлического аккумулятора, второго источника газоснабжения).

2 Потеря функциональности, вероятно, скажется на нескольких ФБ ПСБ и, возможно, нескольких ПСБ. Поэтому необходимо учитывать вероятность отказа по общей причине нескольких ФБ ПСБ.

11.2.12 Проект ПСБ должен быть таким, чтобы он обеспечивал необходимый уровень устойчивости к идентифицированным рискам для защиты (см. 8.2.4).

Примечание — Руководство по защите ПСБ предоставлено в ISA TR84.00.09, ИСО/МЭК 27001:2013 и МЭК 62443-2-1:2010.

11.2.13 Руководство по безопасности, охватывающее эксплуатацию, обслуживание, обнаружение сбоев и ограничения, связанные с ПСБ, должно также охватывать предполагаемую конфигурацию устройств и предполагаемую рабочую среду.

11.2.14 Все коммуникации, применяемые для реализации ФБ ПСБ, должны быть спроектированы с помощью методов, обеспечивающих соответствие приложений безопасности требующимся УПБ.

11.3 Требования к поведению системы при обнаружении отказа

11.3.1 Если в ПСБ обнаруживается опасный отказ (диагностическими тестами, контрольными проверками или любыми другими средствами), то для поддержания безопасного функционирования необходимо применить компенсирующие меры. Если безопасное функционирование невозможно поддерживать, то должно быть выполнено конкретное действие для достижения и поддержания безопасного состояния процесса. Если компенсирующие меры зависят от выполнения оператором определенных действий в ответ на аварийный сигнал (например, управление клапаном или закрытие клапана), то аварийный сигнал следует считать частью ПСБ.

Примечания

1 Конкретное действие, направленное на достижение или поддержание безопасного состояния процесса, может быть определено в СТБ (см. 10.3.1). Оно может заключаться в безопасном завершении процесса или его неисправной части для снижения риска на дефектной ПСБ.

2 Компенсирующие меры, необходимые для непрерывного безопасного функционирования, могут зависеть от требований к полноте безопасности, допустимого риска, связанного с опасным событием, устойчивости к отказам аппаратных средств ПСБ, ожидаемого MRT и готовности любых других слоев защиты. В некоторых случаях адекватным решением может быть обеспечение выполнения действия, гарантирующего устранение причин опасного отказа за время MPRT, принятого для вычисления $ВОНЗ_{ср}$, но в других случаях может быть обосновано, что необходимо обеспечить другие меры, компенсирующие уменьшение снижения риска до тех пор, пока ПСБ не будет полностью восстановлена (см. 16.2.3).

11.3.2 Если опасный сбой в ПСБ доводится до внимания оператора с помощью аварийного сигнала, то аварийный сигнал должен быть подвергнут контрольной проверке и охвачен управлением изменениями.

11.4 Отказоустойчивость аппаратных средств

11.4.1 ПСБ должна иметь минимальное значение HFT по отношению к каждой ФБ ПСБ, которую она реализует.

Примечание — Это не исключает вероятность того, что иногда во время эксплуатации системы после сбоя значение HFT может стать ниже минимально требуемого.

11.4.2 Если ПСБ может быть разделена на независимые подсистемы ПСБ (например, датчики, логические устройства и исполнительные элементы), то значение HFT может быть задано на уровне подсистемы ПСБ.

11.4.3 Значение HFT для ПСБ или подсистем этой ПСБ должно соответствовать требованиям:

- 11.4.5—11.4.9, или
- 7.4.4.2 (способ 1_H) МЭК 61508-2:2010, или
- 7.4.4.3 (способ 2_H) МЭК 61508-2:2010.

Примечание — Способ, разработанный в МЭК 61511, получен из способа 2_H МЭК 61508-2:2010.

11.4.4 При определении достигаемой HFT определенные сбои могут быть исключены, если вероятность их возникновения очень низкая по отношению к требованиям к полноте безопасности. Любые такие исключения сбоев должны быть обоснованы и документально оформлены.

Примечание — Дополнительную информацию об исключении сбоев можно найти в ИСО13849-1:2006 и ИСО13849-2:2012.

11.4.5 Минимальная HFT для ПСБ (или подсистем этой ПСБ), реализующей ФБ ПСБ с заданным УПБ, должна соответствовать таблице 6 и, если необходимо, требованиям 11.4.6 и 11.4.7.

Примечание — Требования к HFT в таблице 6 представляют собой минимальное резервирование системы или, если необходимо, подсистемы ПСБ. В зависимости от применения, интенсивности отказов устройства и интервала времени проверочных испытаний может потребоваться дополнительное резервирование, чтобы обеспечить меру отказов, соответствующую УПБ для ФБ ПСБ согласно 11.9.

Таблица 6 — Минимально требуемая HFT, соответствующая УПБ

УПБ	Минимально требуемая HFT
1 (любой режим)	0
2 (режим с низкой частотой запросов)	0
2 (режим с высокой частотой запросов или непрерывный режим)	1
3 (любой режим)	1
4 (любой режим)	2

11.4.6 Если для ПСБ или подсистемы ПСБ, которая не использует устройства, программируемые на ЯПИ или ЯОИ, минимальная HFT, соответствующая таблице 6, приведет к дополнительным отказам и общему снижению безопасности процесса, то HFT можно понизить. Это должно быть обосновано и документально оформлено. Обоснование должно включать доказательства того, что предложенная архитектура подходит для предназначенной ей цели и соответствует требованиям к полноте безопасности.

Примечание — Отказоустойчивость является предпочтительным решением для достижения требующейся уверенности в том, чтобы была создана устойчивая к сбоям архитектура. Если применяются требования 11.4.6, то целью обоснования является демонстрация того, что предложенная альтернативная архитектура предоставляет равносильное или улучшенное решение. Она может меняться в зависимости от применения и/или используемой технологии, например в зависимости от организации средств резервирования (например, аналитическая избыточность, замена отказавшего вывода датчика на результаты физических вычислений, полученные из

выходных данных других датчиков); использования более надежных элементов той же технологии (если они доступны); перехода на более надежную технологию; смягчения последствий отказов по общей причине при помощи отличающихся технологий; повышения расчетных допусков; ограничения условий окружающей среды (например, для электронных компонентов); понижения неуверенности в безотказности за счет получения дополнительной информации о результатах эксплуатации или проведения экспертной оценки.

11.4.7 Если в результате применения требований 11.4.6 получена отказоустойчивость, равная нулевой, то обоснование, которое требуется предоставить согласно 11.4.6, должно содержать доказательства возможности исключения связанных с проблемой опасных видов отказов в соответствии с 11.4.4, включая рассмотрение потенциальных систематических отказов.

11.4.8 Устройства, программируемые на ЯПИ или ЯОИ, должны иметь охват диагностикой не ниже 60 %.

11.4.9 Надежность данных, используемых при вычислениях меры отказов, должна определяться на основе верхнего максимального значения статистического доверительного интервала, составляющего не меньше 70 %.

11.5 Требования к выбору устройств

11.5.1 Цели

Целями, связанными с требованиями 11.5, являются:

- установить требования для выбора устройств, которые должны использоваться как часть ПСБ;
- установить требования к интеграции устройств в архитектуру ПСБ;
- определить технические условия устройств в терминах, соответствующих ФБ ПСБ, и полноты безопасности.

11.5.2 Общие требования

11.5.2.1 Устройства, выбираемые для использования в качестве части ПСБ и обладающие установленным УПБ, должны соответствовать требованиям МЭК 61508-2:2010 и МЭК 61508-3:2010 и/или 11.5.3—11.5.6, когда это целесообразно.

Примечание — Устройства, проверенные на соответствие МЭК 61508-2:2010 и МЭК 61508-3:2010, могут применяться в соответствии с требованиями к стойкости к систематическим отказам в МЭК 61508-2:2010.

11.5.2.2 Все устройства должны соответствовать условиям эксплуатации, которые определяются в результате анализа документации изготовителя, ограничений в СТБ и параметров безотказности, принятых согласно 11.9. Пригодность выбранных устройств всегда должна рассматриваться в контексте условий эксплуатации.

Примечание — Устройства могут обладать различной интенсивностью отказов, в зависимости от условий эксплуатации и режима работы. Информация об интенсивности отказов, получаемая от изготовителя, не может быть достоверной для всех применений. Например, распределение интенсивности отказов по видам отказов может быть разным у постоянно используемого клапана и клапана, который не используется длительные промежутки времени.

11.5.3 Требования для выбора устройств на основе опыта их предшествующего применения

11.5.3.1 Необходимо располагать надлежащими доказательствами того, что устройства пригодны для использования в составе ПСБ.

Примечания

1 Основной задачей оценивания предыдущего использования является сбор доказательств того, что число систематических сбоев было снижено до достаточно низкого уровня по сравнению с уровнем необходимой полноты безопасности.

2 Уровень подробности доказательства следует выбирать в соответствии со сложностью рассматриваемого устройства.

3 Оценивание предыдущего опыта использования включает сбор документально оформленной информации о рабочих характеристиках устройства в похожей рабочей среде. Предыдущий опыт использования демонстрирует функциональность и полноту установленного устройства, включая интерфейсы с процессом, все интерфейсы, коммуникации и средства обеспечения устройства. Основной задачей оценивания предыдущего опыта использования является сбор доказательств того, что число опасных систематических сбоев было снижено до достаточно низкого уровня по сравнению с требуемым уровнем полноты безопасности.

4 Данные о предыдущем использовании могут внести свой вклад в базу данных для вычисления интенсивностей отказов аппаратных средств, как это описано в 11.9.3.

11.5.3.2 Доказательство пригодности должно включать в себя следующее:

- рассмотрение имеющихся у изготовителя систем управления качеством, управления предприятием и управления конфигурацией изделий;
- адекватность идентификации и спецификации устройств;
- демонстрацию рабочих характеристик устройств в аналогичных условиях эксплуатации.

