ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61511-1 — 2011

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ. СИСТЕМЫ БЕЗОПАСНОСТИ ПРИБОРНЫЕ ДЛЯ ПРОМЫШЛЕННЫХ ПРОЦЕССОВ

Часть 1

Термины, определения и технические требования

IEC 61511-1:2003
Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements (IDT)

Издание официальное

Москва
Стандартинформ
2013

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

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

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 октября 2011 г. № 468-ст

Настоящий стандарт идентичен международному стандарту МЭК 61511-1:2003 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования» (IEC 61511-1:2003 «Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5).

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

4 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2013

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 . . . 5
3 Сокращения, термины и определения . . . 5
3.1 Сокращения . . . 5
3.2 Термины и определения . . . 6
4 Соответствие настоящему стандарту . . . 18
5 Управление функциональной безопасностью . . . 18
5.1 Цель . . . 18
5.2 Требования . . . 19
6 Требования к жизненному циклу безопасности . . . 23
6.1 Цели . . . 23
6.2 Требования . . . 23
7 Верификация . . . 23
7.1 Цель . . . 23
8 Анализ опасностей и рисков процесса . . . 25
8.1 Цели . . . 25
8.2 Требования . . . 25
9 Распределение функций безопасности по слоям защиты . . . 26
9.1 Цели . . . 26
9.2 Требования к процессу распределения . . . 26
9.3 Дополнительные требования для уровня полноты безопасности 4 . . . 27
9.4 Требования к основной системе управления процессом как к слою защиты . . . 28
9.5 Требования к предотвращению отказов по общей причине, отказов общего типа и зависимых отказов . . . 29
10 Спецификация требований к безопасности ПСБ . . . 29
10.1 Цель . . . 29
10.2 Основные требования . . . 29
10.3 Требования к безопасности ПСБ . . . 29
11 Проектирование и разработка ПСБ . . . 30
11.1 Цель . . . 30
11.2 Основные требования . . . 30
11.3 Требования к поведению системы при обнаружении отказа . . . 31
11.4 Требования к отказоустойчивости аппаратных средств . . . 33
11.5 Требования к выбору компонентов и подсистем . . . 34
11.6 Внешние устройства . . . 37
11.7 Интерфейсы . . . 37
11.8 Требования к проектированию обслуживания или испытаний . . . 39
11.9 Вероятность отказа функции безопасности ПСБ . . . 39
12 Требования к прикладному ПО, включая критерии выбора сервисного ПО . . . 40
12.1 Требования к жизненному циклу безопасности прикладного ПО . . . 40
12.2 Спецификация требований к безопасности ППО . . . 45
12.3 Планирование подтверждения соответствия безопасности ППО . . . 47
12.4 Проектирование и разработка ППО . . . 47
12.5 Интеграция ППО с подсистемой ПСБ . . . 52
12.6 Процедуры модификации ПО на ФЯП и ЯОИ . . . 52
12.7 Верификация ППО . . . 53
13 Заводские приемочные испытания . . . 54
13.1 Цель . . . 54
13.2 Рекомендации . . . 54
14 Установка и ввод в действие ПСБ . . . 55
14.1 Цели . . . 55
14.2 Требования . . . 55
15 Подтверждение соответствия безопасности ПСБ . . . 56

15.1 Цель . . . 56
15.2 Требования . . . 56
16 Эксплуатация и техническое обслуживание ПСБ . . . 58
16.1 Цели . . . 58
16.2 Требования . . . 58
16.3 Проверочные испытания и осмотр . . . 59
17 Модификация ПСБ . . . 60
17.1 Цели . . . 60
17.2 Требования . . . 60
18 Снятие с эксплуатации ПСБ . . . 61
18.1 Цели . . . 61
18.2 Требования . . . 61
19 Требования к информации и документации . . . 61
19.1 Цели . . . 61
19.2 Требования . . . 62
Приложение А (справочное) Различия между стандартами . . . 63
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 64
Библиография . . . 65

Введение

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

Область применения настоящего стандарта — приборные системы безопасности, применяемые в промышленных процессах. Он также устанавливает необходимость проведения оценки опасности и риска процесса для обеспечения формирования спецификации приборных систем безопасности. Вклад других систем безопасности может быть учтен только при рассмотрении требований к эффективности приборных систем безопасности. Приборная система безопасности включает все компоненты и подсистемы, необходимые для выполнения функции безопасности, — от датчика(ов) до исполнительного(ых) элемента(ов).

В основе настоящего стандарта лежат две фундаментальные концепции, необходимые для его применения: концепция жизненного цикла безопасности и концепция уровней полноты безопасности.

Настоящий стандарт рассматривает приборные системы безопасности, использующие электрические/электронные/программируемые электронные технологии. Если для логических устройств используют другие принципы действия, то следует применять основные положения настоящего стандарта. Настоящий стандарт также рассматривает датчики и исполнительные элементы приборной системы безопасности независимо от принципа их действия. Настоящий стандарт является конкретизацией общего подхода к вопросам обеспечения безопасности, представленного в МЭК 61508, для промышленных процессов (см. приложение А).

Настоящий стандарт устанавливает подход, минимизирующий стандартизацию деятельности для всех стадий жизненного цикла безопасности. 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. При необходимости он может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск. Системы защиты основаны на применении различных технологий: химических, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных. Для облегчения применения такого подхода настоящий стандарт:

- требует, чтобы выполнялась оценка опасностей и рисков для определения общих требований к безопасности;
- требует, чтобы выполнялось распределение требований к безопасности в (по) приборной(ым) системе(ам) безопасности;
- реализует подход, который применим ко всем приборным методам обеспечения функциональной безопасности;
- подробно рассматривает применение определенных действий, таких как руководство работами по безопасности, которые могут быть применены ко всем методам обеспечения функциональной безопасности.

Настоящий стандарт по приборным системам безопасности для промышленных процессов:

- охватывает все стадии жизненного цикла безопасности — 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 с ним гармонизированы.

Настоящий стандарт призван привести к высокому уровню согласованности (например, основных принципов, терминологии, информации) в рамках конкретных промышленных процессов. Это принесет преимущества как в плане безопасности, так и в плане экономики.

В пределах своей юрисдикции соответствующие регулирующие органы (например, национальные, федеральные, штата, провинции, округа, города) могут устанавливать требования к проектированию безопасности процесса, к управлению безопасностью процесса или другие требования, которые должны превалировать над требованиями, определенными в настоящем стандарте.

На рисунке 1 представлена общая структура настоящего стандарта.

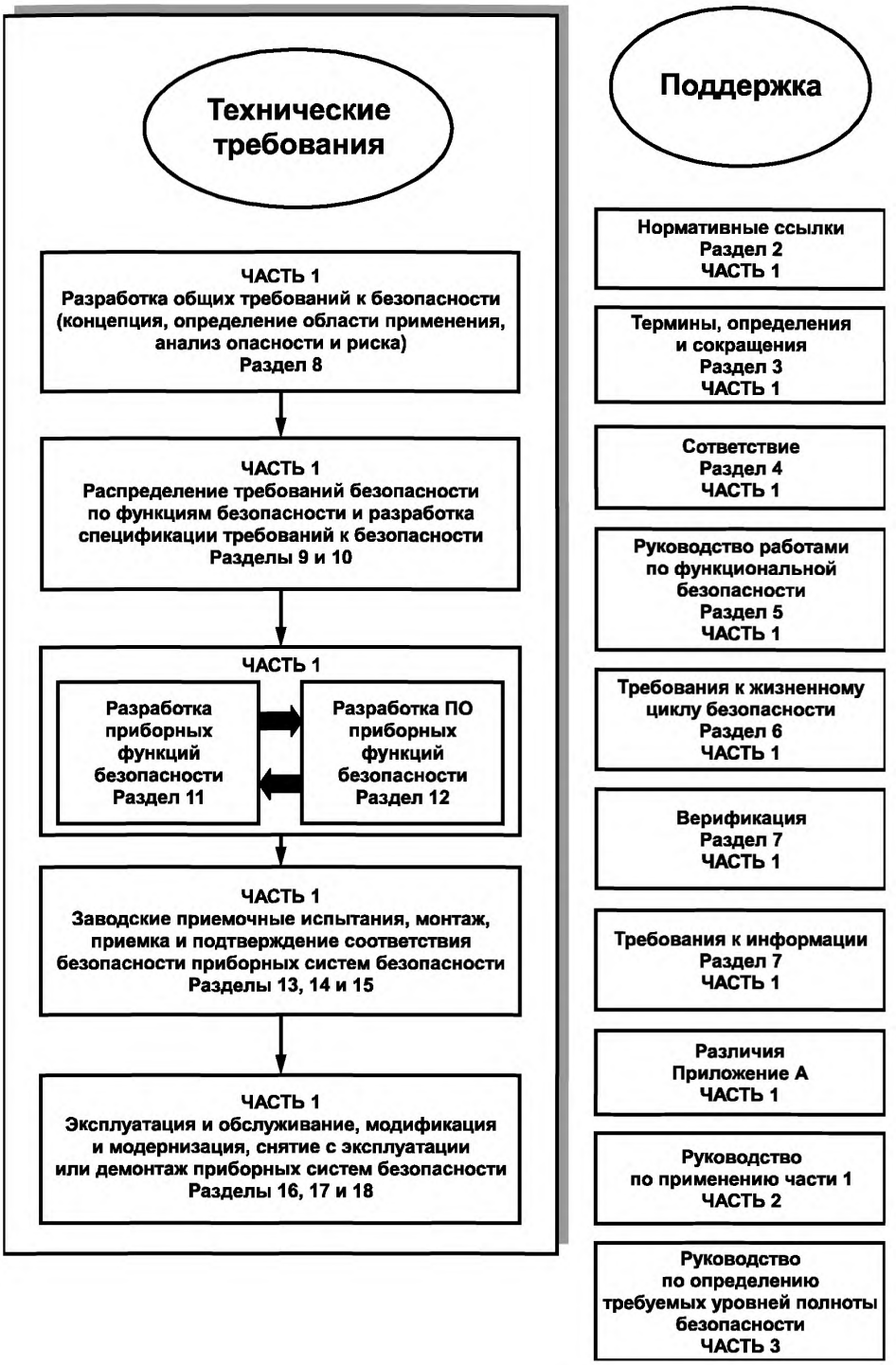


Рисунок 1 — Общая структура настоящего стандарта

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 industrial proceses.
Part 1. Terms, definitions and technical requirements