Примечание — Внешние устройства (например, датчики и исполнительные элементы), удовлетворяющие заданной спецификации, как правило, ведут себя идентично как в приложениях, связанных с безопасностью, так и в приложениях, не связанных с безопасностью. Поэтому рассмотрение рабочих характеристик подобных устройств при работе в приложениях, не связанных с безопасностью, также может считаться выполнением данного требования;

- объем опыта эксплуатации.

Примечания

1 Информация об опыте эксплуатации внешних устройств регистрируется главным образом в установленных журналах пользователя и основана на обширной предыстории их успешной работы в безопасных и небезопасных приложениях и на исключении сведений об оборудовании, не работающем удовлетворительно. Такой журнал эксплуатируемых устройств может быть использован для получения сведений об опыте эксплуатации при следующих условиях:

- журнал ведут и контролируют регулярно;
- эксплуатируемые устройства добавляют в журнал, только когда получен положительный опыт эксплуатации;
- эксплуатируемые устройства удаляют из журнала, когда история их применения показывает, что их функционирование проходит неудовлетворительно;
- рабочая среда включается в журнал только там, где она имеет значение.

2 Значительное влияние на рабочие характеристики устройства оказывает рабочая среда. Как правило, рекомендуется выбирать устройства на основе соответствующих рабочих характеристик достаточного числа установленных устройств в нескольких установках, работающих достаточное время. Полученный опыт может позволить в течение времени выявить ранние отказы, такие как те, что связаны со спецификацией, обработкой, установкой и вводом в эксплуатацию.

3 Опыт эксплуатации, необходимый для получения достоверной статистической информации о безотказности, как правило, значительно превышает опыт эксплуатации, необходимый для получения доказательств о предыдущем использовании.

11.5.3.3 Все устройства, выбранные на основе предыдущего использования, должны быть идентифицированы с помощью указанного номера версии и должны подчиняться процедуре управления изменениями. В случае внесения изменений в устройство сохранение действительности доказательств о предыдущем использовании должно быть обосновано оценкой значимости внесенных изменений.

11.5.4 Требования к выбору программируемых на ЯФП устройств (например, внешних устройств) на основе опыта их предыдущего использования

11.5.4.1 Для УПБ 1, УПБ 2 и УПБ 3 применимы требования, установленные в 11.5.2 и 11.5.3, вместе со следующими пунктами.

11.5.4.2 Должны быть идентифицированы и рассмотрены все варианты конфигурации устройства, которые, вероятно, скажутся на безопасности. Важно проверить, что подтверждается возможность использования настроек по умолчанию, если конкретные настройки не определены. При доказательстве пригодности следует выявить неиспользуемые характеристики компонентов и подсистем и установить, что они едва ли могут порождать опасность при выполнении требуемой ФБ ПСБ.

11.5.4.3 Для доказательства пригодности конкретной конфигурации и конкретных условий работы устройства следует рассмотреть:

- характеристики входных и выходных сигналов;
- режимы использования;
- применяемые функции и конфигурации;
- предшествующее использование при аналогичных физических условиях окружающей среды.

11.5.4.4 Для приложений с УПБ 3 должна быть дополнительно выполнена оценка устройства на ФЯП, чтобы показать, что:

- такое устройство не только способно выполнять требуемые функции, но и, как показывает опыт его предшествующего применения, обладает достаточно низкой вероятностью таких отказов, которые могут привести к опасному событию при его использовании в качестве части ПСБ, включая как случайные отказы аппаратных средств, так и систематические отказы в аппаратных средствах и ПО;

- применены соответствующие стандарты для аппаратных средств и ПО;
- такое устройство применено и испытано в составе конфигурации, представляющей ожидаемые условия его работы.

11.5.5 Требования к выбору программируемых на ЯОИ устройств на основе опыта их предыдущего использования

11.5.5.1 Следующие требования применимы только к ПЭ-устройствам, используемым в системах ПСБ, реализующих ФБ ПСБ с УПБ 1 или УПБ 2.

11.5.5.2 Применимы требования подраздела 11.5.4.

11.5.5.3 Если существует какое-либо различие между рабочей средой устройства, в которой оно ранее использовалось, и рабочей средой устройства, применяемого в ПСБ, то любые такие различия должны быть выявлены и им должна быть дана соответствующая оценка, основанная на анализе и испытаниях (когда это целесообразно), чтобы показать, что вероятность систематических сбоев при использовании устройства в ПСБ достаточно мала.

11.5.5.4 Для подтверждения пригодности должен быть определен необходимый опыт работы, учитывающий:

- УБП для ФБ ПСБ;
- сложность и функциональные возможности устройств.

11.5.5.5 Для случаев применения с УПБ 1 или УБП 2 конфигурируемые логические устройства безопасности с программируемой электроникой могут быть применены при соблюдении следующих условий:

- понимании того, какие отказы относятся к опасным видам;
- применении способов обеспечивающей безопасность конфигурации, учитывающих установленные виды отказов;
- использовании встроенного ПО, имеющего хорошую историю применения на опасных объектах;
- защиты против несанкционированных или непреднамеренных изменений.

Примечание — Конфигурируемые логические устройства безопасности с программируемой электроникой представляют собой программируемые электронные устройства общего назначения в промышленном исполнении, которые специально конфигурируются OEM, специалистом по системам управления или конечным пользователем для применения на опасных объектах.

11.5.5.6 В случаях применения с УПБ 2 формальную оценку любого логического устройства с программируемой электроникой следует выполнить так, чтобы показать, что:

- данное устройство не только способно выполнять требуемые функции, но и, как показывает опыт его предшествующего использования, обладает достаточно низкой вероятностью таких отказов, которые могут привести к опасному событию при его использовании в качестве части ПСБ, включая как случайные отказы аппаратных средств, так и систематические отказы аппаратных средств или ПО;
- предусмотрены меры для обнаружения ошибок в процессе выполнения программы и соответствующего реагирования на них; такие меры должны включать в себя все следующие позиции:
  - контроль последовательности выполнения программы;
  - защиту кода от изменений или обнаружение отказов с помощью оперативного мониторинга;
  - программирование выявления отказов или разнотипное программирование;
  - проверку диапазонов переменных или проверку правдоподобия значений величин;
  - модульный подход;
  - применение соответствующих стандартов кодирования для встроенного и сервисного ПО;
  - испытания в составе типовых конфигураций, соответствующих предполагаемым условиям работы;
  - применение хорошо проверенных программных модулей и компонентов;
  - проведение динамического анализа и испытаний системы;
  - система не использует ни методы искусственного интеллекта, ни средства динамического изменения;
  - документально оформленное выполнение проверки с введением неисправностей (негативное тестирование).

11.5.6 Требования к выбору программируемых устройств, использующих ЯПИ

Если в приложениях использован ЯПИ, то ПЭ-устройство должно соответствовать требованиям МЭК 61508-2:2010 и МЭК 61508-3:2010.

11.6 Внешние устройства

11.6.1 Внешние устройства следует выбирать и устанавливать так, чтобы минимизировать отказы, неточная информация о которых может появиться из-за обстоятельств, возникающих в рабочей среде. Обстоятельства, которые следует рассмотреть, включают: коррозию, замерзание веществ в трубах, взвешенность твердых частиц, полимеризацию, спекание, экстремальные значения температуры и давления, конденсацию в незаполненных или не полностью заполненных импульсных линиях.

11.6.2 Цепи срабатывания защиты при подаче питания должны применять средства, гарантирующие целостность цепи и источника электропитания.

Примечания

1 Примером такого средства является средство контроля разрыва цепи, в котором сигнальный ток непрерывно контролирует целостность цепи, но при этом сам сигнальный ток такой величины, которая не способна повлиять на значения сигналов входа/выхода.

2 Дополнительные требования для случаев потери питания можно найти в 11.2.11.

11.6.3 Память интеллектуальных датчиков должна быть защищена от записи, чтобы предотвратить неосторожные изменения, кроме тех случаев, когда надлежащий анализ безопасности (например, анализ опасностей и рисков) позволяет чтение/запись.

Примечание — Этот анализ может учитывать человеческие факторы, такие как неправильное выполнение процедур.

11.7 Интерфейсы

11.7.1 Общие положения

Интерфейсы ПСБ могут включать в себя (но не ограничиваются ими) интерфейсы следующих видов:

- интерфейс(интерфейсы) оператора;
- интерфейс(интерфейсы) обслуживания/разработки;
- коммуникационный(ые) интерфейс(интерфейсы).

11.7.2 Требования к интерфейсу оператора

11.7.2.1 Если интерфейс оператора ПСБ реализуется через интерфейс оператора ОСУП, то должны быть учтены возможные отказы, которые могут произойти в интерфейсе оператора ОСУП.

Примечание — Это включает в себя подготовку планов по реализации упорядоченного безопасного останова в случае полного отказа экранов оператора.

11.7.2.2 При разработке ПСБ следует свести к минимуму необходимость выбора оператором опций и способов байпаса системы при наличии опасностей. Если проект действительно предусматривает определенные действия оператора, то в проект должны быть включены средства защиты от ошибок оператора.

Примечание — Если оператор должен выбрать конкретное действие, следует предусматривать шаг его подтверждения.

11.7.2.3 Доступ к переключателям или средствам обеспечения байпаса должен быть защищен (например, ключами или паролями, используемыми в комбинации с эффективными средствами управления), чтобы предотвратить несанкционированное использование этой возможности.

Примечание — Можно также рассмотреть возможность установки ограничений на байпас по времени и числу байпасов, которые могут быть активными в любой момент времени.

11.7.2.4 Информация о состоянии ПСБ, которая важна для поддержки ФБ ПСБ, должна быть доступна оператору и представлена в его интерфейсе. Эта информация может включать:

- сведения о состоянии, в котором находится процесс;
- индикацию защитных действий, выполненных ПСБ;
- индикацию того, что функция защиты не сработала;
- индикацию автоматических действий, таких как деградация при голосовании и/или трактовка происшедших ошибок;
- состояние датчиков и исполнительных элементов;
- потерю электропитания, если она влияет на безопасность;

- результаты диагностики;
- сведения об отказе оборудования кондиционирования окружающей среды, если оно необходимо для обеспечения работы ПСБ.