Дата введения — 2012— 08—01

1 Область применения

1.1 Настоящий стандарт определяет требования к спецификации, проектированию, монтажу, эксплуатации и техническому обслуживанию приборных систем безопасности так, чтобы можно было уверенно удерживать и/или обслуживать конкретный процесс в безопасном состоянии. Настоящий стандарт разработан для внедрения МЭК 61508 в области промышленных процессов.

1.2 В частности, настоящий стандарт:

a) определяет требования к достигаемой 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 и национальному законодательству;

b) распространяется на случаи, когда оборудование, удовлетворяющее требованиям МЭК 61508 или 11.5, применяется в общей системе управления промышленным процессом, но не распространяется на изготовителей, желающих заявить, что их устройства подходят для использования в приборных системах безопасности для промышленных процессов (см. МЭК 61508-2 и МЭК 61508-3);

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

d) применяется в тех случаях, когда прикладное программное обеспечение (ПО) разработано для систем, использующих языки с ограниченной изменчивостью или фиксированные языки, но не применяется к изготовителям, разработчикам приборных системах безопасности, интеграторам и пользователям, разрабатывающим встроенное (системное) ПО либо использующим языки с полной изменчивостью (см. МЭК 61508-3);

e) распространяется на большое количество промышленных процессов различных отраслей промышленности, включая химическую, нефтеперерабатывающую, нефтегазодобывающую, целлюлозно-бумажное производство, неядерную энергетику.

Примечание — Для некоторых промышленных процессов (например, использующихся на морских установках) могут быть установлены дополнительные обязательные требования;

f) определяет отношение между функциями безопасности приборных систем безопасности и другими функциями (см. рисунок 4);

g) определяет функциональные требования и требования к полноте безопасности для функции(й) безопасности приборных систем безопасности, учитывая снижение риска, достигаемое другими средствами;

h) определяет требования к архитектуре системы и конфигурации ее технических средств, прикладного ПО и к системной интеграции;

Издание официальное

i) определяет требования к прикладному ПО, предъявляемые к пользователям и интеграторам приборных системах безопасности (см. раздел 12). В частности, в них должно быть учтено следующее:

- стадии жизненного цикла безопасности и действия, которые должны быть выполнены в процессе проектирования и разработки прикладного ПО (модель жизненного цикла безопасности ПО). Эти требования включают применение мер и методик, которые предназначены для предотвращения ошибок в ПО и управления возможными отказами;

- информация о подтверждении соответствия безопасности ПО, передаваемая организации, выполняющей интеграцию приборных системах безопасности;

- подготовка информации и процедур для ПО, необходимых пользователям для эксплуатации и технического обслуживания приборных систем безопасности;

- процедуры и спецификации, по которым должны работать организации, выполняющие модификации ПО безопасности;

j) применяется, когда функциональная безопасность достигается с помощью одной или более функций безопасности приборной системы безопасности 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 функций безопасности приборных систем безопасности как часть общих требований по достижению функциональной безопасности;

m) использует полный жизненный цикл безопасности (см. рисунок 8) и определяет список действий, которые необходимы для определения функциональных требований и требований к полноте безопасности приборных систем безопасности;

n) требует, чтобы была выполнена оценка опасности и степени риска для каждой функции безопасности приборной системы безопасности при определении требований к функциональной безопасности и к уровню полноты безопасности.

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

o) устанавливает количественные задания для средней вероятности отказа по запросу и частоты опасных отказов в час для различных уровней полноты безопасности;

p) определяет минимальные требования для отказоустойчивости аппаратных средств;

q) определяет методы/средства, необходимые для достижения указанных уровней полноты безопасности;

r) определяет максимальный уровень полноты безопасности (УПБ 4), который может быть достигнут для функции безопасности приборной системы безопасности, реализуемой в соответствии с настоящим стандартом;

s) определяет минимальный уровень полноты безопасности (УПБ 1), ниже которого настоящий стандарт не применяется;

t) является основой для установления уровней полноты безопасности, но не определяет уровни полноты безопасности для конкретных приложений (которые должны быть установлены на основании знаний о каждом конкретном приложении);

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

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

w) требует, чтобы при разработке функции безопасности приборной системы безопасности учитывался человеческий фактор;

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



Рисунок 2 — Соотношение между МЭК 61511 и МЭК 61508



Рисунок 3 — Соотношение между МЭК 61511 и МЭК 61508 (см. раздел 1)