11.7.2.5 Проект интерфейса оператора ПСБ (см. 11.7.2.7) должен быть таким, чтобы предотвратить изменения прикладной программы ПСБ.

11.7.2.6 Если информация передается из ОСУП в ПСБ, то следует использовать системы, оборудование или процедуры, чтобы подтвердить, что была передана корректная информация и полнота безопасности ПСБ не пострадала.

Примечание — Используемые системы, оборудование и процедуры могут включать в себя управление селективной записью из ОСУП в специальные переменные ПСБ.

11.7.2.7 Проект интерфейса оператора ПСБ через интерфейс оператора ОСУП должен быть таким, чтобы передача неверной информации или данных из ОСУП в ПСБ не привела к ухудшению безопасности.

11.7.3 Требования к интерфейсу обслуживания/разработки

11.7.3.1 Проект интерфейса обслуживания/разработки ПСБ должен гарантировать, что любой отказ такого интерфейса не должен неблагоприятно влиять на способность ПСБ выполнять требующиеся ФБ ПСБ функции. Для этого может потребоваться отсоединить интерфейсы обслуживания/разработки (например, панели программирования) во время нормального функционирования ПСБ.

11.7.3.2 Интерфейс обслуживания/разработки должен обеспечивать выполнение следующих функций, обеспечивая защиту доступу к каждой:

- рабочий режим, программа, данные, средства отключения сигнализации, тестирование, байпас, обслуживание ПСБ;
- диагностика, голосование и разбор ошибки ПСБ;
- добавление, удаление или модификация прикладной программы;
- данные, необходимые для поиска неисправностей в ПСБ;
- байпасы, где они требуются, должны быть установлены так, чтобы сигнализация и средства ручного останова не отключались.

11.7.3.3 Интерфейс обслуживания/разработки не должен быть использован в качестве интерфейса оператора.

11.7.3.4 Предоставление и отключение доступа для чтения-записи должны быть выполнены только в процессе управления конфигурированием, используя интерфейс обслуживания/разработки с соответствующим документированием и мерами защиты, такими как аутентификация и защищенные каналы пользователя.

11.7.4 Требования к коммуникационным интерфейсам

11.7.4.1 Проект коммуникационного интерфейса ПСБ должен гарантировать, что любой отказ такого интерфейса не будет вредно влиять на способность ПСБ удерживать процесс в безопасном состоянии.

11.7.4.2 Если ПСБ обменивается информацией с ОСУП и периферийными устройствами, то коммуникационный интерфейс, ОСУП или периферийные устройства не должны оказывать негативное воздействие на ФБ ПСБ в этой ПСБ.

11.7.4.3 Коммуникационный интерфейс должен быть достаточно устойчив к электромагнитным помехам, включая скачки напряжения, и не приводить к опасным отказам ПСБ.

11.7.4.4 Коммуникационный интерфейс должен быть пригоден для передачи информации между устройствами, имеющими различные потенциалы заземления.

Примечание — При этом может потребоваться альтернативная физическая среда передачи (например, оптоволокно).

11.8 Требования к проектированию обслуживания или испытаний

11.8.1 Проект должен допускать проведение испытаний ПСБ как в целом (от начала до конца), так и по частям. Если периодичность запланированных остановов процесса превышает интервал между проверочными испытаниями, то следует предусмотреть средства проведения испытаний на действующем объекте.

Примечание — Термин «от начала до конца» означает, что испытания проводят от датчика до исполнительного устройства.

11.8.2 Если требуется проведение проверочных испытаний на действующем объекте, то испытательные средства должны быть неотъемлемой частью проекта ПСБ.

11.8.3 Если в состав ПСБ включены средства для проведения испытаний или байпаса, то она должна отвечать следующим требованиям:

- ПСБ должна быть спроектирована в соответствии с требованиями к техническому обслуживанию и испытаниям, определенными в СТБ;
- оператор должен быть осторожен при использовании обхода любой части ПСБ в случае поступления аварийной сигнализации или выполнения технологического процесса.

11.8.4 Должно быть определено максимальное время, в течение которого ПСБ может находиться в байпасе (для ремонта или испытания), пока продолжается безопасное выполнение процесса.

11.8.5 Когда ПСБ находится в байпасе (для ремонта или испытания), должны предоставляться компенсирующие меры, обеспечивающие непрерывное безопасное выполнение процесса и соответствующие 11.3.

11.8.6 Принудительная установка входов и выходов программируемой электроники ПСБ не должна использоваться в прикладных программах, управляющих процедурах, обслуживании (кроме случаев, отмеченных ниже).

Принудительное воздействие на входы и выходы, за исключением случаев изъятия ПСБ на техническое обслуживание, не допускается без применения дополнительных процедур и защиты доступа. О любом принудительном воздействии в установленном порядке должно быть сделано объявление или должен срабатывать аварийный сигнал.

11.9 Количественная оценка случайного отказа

11.9.1 Расчетная мера отказа каждой ФБ ПСБ должна быть равной или меньше целевой меры отказов, связанной с УПБ, в соответствии с СТБ. Это должно определяться с помощью вычисления.

Примечание — В сложных приложениях частота возникновения опасных событий может использоваться как альтернатива целевым мерам отказов (например, если различные причины запросов имеют различные требования к полноте безопасности или если зависимые ПСБ работают последовательно).

11.9.2 Расчетная мера отказов каждой ФБ ПСБ, вызванных случайными отказами, должна учитывать все влияющие на нее факторы, включая следующее:

a) архитектуру ПСБ и подсистем ПСБ (там, где это имеет значение) в части, связанной с выполнением каждой рассматриваемой ФБ ПСБ;

b) оценку интенсивности отказов, связанную с каждым видом отказов, вызванных случайными отказами аппаратных средств, которые приводят к опасному отказу ПСБ, но выявляются с помощью диагностических проверок;

c) оценку интенсивности отказов, связанную с каждым видом отказов, вызванных случайными отказами аппаратных средств, которые приводят к опасному отказу ПСБ и не выявляются с помощью диагностических проверок, но обнаруживаются с помощью контрольных проверок;

d) оценку интенсивности отказов, связанной с каждым видом отказов, вызванных случайными отказами аппаратных средств, которые приводят к опасному отказу ПСБ, не выявляются с помощью диагностических проверок и не обнаруживаются с помощью контрольных проверок;

e) чувствительность ПСБ к отказам, вызванным самими контрольными проверками;

f) чувствительность ПСБ к отказам по общей причине;

g) охват диагностикой для любого периодического диагностического испытания, а также связанные с ним диагностический интервал и вероятность отказа реализующих его диагностических средств;

h) охват любых периодических контрольных проверок, а также связанные с ними процедура контрольной проверки и безотказность средств проведения контрольных проверок и процедуры;

i) время восстановления для выявленных отказов и состояние ПСБ во время восстановления (в неавтономном или автономном режиме);

j) оценку интенсивности опасных отказов любого процесса передачи данных в любых режимах, способных вызвать опасный отказ ПСБ (как обнаруживаемый, так и не обнаруживаемый диагностическими проверками);

k) оценку вероятности того, что реакция оператора приведет к опасному отказу ПСБ (как обнаруживаемому, так и не обнаруживаемому диагностическими проверками);

l) безотказность любых средств, необходимых для ПСБ.

Примечание — Среди множества доступных подходов к моделированию наиболее подходящий подход выбирает аналитик, и его выбор может зависеть от обстоятельств. Доступные методы включают в себя [см. МЭК 61508-6: 2010 (приложение В)]:

- причинно-следственный анализ;
- блок-схемы надежности;
- анализ дерева отказов;
- модели Маркова;
- модели сетей Петри.

Вероятностные вычисления могут выполняться аналитически или с помощью численного моделирования (например, моделированием методом Монте-Карло).

11.9.3 Данные по безотказности, используемые при количественной оценке влияния случайных отказов, должны быть достоверными, отслеживаемыми, документально оформленными, обоснованными и должны основываться на информации пользователей об эксплуатации похожих устройств, применявшихся в похожей рабочей среде.

Примечания

1 Эти данные включают в себя данные, собранные пользователем, данные от производителя/поставщика/пользователя, полученные из данных, собранных при работе с устройствами, данные из общих баз данных по безотказности, в которых собраны результаты эксплуатации внешних устройств, и т. п. В некоторых случаях для оценки недостающих данных по безотказности или оценивания влияния, оказываемого на данные по безотказности, собранные в разных рабочих средах, может потребоваться инженерная оценка.

2 Нехватка данных по безотказности, отражающих рабочую среду, является часто встречающимся недостатком вероятностных вычислений. Конечные пользователи могут организовать комплекты данных по безотказности для соответствующих устройств согласно МЭК 60300-3-2:2004 или ИСО 14224:2006, чтобы улучшить применение комплекса стандартов МЭК 61511.

3 Данные производителя, основанные на возвращаемой информации, могут быть доступны только ограниченному кругу лиц, обладающих полным знанием о рабочей среде, и полностью документально оформлены в соответствии с МЭК 60300-3-2:2004 или ИСО 14224:2006. Пользователь может также записать информацию о рабочей среде для ФБ ПСБ и должен продемонстрировать соответствие данных о рабочей среде ФБ ПСБ данным о рабочей среде от производителя.

11.9.4 Неопределенности данных по безотказности должны оцениваться и учитываться при вычислении меры отказов.

Примечания

1 Неопределенности данных по безотказности могут быть оценены на основании объема информации об эксплуатации (меньший объем информации об эксплуатации приводит к большей погрешности) и/или на основании экспертного мнения. Опубликованные стандарты (МЭК 60605-4), Байесовский подход, методы инженерной оценки и т. п. могут использоваться для оценки погрешностей данных по безотказности.

2 Для вычисления мер отказов могут применяться следующие методы (дополнительную информацию см. в МЭК 61511-2:2016):

- использовать верхнюю доверительную границу, составляющую 70 %, для каждого входного параметра безотказности вместо его среднего значения, чтобы получить консервативную точечную оценку мер отказов, или
- использовать вероятностные функции распределения для входных параметров безотказности, выполнить моделирование методом Монте-Карло, чтобы получить гистограмму, отображающую распределение меры отказов, и оценить консервативное значение, полученное из этого распределения (например, уверенность в том, что истинная мера отказов точнее, чем вычисленное значение, составляет 90 %).

11.9.5 Если для определенного проекта целевая мера отказов для соответствующей ФБ ПСБ не достигнута, то необходимо:

a) идентифицировать устройства и параметры, вносящие наибольший вклад в меру отказов.

Примечание — В этом случае может быть полезен анализ дерева отказов методом сечения;

b) оценить влияние возможных мер улучшения для определенных устройств или параметров (например, использование более надежных устройств, дополнительных средств защиты от отказов общего вида, повышение охвата диагностикой или контрольными проверками, повышение избыточности, сокращение интервала контрольной проверки, проверки с разнесением по времени и т. д.);

c) выбрать и реализовать меры по улучшению для получения нового результата;

d) сравнить новый результат с целевой мерой отказов и повторять шаги с a) по d) до тех пор, пока консервативным способом не будет достигнута целевая мера отказов.

12 Требования к разработке прикладной программы приборной системы безопасности

12.1 Цель

Целью настоящего раздела является определение требований к разработке прикладной программы.

12.2 Общие требования

12.2.1 Прикладная программа ПСБ должна соответствовать требованиям к безопасности прикладной программы (см. 10.3.3) и всем требованиям настоящего раздела для всех УПБ вплоть до (и включая) УПБ 3.

12.2.2 Программист, разрабатывающий прикладную программу, должен сделать обзор информации в СТБ и ознакомиться с требованиями к безопасности прикладной программы, чтобы гарантировать исчерпывающие, однозначные, понятные и согласованные требования. Любые недостатки в требованиях к безопасности прикладной программы должны быть идентифицированы и разрешены, а если в эти требования вносятся изменения, то необходимо провести анализ их влияния.

12.2.3 Комплекс стандартов МЭК 61511 рассматривает программирование на языках с ограниченной изменчивостью (ЯОИ) и использование устройств, применяющих фиксированные языки программирования (ФЯП). Комплекс стандартов МЭК 61511 не затрагивает язык программирования с полной изменчивостью (ЯПИ), а также комплекс стандартов МЭК 61511 не рассматривает прикладное программирование для УПБ 4. Если функциональные блоки написаны на ЯПИ, то их следует разрабатывать и модифицировать в соответствии с МЭК 61508-3:2010.

12.2.4 Если прикладная программа ПСБ должна осуществлять и функции безопасности, и функции, не связанные с безопасностью, то все составляющие прикладной программы должны рассматриваться как часть ПСБ и быть выполнены в соответствии с требованиями настоящего стандарта, а также с помощью оценки и испытания должно быть показано, что функции, не связанные с безопасностью, не могут причинять вред функции безопасности.

12.2.5 Прикладная программа должна быть спроектирована таким образом, чтобы она обеспечивала сохранение процесса в безопасном состоянии после того, как ПСБ переведет процесс в это состояние, включая условия потери питания и восстановления питания, и до тех пор, пока не будет инициирована установка в исходное состояние, если в соответствии с СТБ не должно выполняться обратное.

Примечания

1 Если ФБ ПСБ не обладает функцией установки в исходное состояние, то в документально оформленном техническом обосновании необходимо рассмотреть допустимость повторной инициации процесса без необходимой его задержки в безопасном состоянии, определяемой функцией установки в исходное состояние.

2 Дополнительную информацию см. в 11.2.7.

12.2.6 Во время запуска ПСБ (или включения питания) прикладная программа должна гарантировать, что выходы безопасности остаются в безопасном состоянии (как правило, это состояние с отключенным электропитанием) до тех пор, пока не будет инициирована установка в исходное состояние, если в соответствии с СТБ не должно выполняться другое действие.

12.2.7 Прикладная программа должна быть спроектирована таким образом, чтобы все компоненты прикладной программы выполнялись при каждом сканировании прикладной программы, если не существует конкретного альтернативного требования, представленного в руководстве по безопасности. При определении требований к сканированию прикладной программы следует учитывать требования к времени безопасности процесса.

12.2.8 Для прикладных программ и данных ПСБ должна быть возможность осуществлять процедуры их модификации, управления изменениями, управления версиями, резервирования и восстановления.

12.2.9 В прикладной программе устанавливаются требования к прикладному программированию для пользователей и специалистов по интеграции ПСБ. В частности, указываются требования:

- к стадиям жизненного цикла системы безопасности и действиям, которые должны быть выполнены в процессе проектирования и разработки прикладной программы. Эти требования включают применение мер и методов, которые предназначены для предотвращения ошибок в прикладной программе и для управления возможными отказами;

- информации о подтверждении соответствия прикладной программы, передаваемой организации, выполняющей интеграцию ПСБ;
- подготовке информации и процедур для прикладных программ, необходимых пользователям для эксплуатации и технического обслуживания ПСБ;
- процедурам и спецификациям, по которым должны работать организации, выполняющие модификации прикладных программ.

12.3 Проектирование прикладных программ

12.3.1 Проект прикладной программы должен рассматривать всю логику ПСБ, включая все режимы работы процесса для каждой ФБ ПСБ.

12.3.2 Входная информация для проекта прикладной программы должна включать в себя СТБ вместе с требованиями к прикладной программе (см. раздел 10), архитектуру ПСБ (см. раздел 11), а также средства и инструменты для разработки проекта прикладной программы (см. 12.6). Проект прикладной программы должен согласовываться с СТБ, и его обратная связь с СТБ должна прослеживаться.

12.3.3 Проект прикладной программы должен позволять проводить оценку функциональной безопасности.

12.3.4 При проектировании прикладной программы и разбиении ее на модули (если требуется) необходимо рассмотреть, как будут реализовываться требования, включая следующие (там, где необходимо):

- функции, которые позволяют процессу достигать безопасного состояния или поддерживать его;
- спецификация всех установленных компонентов прикладной программы и описание связей и взаимодействий между установленными компонентами;
- ограничения по времени, связанные с функциями прикладной программы, и их реализация с учетом времени сканирования программы;
- подробное описание используемых стандартных библиотечных модулей (функциональных блоков);
- подробное описание используемых модулей, ориентированных на конкретное приложение (функциональных блоков);
- описание способа, которым было выполнено распределение памяти;
- список используемых глобальных переменных и то, каким образом защищается их целостность;
- идентификация всех функций, не являющихся ФБ ПСБ, и интерфейсов к частям прикладной программы, не связанным с безопасностью, для обеспечения того, что они не могут повлиять на надлежащую работу ФБ ПСБ;
- определение интерфейсов ввода и вывода, включая списки тегов и связанные с ними типы данных;
- подробное описание данных, которыми обмениваются прикладная программа ПСБ и интерфейсы оператора;
- подробное описание данных, которыми обмениваются прикладная программа ПСБ и ОСУП вместе с периферийными устройствами, такими как принтеры, хранилище данных и т. п.;
- способ, которым осуществляется обработка и регистрация внутренней и внешней диагностической информации;
- подробное описание того, как реализуются интерфейсы эксплуатации и обслуживания, включая то, каким образом устанавливаются приоритеты, осуществляется индикация и принятие аварийных сигналов;
- подробное описание любой диагностики на уровне приложения, которая может быть реализована, например внешние сторожевые таймеры, проверка целостности данных приложения, подтверждение соответствия датчика требующемуся УПБ;
- проверки конфигурации системы, включая наличие и доступность ожидаемых устройств аппаратных средств и модулей ПО;
- то, каким образом минимизируется сложность проекта прикладной программы, например, используя модульное проектирование и простую функциональность;
- функции, связанные с обнаружением, визуальной индикацией и управлением сбоями в подсистемах ПСБ;
- функции, связанные с периодическим тестированием ФБ ПСБ при действующем процессе;
- функции, связанные с периодическим тестированием ФБ ПСБ в автономном режиме;

- функции, обеспечивающие безопасное выполнение обслуживания ПСБ;
- ссылки на документы, на которых основывается спецификация проекта прикладной программы.

12.3.5 Проект прикладной программы должен обеспечивать:

- полноту реализации СТБ и предназначенной цели;
- корректность реализации СТБ и предназначенной цели;
- отсутствие неоднозначности, т. е. проект должен быть понятен тем, кто будет использовать документ на любой стадии жизненного цикла ПСБ, что включает использование терминов и описаний, которые однозначны и легко понятны операторам объекта и специалистам по обслуживанию системы, а также прикладным программистам;
- отсутствие ошибок проектирования.

12.4 Реализация прикладной программы

12.4.1 Методология разработки прикладной программы должна соответствовать инструментальным средствам разработки и ограничениям, заданным изготовителем ПЭ подсистемы ПСБ, на которой должна использоваться прикладная программа.

12.4.2 Документация на прикладную программу (или другая связанная с ней документация) должна содержать, как минимум, информацию по следующим вопросам:

a) создатель прикладной программы;

b) описание цели прикладной программы;

c) версии используемых инструкций по безопасности;

d) идентификация и зависимость каждой ФБ ПСБ от частей (модулей) прикладной программы;

e) прослеживаемость связи со спецификацией требований к безопасности прикладной программы;

f) идентификация каждой ФБ ПСБ и ее УПБ;

g) идентификация и описание используемых символов, включая условные обозначения логики, стандартные библиотечные функции, прикладные библиотечные функции;

h) идентификация сигналов ввода и вывода логического устройства ПСБ;

i) если ПСБ целиком использует коммуникации, то описание информационного потока коммуникаций.

Примечание — Примером может служить ПСБ, использующая несколько логических устройств;

j) описание структуры программы, включая описание порядка логической обработки данных по отношению к подсистемам ввода/вывода и любые ограничения, вызванные временами сканирования;

k) если требуется в СТБ, то средства, с помощью которых:

- обеспечивается корректность данных внешних устройств, (например, сравнение между аналоговыми датчиками для повышения охвата диагностикой),
- обеспечивается корректность данных, посылаемых по коммуникационному каналу (например, при коммуникациях, осуществляемых через ЧМИ, перед передачей реализации команды «ack» или «acknowledge»),
- обеспечивается защита коммуникаций (например, меры киберзащиты);

l) идентификация версий и история изменений.

12.4.3 Если ранее разработанные библиотечные функции прикладной программы будут использоваться как часть проекта, то их пригодность для этого должна быть обоснована и должна основываться на:

- соответствии МЭК 61508; если оценивание проверкой в эксплуатации при использовании ЯПИ выполнено в соответствии с МЭК 61508-3:2010, то программируемые устройства, на которых выполняются библиотечные функции прикладной программы, должны также подвергнуться оцениванию проверкой в эксплуатации в соответствии с МЭК 61508-2:2010; или
- соответствии требованиям к предыдущему использованию в МЭК 61511 (см. 11.5.4 или 11.5.5) при использовании ЯПИ или ЯОИ;
- демонстрации того, что любые неиспользуемые функции не оказывают негативного влияния на прикладную программу во всех случаях.

12.4.4 Прикладная программа должна быть создана структурированным образом, чтобы добиться:

- разбиения функционала на модули;
- обеспечения минимальной сложности прикладной программы ФБ ПСБ, соответствующей сложности, требующейся ФБ ПСБ;
- возможности испытания функционала (включая свойства, обеспечивающие отказоустойчивость) и внутренней структуры прикладной программы;

- прослеживаемости и объяснения ее связи с прикладными функциями и связанными с ними ограничениями;

- отображения «один к одному» между архитектурой аппаратных средств и архитектурой прикладной программы.

12.5 Требования к верификации прикладной программы (проверка и тестирование)

12.5.1 Планирование верификации должно выполняться в соответствии с требованиями раздела 7.

12.5.2 Прикладная программа, включая ее документацию, должна быть подвергнута проверке компетентным лицом, не вовлеченным в начальную разработку. Подход к проверке и ее результаты должны быть документально оформлены.

12.5.3 Прикладная программа, включая ее разбиение на модули (если это необходимо), должна быть верифицирована с помощью методов проверки, анализа, моделирования и тестирования с использованием документально оформленных процедур и спецификаций для тестирования, которые должны быть выполнены, чтобы подтвердить, что функции прикладной программы соответствуют СТБ, а также то, что непредназначенные ей функции не выполняются и какие-либо непредназначенные побочные эффекты по отношению к ФБ ПСБ отсутствуют. Следует рассмотреть следующие положения:

- соответствие спецификации проекта прикладной программы, заданные меры и процедуры, а также требования к планированию подтверждения соответствия безопасности и тестирования;

- испытание всех частей прикладной программы;

- испытание типичного диапазона условий данных;

- тестирование для обнаружения условий отказов (т. е. негативное тестирование);

- синхронизацию и последовательность выполнения;

- тестирование коммуникаций от ПСБ и к ПСБ.

Примечание — Везде, где выполняются коммуникации, должно быть проверено и протестировано условие их перегрузки;

- интеграцию автономной прикладной программы с аппаратными средствами логического устройства и его ПЭ;

- проверки внутренних потоков данных для подтверждения того, что логическое устройство не только работает, но и работает, как и предполагалось;

- когда возможно, интеграцию прикладной программы с устройствами третьей стороны.

12.5.4 Отображение данных ввода/вывода на прикладную программу, включая типы данных и их диапазон, должно подвергаться верификации.

12.5.5 Во время тестирования модификации прикладной программы должны подвергаться анализу оказанного на них влияния, чтобы определить:

- все части прикладной программы, на которые повлияли модификации;

- необходимые действия для перепроектирования и повторной верификации.

12.5.6 Результаты тестирования прикладной программы должны быть документально оформлены и должны включать:

- результаты тестирования версий прикладной программы и поддерживаемую их документацию;

- версии поддерживающего ПО и инструментов тестирования;

- имя(имена) лица(лиц), выполнявшего(их) тестирование и проверки вместе с датами их проведения;

- описания выполненных тестов, проверок и дат их проведения;

- результаты тестирования;

- информацию о том, были достигнуты цель и критерии тестирования или нет;

- если во время тестирования произошел отказ, то должны быть указаны причины отказа, выполнен его анализ, а также сделаны записи мер по устранению отказа и требований к повторному тестированию.

12.6 Требования к методологии и инструментальным средствам разработки прикладной программы

12.6.1 Разработка прикладной программы должна соответствовать ограничениям, указанным в применяемой(ых) инструкции(ях) по безопасности.

Примечание — Необходимо провести проверку инструкции(ий) по безопасности, и если это требуется для конкретного приложения, могут быть реализованы дополнительные процедуры и/или ограничения для использования методологий и инструментальных средств.

12.6.2 Методы, методики и инструментальные средства следует выбирать и применять для каждой стадии жизненного цикла так, чтобы:

- минимизировать риск появления ошибок в прикладной программе;
- выявлять и устранять ошибки, которые уже существуют в прикладной программе;
- обеспечивать настолько, насколько это практически возможно, чтобы любые ошибки, остающиеся в прикладной программе, не приводили к неприемлемым результатам;
- улучшить средства управления модификациями прикладной программы на протяжении жизненного цикла ПСБ;
- предоставить свидетельства того, что прикладная программа обладает требуемым уровнем качества.

13 Заводские приемочные испытания

13.1 Цель

Целью настоящего раздела является проведение испытаний устройств ПСБ для обеспечения соответствия требованиям, определенным в СТБ.

Примечания

1 Путем испытаний логического устройства с соответствующим программным обеспечением и аппаратными средствами, проведенных перед их установкой на объекте, можно легко выявить и скорректировать ошибки.

2 Заводские приемочные испытания (ЗПИ) иногда называются комплексными или интеграционными испытаниями, и они могут быть частью подтверждения соответствия.

3 Тестирование внешних элементов вместе с логическим решающим устройством может быть рекомендовано для случаев, когда до окончательной установки необходимо быть уверенным в том, что функционирование будет осуществляться надлежащим образом, например для работы под водой.

13.2 Рекомендации

13.2.1 Необходимость проведения ЗПИ следует определить на стадии планирования обеспечения безопасности проекта.

Примечания

1 Для разработки интеграционных тестов может требоваться тесное сотрудничество между поставщиком логического устройства и проектирующим его подрядчиком.

2 ЗПИ следуют за стадиями проектирования и разработки, но предшествуют установке и вводу в действие.

3 ЗПИ применимы к подсистемам ПСБ, использующим как программируемые, так и непрограммируемые электронные изделия.

4 Обычно ЗПИ проводят в заводских условиях до установки и ввода в действие на объекте.

13.2.2 При планировании проведения ЗПИ должно устанавливаться следующее:

- типы проводимых испытаний, в том числе: функциональные испытания системы как «черного ящика»; испытания для оценки рабочих характеристик; испытания на воздействие окружающей среды; проверки интерфейсов; испытания в режимах отказов и/или деградации; испытания исключительных ситуаций; испытание безопасной реакции в случае отказа подачи питания (включая перезапуск после восстановления подачи питания); проверки применимости инструкций по эксплуатации и обслуживанию ПСБ.

Примечания

1 Функциональные испытания системы как «черного ящика» выполняется методом разработки испытаний, при котором система рассматривается как «черный ящик», без явного использования знания о ее внутренней структуре. Разработка испытаний в методе «черного ящика» обычно концентрирует внимание на требованиях к испытываемым функциям. Синонимами испытаний по методу «черного ящика» являются поведенческие и функциональные испытания, а также испытания методом непрозрачного или закрытого ящика.

2 Испытания для оценки рабочих характеристик определяют, соответствует ли система требованиям к синхронизации, безотказности и готовности, полноте, а также целевым значениям и ограничениям системы безопасности.

3 Испытания на воздействие окружающей среды включают ЭМС, испытания в реальных условиях эксплуатации и в «стрессовых» условиях.

4 Внутренние проверки потоков данных могут выполняться для подтверждения того, что ПСБ обрабатывает входные данные и генерирует выходную реакцию как специфицировано;

- сценарии испытаний, описание и данные испытаний.

Примечание — Очень важно добиться ясности в том, кто отвечает за разработку сценария испытаний, а кто — за их проведение и удостоверение;

- зависимость от других систем и/или интерфейсов;
- окружающие внешние условия и средства проведения испытаний;
- конфигурация логического устройства, датчика и исполнительного элемента;
- критерий принятия решения о прохождении испытаний;
- процедуры корректирующих действий при появлении отказа в процессе испытаний;
- компетентность персонала, выполняющего испытание;
- физическое размещение;
- опасности, возникающие в результате выполнения испытания, в частности связанные с накопленной энергией;
- ясная диаграмма схемы проведения испытания;
- записи выполненных испытаний, данных, результатов и наблюдений, выполняемые во время проведения испытаний.

Примечание — Для испытаний, которые не могут быть физически продемонстрированы, обычно допускается привести формальное рассуждение, доказывающее, что ПСБ отвечает требованиям, целям и ограничениям.

13.2.3 ЗПИ следует проводить на установленной версии логического устройства.

13.2.4 ЗПИ следует проводить в соответствии с планом ЗПИ. Такие испытания должны показать, что вся логика выполняется правильно.

13.2.5 Для каждого проводимого испытания следует указывать:
- используемую версию плана испытаний;
- ФБ ПСБ и рабочую характеристику, проверяемую в данном испытании;
- подробные процедуры и описание испытания;
- хронологический отчет действий по испытанию;
- используемые инструментальные средства, оборудование и интерфейсы.

13.2.6 По результатам ЗПИ следует подготовить документ, фиксирующий:
a) постановку задачи испытаний;
b) результаты испытаний и
c) были ли выполнены цели и критерий прохождения испытаний.

Если в ходе испытаний были отказы, то следует документировать их причины, провести анализ отказов и соответствующие корректирующие действия.

13.2.7 Любые модификации или изменения, проводимые в течение ЗПИ, следует подвергать анализу на безопасность, позволяющему определить:
- степень их влияния на каждую ФБ ПСБ и
- объем испытаний и верификаций, который должен быть установлен и выполнен.

Примечание — В зависимости от результатов ЗПИ приемка может быть начата до завершения корректирующих действий.

14 Установка и ввод в действие приборной системы безопасности

14.1 Цели

Цели требований настоящего раздела состоят в том, чтобы обеспечить:
- установку ПСБ согласно спецификациям и конструкторской документации;
- ввод в действие ПСБ так, чтобы она была готова к заключительному подтверждению соответствия.

Примечание — Целью деятельности по вводу в эксплуатацию в соответствии с требованиями стадии проектирования является обеспечение того, что каждое из устройств ПСБ индивидуально готово функционировать.

14.2 Требования

14.2.1 Планирование установки и ввода в действие должно определить все действия, требуемые для установки и ввода в действие, и обеспечить следующее:
- действия по установке и вводу в действие;
- процедуры, показатели и приемы, используемые при установке и вводе в действие;
- указания, когда эти действия следует проводить;
- перечень лиц, подразделений и организаций, ответственных за эти действия.

План установки и ввода в действие может быть при необходимости включен в общий план проекта.

14.2.2 Все устройства ПСБ должны быть установлены правильно, в соответствии с проектом и планами установки (см. 14.2.1).

14.2.3 ПСБ должна быть введена в действие в соответствии с планом подготовки к заключительному подтверждению соответствия системы. Мероприятия по вводу в действие должны включать следующие проверки, но не ограничиваться ими:

- заземление подсоединено правильно;
- источники питания подсоединены правильно и включены;
- транспортировочные фиксаторы и упаковочные материалы удалены;
- какие-либо физические опасности отсутствуют;
- все приборы прокалиброваны;
- все внешние устройства находятся в рабочем состоянии;
- логические устройства и устройства ввода/вывода включены;
- интерфейсы с другими системами и периферийными устройствами включены;
- все коммуникации между удаленными системами ПСБ работают нормально.

14.2.4 Следует вести соответствующие записи мероприятий по вводу в действие ПСБ, фиксируя результаты деятельности, и выполнены ли цели и критерии, установленные на стадии проектирования ПСБ. Если наблюдались отказы, их причины должны быть записаны.

14.2.5 В том случае, если будет обнаружено, что реально выполненная установка не соответствует данным проекта, следует получить оценку таких отклонений, сделанную компетентным лицом, и определить их вероятное влияние на безопасность. Если будет установлено, что отклонения не влияют на безопасность, информация проекта должна быть дополнена статусом «как выполнено». Если отклонения оказывают отрицательное влияние на безопасность, то установка должна быть модифицирована так, чтобы она соответствовала требованиям проекта.

15 Подтверждение соответствия безопасности приборной системы безопасности

15.1 Цель

Цель требований настоящего раздела состоит в том, чтобы путем осмотра и испытаний можно было проверить, что установленная и введенная в эксплуатацию ПСБ и связанные с ней ФБ ПСБ соответствуют требованиям, установленным в СТБ.

Примечание — Иногда такое подтверждение соответствия называют приемными испытаниями на объекте (ПИО).

15.2 Требования

15.2.1 Планирование подтверждения соответствия ПСБ должно выполняться на протяжении всего жизненного цикла ПСБ и определить все действия и оборудование, требуемые для проведения подтверждения соответствия, среди которых должны быть:

- действия, связанные с подтверждением соответствия всех ПСБ спецификации требований к безопасности, включая реализацию и принятие решений по итоговым рекомендациям;
- подтверждение соответствия всех соответствующих режимов работы процесса и связанного с ним оборудования, включая подтверждение соответствия:
  - режима подготовки к использованию, в том числе наладку и настройку,
  - режима пуска, автоматического, ручного, полуавтоматического и стационарного,
  - режима переналадки, останова, обслуживания,
  - других режимов, установленных на предыдущих стадиях жизненного цикла ПСБ;
- процедуры, меры и методики, используемые для подтверждения соответствия, включая то, каким образом могут выполняться действия по подтверждению соответствия без риска опасных событий (от которых должна защищать ПСБ) для объекта и процесса;
- время выполнения действий по подтверждению соответствия;
- лица, подразделения и организации, ответственные за эти действия, и уровни их независимости для действий при подтверждении соответствия;

- ссылки к информации, с учетом которой должно быть выполнено подтверждение соответствия (например, причинно-следственная диаграмма);

- оборудование и средства обеспечения, которые необходимо установить или сделать доступными (например, отсечные клапаны и оборудование обнаружения утечки, которое потребуется для испытаний клапанов).

Примечание — Примерами действий по подтверждению соответствия могут служить испытания в замкнутом контуре, испытания логики, процедуры калибровки, моделирование работы прикладной программы.

15.2.2 Планирование подтверждения соответствия безопасности для прикладной программы должно включать:

- идентификацию функций прикладной программы, для которой должна быть проведена процедура подтверждения соответствия, для каждого режима работы процесса до начала ввода в действие;

- техническую стратегию для подтверждения соответствия, включая (где это важно) информацию:
  - о ручных и автоматических методах,
  - статических и динамических методах,
  - аналитических и статистических методах;

- меры (методики) и процедуры, соответствующие предыдущему перечислению, которые должны использоваться для подтверждения того, что каждая ФБ ПСБ соответствует установленным требованиям к безопасности и указанному УПБ;

- требуемое окружение, при котором проводят испытания на подтверждение соответствия (например, средства калибровки и испытательное оборудование);

- прикладную программу;

- критерии положительного/отрицательного результата выполнения подтверждения соответствия должны включать:
  - необходимые входные сигналы для процесса и оператора, включая их последовательности и значения,
  - предполагаемые выходные сигналы, включая их последовательность и значения, и
  - другие критерии приемки, например использование памяти, временные допуски и допуски значений;

- политику и процедуры, используемые для оценки результатов подтверждения соответствия, в особенности при оценке отказов;

- все документы (см. раздел 19) проходят подтверждение соответствия для повышения точности, согласованности и чтобы было возможно проследить ФБ ПСБ от ее создания во время анализа опасностей и рисков до финальной установки ФБ ПСБ.

15.2.3 Если для подтверждения соответствия требуется провести проверку точности измерений, тогда используемые для этой функции приборы должны быть прокалиброваны с использованием поддерживаемых эталонов общего применения. Если такая калибровка не очевидна, то должен использоваться альтернативный метод, что должно быть документально оформлено.

15.2.4 Подтверждение соответствия ПСБ и связанных с ней ФБ ПСБ должно проводиться в соответствии с планом подтверждения соответствия ПСБ. Действия, связанные с подтверждением соответствия, должны включать, но этим не ограничиваться, следующее:

- подтверждение того, что ПСБ работает в обычных и необычных режимах (например, при пуске или останове) так, как это установлено в СТБ;

- подтверждение того, что неблагоприятное взаимодействие ОСУП с другими подключенными системами не затрагивает правильного функционирования ПСБ;

- ПСБ должным образом обменивается информацией (если это требуется) с ОСУП или с любой другой системой или с сетью, включая ненормальные условия, такие как перегрузка данными;

- датчики, логические устройства и исполнительные элементы, включая все каналы с резервированием и ненормальные условия работы, такие как перегрузка данными, работают в соответствии с СТБ.

Примечание — Если логическое устройство проходило ЗПИ, как это описано в разделе 13, то можно доверять полученным в процессе ЗПИ результатам подтверждения соответствия. После установки всего оборудования на объекте функциональность логического устройства и его соединения с подсистемами ПСБ будет проверена с помощью подтверждения соответствия всего контура;

- документация на ПСБ соответствует установленной системе;

- подтверждение того, что ФБ ПСБ при недопустимых значениях переменных процесса (например, при значениях вне заданного диапазона) выполняется, как и было установлено;

- последовательность останова выполняется правильно;
- ПСБ обеспечивает выдачу надлежащих сообщений и их надлежащее представление на дисплее;
- вычисления, порученные ПСБ, выполняются правильно для заданного диапазона значений, но также для самих граничных значений и за их пределами;
- функции установки ПСБ в исходное состояние выполняются так, как установлено в СТБ;
- функции байпаса (обхода) выполняются правильно;
- пусковые перенастройки ведутся правильно;
- системы ручного останова работают правильно;
- политика для контрольных испытаний зафиксирована в документации на процедуры обслуживания;
- функции сигнализации результатов диагностики выполняются, как это требуется;
- подтверждение того, что при потере ресурса (например, электрического питания, воздуха, гидравлики) ПСБ выполняет все действия в соответствии с требованиями и что после восстановления ресурса она возвращается в желательное состояние;
- подтверждение того, что устойчивость к электромагнитным помехам, соответствующая спецификации требований по безопасности (см. 10.3), достигнута.

15.2.5 Подтверждение соответствия прикладной программы должно показывать, что:

- все установленные требования по безопасности прикладной программы (см. 10.3.2) выполняются правильно;
- прикладная программа не ставит под угрозу выполнение требований безопасности в условиях сбоя в ПСБ, при режимах с деградацией, а также для условий сбоя ОСУП и для любых интерфейсов между ПСБ и ОСУП;
- прикладная программа не ставит под угрозу выполнение требований безопасности путем выполнения «неиспользуемых» функций ПО, т. е. не установленных в спецификации.

Информация о действиях по подтверждению соответствия должна быть доступной.

15.2.6 Результаты деятельности по плану подтверждения соответствия должны охватывать весь процесс подтверждения соответствия ПСБ. Должна быть произведена документация по подтверждению соответствия ПСБ, содержащая следующие данные:

- использованная версия плана проведения подтверждения соответствия ПСБ;
- испытуемая (или оцениваемая) ФБ ПСБ вместе с конкретными ссылками на требования, установленные в ходе планирования проведения подтверждения соответствия ПСБ;
- использованные средства и оборудование вместе с данными калибровки;
- результаты каждого испытания;
- использованная версия требований к испытаниям;
- критерии прохождения завершенных испытаний;
- испытуемая версия аппаратных средств, прикладных программ и другого испытуемого ПО ПСБ;
- любое несоответствие между ожидаемыми и действительными результатами и меры разрешения этого несоответствия;
- проведенный анализ и принятые решения по вопросу, следует ли при обнаружении расхождений продолжать испытания или выпустить запрос на изменение.

15.2.7 Должна быть проведена верификация результатов путем сравнения их с ожидаемыми результатами. Все несоответствия должны быть проанализированы, а обнаруженные должны быть описаны в документации по подтверждению соответствия. В этой документации должны быть представлены проведенные анализы и решения, принятые решения о продолжении подтверждения соответствия или о запросе на разрешение изменения и возвращении на более раннюю стадию жизненного цикла разработки.

15.2.8 После подтверждения соответствия ПСБ и до появления установленных опасностей необходимо выполнить следующие операции:

- все функции байпаса (например, выполняемые ПЭ логическим устройством и комплексом ПЭ-датчиков и отключенные аварийные сигналы) должны быть возвращены в их нормальное положение;
- все отсечные клапаны процесса должны быть установлены в положение, соответствующее требованиям и процедурам пуска;
- все материалы, использующиеся при испытаниях (например, жидкости), должны быть удалены;
- все пусконаладочные работы должны быть отменены, и все принудительно настроенные значения программируемого устройства должны быть устранены.

16 Эксплуатация и техническое обслуживание приборной системы безопасности

16.1 Цели

Целями требований настоящего раздела являются:

- обеспечить для каждой ФБ ПСБ поддержание требуемого УПБ в процессе эксплуатации и технического обслуживания системы;
- эксплуатировать и выполнять техническое обслуживание ПСБ так, чтобы поддерживать необходимую полноту безопасности.

16.2 Требования

16.2.1 Необходимо составить план эксплуатации и технического обслуживания ПСБ, который должен содержать сведения по следующим вопросам:

- штатные и нештатные действия по эксплуатации;
- осмотр, контрольные испытания, превентивные и аварийные действия по техническому обслуживанию;
- процедуры, меры и методики, используемые при эксплуатации и техническом обслуживании;
- операционная реакция на сбои и отказы, идентифицированные в ходе диагностики, осмотров или контрольных испытаний;
- проверка адекватности процедур эксплуатации и технического обслуживания;
- когда эти действия должны происходить;
- лица, подразделения и организации, ответственные за эти действия;
- план обслуживания ПСБ.

Примечание — План технического обслуживания ПСБ может содержать различные функции, зависящие от УПБ.

16.2.2 Процедуры эксплуатации и технического обслуживания должны быть разработаны согласно соответствующему плану обеспечения безопасности и поддерживать следующее:

a) штатные методы и процедуры, которые необходимо выполнять, чтобы поддерживать функциональную безопасность ПСБ на проектном уровне;

b) процедуры, применяемые для обеспечения качества и согласованности контрольных проверок, а также обеспечить выполнение надлежащего подтверждения соответствия после замены любого устройства;

c) необходимые меры и ограничения для предотвращения опасных состояний и/или уменьшения последствий опасных событий во время технического обслуживания или эксплуатации (например, дополнительные шаги по сокращению риска, когда система блокируется для выполнения тестирования или технического обслуживания);

d) методы и процедуры, применяемые для испытания диагностики;

e) информацию (которая должна поддерживаться) по интенсивности отказов ПСБ и запросов на срабатывание ПСБ;

f) процедуры для сбора данных, связанных с интенсивностью отказов и параметрами безотказности ПСБ.

Примечание — Сбор и анализ данных по отказам несут в себе множество преимуществ, включая возможное понижения затрат на обслуживание, если интенсивность отказов при работе оказывается значительно ниже предполагаемой во время проектирования. Стоимость реализации новых установок также может быть снижена, так как новые проекты могут основываться на менее консервативных значениях интенсивности отказов;

g) информацию (которая должна поддерживаться), хранящую результаты аудитов и испытаний ПСБ;

h) процедуры технического обслуживания, которые должны быть выполнены после отказов и ошибок, произошедших в ПСБ, включая:

- процедуры диагностики и устранения отказов,
- процедуры повторного подтверждения соответствия,
- требования по ведению регистрации технического обслуживания,
- процедуры отслеживания за выполнением технического обслуживания.

Примечание — Процедуры включают:
- процедуры регистрации отказов;
- процедуры анализа систематических отказов;
- действия, обеспечивающие безопасный останов в случае отказа ОСУП;
- обеспечение надлежащей калибровки и обслуживания тестового оборудования.

16.2.3 Эксплуатационные процедуры должны быть доступны. Компенсационные меры, обеспечивающие непрерывную безопасность в случае отключения или в режиме с ограниченной функциональностью ПСБ при байпасе (для ремонта или тестирования), должны применяться вместе с соответствующими ограничениями (по длительности, параметрам процесса и т. п.). Оператору должна предоставляться информация по процедурам, которые применяются до и во время байпаса, а также по тому, что необходимо сделать перед удалением байпаса, и по максимальному допустимому времени пребывания в состоянии байпаса. Такая информация должна проверяться регулярно.

Примечание — Процедуры эксплуатации и обслуживания могут включать в себя верификацию удаления байпасов после контрольной проверки.

16.2.4 Если в ходе анализа опасностей было установлено, что имеются компенсирующие меры, обеспечивающие адекватное сокращение риска, то должна допускаться непрерывная работа процесса и устройства ПСБ с байпасом. В соответствии с этим должны разрабатываться и эксплуатационные процедуры.

16.2.5 Эксплуатация и обслуживание должны продолжаться в соответствии с соответствующими процедурами.

16.2.6 Операторы должны быть подготовлены к функциям и эксплуатации ПСБ в сфере ее работы. Это обучение должно обеспечить:

- понимание операторами того, как функционирует ПСБ (основные узлы ПСБ и результат их работы).

Примечание — Это может также включать понимание того, как деятельность ПСБ влияет на остальную работу на объекте;

- знание об опасности, от которой защищает ПСБ;
- корректное действие и управление всеми переключателями байпаса/перекрытия и знание обстоятельств, при которых такие байпасы должны использоваться;
- действие каждого из ключей ручного останова и пуска, а также когда такие ключи должны применяться.

Примечание — В состав таких ключей могут входить «установка в исходное состояние системы» и «перезапуск системы»;

- ожидаемую реакцию при срабатывании любых диагностических аварийных сигналов (например, какое действие должно быть предпринято при любом аварийном сигнале ПСБ, обозначающем, что в ПСБ появилась проблема).
- надлежащая верификация диагностики.

16.2.7 Статус всех байпасов должен записываться в журнале байпаса. Все байпасы нуждаются в авторизации и индикации.

16.2.8 Обслуживающий персонал должен быть подготовлен настолько, как это требуется для обеспечения функционирования ПСБ (включая ее аппаратные средства и ПО) с заданным УПБ каждой ФБ ПСБ.

16.2.9 Несоответствия между ожидаемым и фактическим поведением ПСБ должны быть проанализированы и, где необходимо, устранены с помощью модификаций, проведенных так, чтобы поддерживалась требуемая безопасность. Для этого необходимо контролировать:

- интенсивность запросов на срабатывание каждой ФБ ПСБ (см. 5.2.5.3);
- действия, выполняемые при запросе на срабатывание системы;
- отказы и виды отказов оборудования, составляющего часть ПСБ, включая те, что были идентифицированы во время нормальной работы, испытания или запроса к ФБ ПСБ;
- причины запросов;
- причины и частоту ложных срабатываний;
- отказ оборудования, составляющего часть любых компенсирующих мер.

16.2.10 Процедуры эксплуатации и обслуживания в случае необходимости могут потребовать повторного проведения:

- аудита функциональной безопасности;
- испытаний ПСБ;
- сбора информации по опыту работы в нормальных и ненормальных условиях и событиям обслуживания.

16.2.11 Чтобы обнаруживать опасные отказы, не выявленные диагностикой, следует для каждой функции безопасности ПСБ разработать документально оформленные процедуры проверочных испытаний. Такие процедуры должны описывать каждый из шагов, которые должны быть выполнены, и включать проверки:

- правильности работы каждого датчика и исполнительного элемента;
- правильности логических операций;
- правильности выполнения аварийных сигналов и сообщений.

Примечание — Для определения невыявленных отказов могут быть применены следующие методы:
- анализ дерева отказов;
- анализ видов и последствий отказов;
- техническое обслуживание с целью обеспечения безотказности.

16.2.12 Запасные части ПСБ должны быть идентифицированы и подготовлены для минимизации длительности байпаса, которая зависит от неготовности какой-либо части ПСБ для замены.

Примечание — Замены, не являющиеся заменами на идентичный элемент, могут обрабатываться как модификации ПСБ.

16.2.13 Лица, ответственные за эксплуатацию и обслуживание, должны осуществлять проверку анализа опасностей и рисков, распределения и проекта, чтобы обеспечить правильность сделанных заключений, например предположения о сроке использования и защите от коррозии.

16.3 Контрольная проверка и осмотр

16.3.1 Контрольные проверки

16.3.1.1 Для обнаружения необнаруженных отказов, препятствующих ПСБ действовать в соответствии с СТБ, следует, используя документально оформленные процедуры, проводить периодические контрольные проверки.

Примечания

1 Особое внимание можно уделить идентификации причин отказов, которые могут повлечь за собой отказы по общей причине.

2 Программа функциональных испытаний может также предусмотреть потребность в предотвращении внесения отказов по общей причине.

16.3.1.2 Все компоненты ПСБ должны быть проверены, включая датчики, логическое устройство и исполнительные элементы (например, клапаны останова и двигатели).

Примечание — Испытание ПСБ может проводиться либо целиком, либо частями (см. 11.8.1).

16.3.1.3 График контрольных проверок должен быть составлен в соответствии с СТБ. Частота проведения контрольных проверок должна быть определена путем расчета ВОНЗ или ВОЧ в соответствии с 11.9 для ПСБ в том виде, в котором она установлена в рабочую среду.

Примечание — Различные части ПСБ могут потребовать различных интервалов проверок, например логическому устройству может потребоваться интервал, отличающийся от испытательного интервала для датчиков или исполнительных элементов.

16.3.1.4 Любые отклонения, обнаруженные в ходе контрольных проверок, должны быть устранены безопасным способом и своевременно. После завершения устранения контрольные проверки должны быть проведены повторно.

16.3.1.5 Через некоторый период времени, определяемый пользователем, частоту проверок следует вычислять заново с учетом различных факторов, включая накопленные данные проверок, опыт эксплуатации и старение аппаратных средств.

Примечание — Пользователь может настраивать частоту проверок, основываясь на этих данных и анализе того, на чем частота проверок была основана изначально.

16.3.1.6 Любое изменение в прикладной программе требует полного подтверждения соответствия и проведения контрольных проверок любой ФБ ПСБ, на которой сказалось это изменение. Исключения из этого правила допускаются, только если будут проведены соответствующий критический анализ и частичные испытания, подтверждающие, что изменения были спроектированы в соответствии с обновленными требованиями к безопасности и введены правильно.

16.3.1.7 Для анализа отсрочек и предотвращения значительных задержек контрольных проверок должны применяться подходящие процедуры управления.

16.3.2 Осмотр

Каждая ПСБ подлежит периодическому визуальному контролю, чтобы убедиться в отсутствии неразрешенных модификаций и наблюдаемых неисправностей (например, отсутствующие болты или приборные крышки, подвергнутые коррозии кронштейны, неизолированные провода, нарушенные проводники, теплопроводы или изоляция).

Примечание — Эти проблемы могут указывать на повышение частоты сбоев.

16.3.3 Документальное оформление контрольных проверок и осмотров

Пользователь должен выполнять отчеты, удостоверяющие, что контрольные проверки и осмотры были выполнены в соответствии с требованиями. Эти отчеты должны включать, как минимум, следующую информацию:

a) описание выполненных проверок и осмотров, включая идентификацию использованной процедуры испытания;

b) даты проверок и осмотров;

c) фамилии лиц, выполнявших проверки и осмотры;

d) порядковый номер или другой уникальный идентификатор испытуемой системы (например, номер контура, маркера, оборудования и номер ФБ ПСБ);

e) результаты проверок и осмотра, включая условия «как создано», все обнаруженные сбои (включая вид отказа) и условия «как оставлено».

17 Модификация приборной системы безопасности

17.1 Цели

Цели требований настоящего раздела:

- обеспечить, чтобы проведение модификаций любой ПСБ было спланировано надлежащим образом, проверено и утверждено до выполнения изменений; и
- быть уверенным в том, что требуемый уровень полноты безопасности ПСБ сохраняется, несмотря на любые изменения, проведенные в ПСБ.

Примечание — Следует рассмотреть модификации ОСУП, другого оборудования, условий процессов или работы для того, чтобы определить, насколько они повлияют на природу или частоту запросов к ПСБ. Модификации, которые обладают отрицательным влиянием, следует рассмотреть подробнее, чтобы определить, остается ли еще достаточным уровень снижения риска.

17.2 Требования

17.2.1 До выполнения любой модификации ПСБ должны быть выполнены процедуры получения разрешения и управления изменениями.

17.2.2 Указанные процедуры должны включать понятный метод определения и организации выполняемой работы по модификации, а также определять опасности, которые могут появиться.

17.2.3 Перед выполнение какой-либо модификации ПСБ (включая модификации прикладных программ) следует провести анализ влияния предлагаемой модификации на функциональную безопасность. Если анализ показывает, что предлагаемая модификация будет влиять на безопасность, то следует вернуться к самой ранней стадии жизненного цикла ПСБ, затронутой модификацией.

17.2.4 План обеспечения безопасности для модификаций и повторной верификации должен быть доступен. Модификации и повторные верификации должны выполняться в соответствии с планом.

17.2.5 Вся документация, на которую влияют модификации, должна обновляться.

17.2.6 Работы по модификации не должны начинаться перед тем, как в соответствии с 5.2.6.1.9 не будет выполнена ОФБ и не будет получено надлежащее разрешение.

17.2.7 Для всех изменений ПСБ должна быть сформирована соответствующая информация, включающая:

- описание модификации или изменения;
- причину изменения;
- установленные опасности и ФБ ПСБ, на которые могут повлиять изменения;
- анализ влияния работ по модификации ПСБ;
- все разрешения, требуемые для проведения изменений;
- испытания, проверяющие, что изменения проведены надлежащим образом, и ПСБ выполняет свои функции в соответствии с требованиями;
- подробное описание всех действий по модификации ПСБ (например, журнал модификаций);
- соответствующую хронологию конфигурации;
- испытания, проверяющие, что изменения не повлияли неблагоприятно на элементы ПСБ, которые не подлежали модификации.

17.2.8 Модификацию должен проводить квалифицированный персонал, имеющий соответствующую подготовку. Весь персонал, на работу которого эта модификация влияет и который занят ее проведением, должен быть предупрежден и подготовлен к соответствующим изменениям.

18 Снятие с эксплуатации приборной системы безопасности

18.1 Цели

Целями требований настоящего раздела являются:

- обеспечить проведение соответствующего критического анализа и получение необходимого разрешения перед тем, как любая ПСБ будет выведена из эксплуатации;
- обеспечить сохранение работоспособности требуемых ФБ ПСБ в период выполнения действий по выводу из эксплуатации.

18.2 Требования

18.2.1 До выполнения вывода из эксплуатации части или всей ПСБ или ФБ ПСБ следует выполнить процедуры получения разрешения и управления изменениями.

18.2.2 Указанные процедуры должны включать понятный метод определения и организации выполняемой работы по выводу ПСБ из эксплуатации, а также определять опасности, которые могут появиться.

18.2.3 Должен быть проведен анализ того, как предполагаемый вывод системы из эксплуатации влияет на функциональную безопасность. Оценка должна включать в себя обновленный анализ опасностей и рисков, достаточный, чтобы определить области влияния на жизненный цикл ПСБ. Последующие стадии жизненного цикла ПСБ должны быть повторно оценены. При оценке следует также рассмотреть:

- функциональную безопасность во время выполнения действий по выводу системы из эксплуатации и
- влияние вывода ПСБ из эксплуатации на смежные действующие установки и на вспомогательные службы.

18.2.4 Результаты анализа влияний следует использовать при планировании обеспечения безопасности, чтобы повторно применить соответствующие требования комплекса стандартов МЭК 61511, включая повторное проведение верификации и подтверждения соответствия.

18.2.5 Работы по выводу из эксплуатации не должны начинаться до получения надлежащей документации и разрешения.

19 Требования к информации и документации

19.1 Цели

Целью требований настоящего раздела является обеспечение наличия соответствующей документально оформленной информации, чтобы:

- успешно выполнить все стадии жизненного цикла ПСБ;
- сделать возможным успешное проведение верификации, подтверждения соответствия и деятельности по ОФБ.

19.2 Требования

19.2.1 Документация, требования к которой установлены в комплексе стандартов МЭК 61511, должна быть доступна персоналу, реализующему требования комплекса стандартов МЭК 61511.

19.2.2 Документация должна:

- описывать установку, систему или оборудование и их применение;
- быть точной и актуальной;
- быть понятной;
- соответствовать цели, для которой она предназначена, и
- быть доступной в форме, позволяющей ее поддерживать и редактировать, чтобы надлежащие и значимые документы можно было бы просто и точно идентифицировать, найти, получить и переиздать.

Примечание — Дополнительное описание требований к информации включено в разделы 14 и 15.

19.2.3 Документация должна иметь уникальный идентификатор, позволяющий ссылаться на ее различные части.

19.2.4 Документация должна иметь обозначение, указывающее на тип информации.

19.2.5 Документация должна быть пригодна к прослеживанию функциональных требований и требований к полноте безопасности, представленных в настоящем стандарте, включая анализ опасностей и рисков.

19.2.6 Документация должна иметь номер изменения (например, номер версии), позволяющий определить различные версии информации.

19.2.7 Документация должна быть структурирована так, чтобы был возможен поиск необходимой информации. Должна быть возможность доступа к последней версии документа.

Примечание — Физическая структура документации может меняться в зависимости от ряда факторов, таких как размер системы, ее сложность и организационные требования.

19.2.8 Вся соответствующая документация должна быть проверена, отредактирована, пересмотрена, утверждена и находиться под контролем соответствующей схемы управления информацией.

19.2.9 Должна поддерживаться текущая версия документации, содержащая:

a) результаты оценки опасностей и рисков и связанные с ней допущения;

b) описание оборудования, выполняющего ФБ ПСБ, и требования к его безопасности;

c) информацию об организации, отвечающей за поддержание функциональной безопасности;

d) процедуры, необходимые для достижения и поддержания функциональной безопасности ПСБ;

e) информацию о модификации, установленную в 17.2.5;

f) инструкцию(ии) по обеспечению безопасности;

g) информацию о результатах проектирования ПСБ, его реализации, проверки и подтверждения соответствия.

Примечание — Более подробные требования к информации приведены в 12.4.2, разделах 14 и 15, а также в 16.3.3.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1—2012 «Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 1. Общие требования»
IEC 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»
IEC 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»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
- IDT — идентичный стандарт.

УДК 62-783:614.8:331.454:006.354 ОКС 13.110 Т51

Ключевые слова: безопасность функциональная, жизненный цикл систем, промышленные процессы, приборные системы безопасности, планирование функциональной безопасности, жизненный цикл системы безопасности, уровень полноты безопасности

БЗ 11—2017/54

Редактор *Р.Г. Говердовская*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Л.В. Софейчук*

Сдано в набор 09.08.2018. Подписано в печать 27.08.2018. Формат 60 × 84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 8,37. Уч.-изд. л. 7,57.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
gost.e-ecolog.ru gost.e-ecolog.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
123001 Москва, Гранатный пер., 4. www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru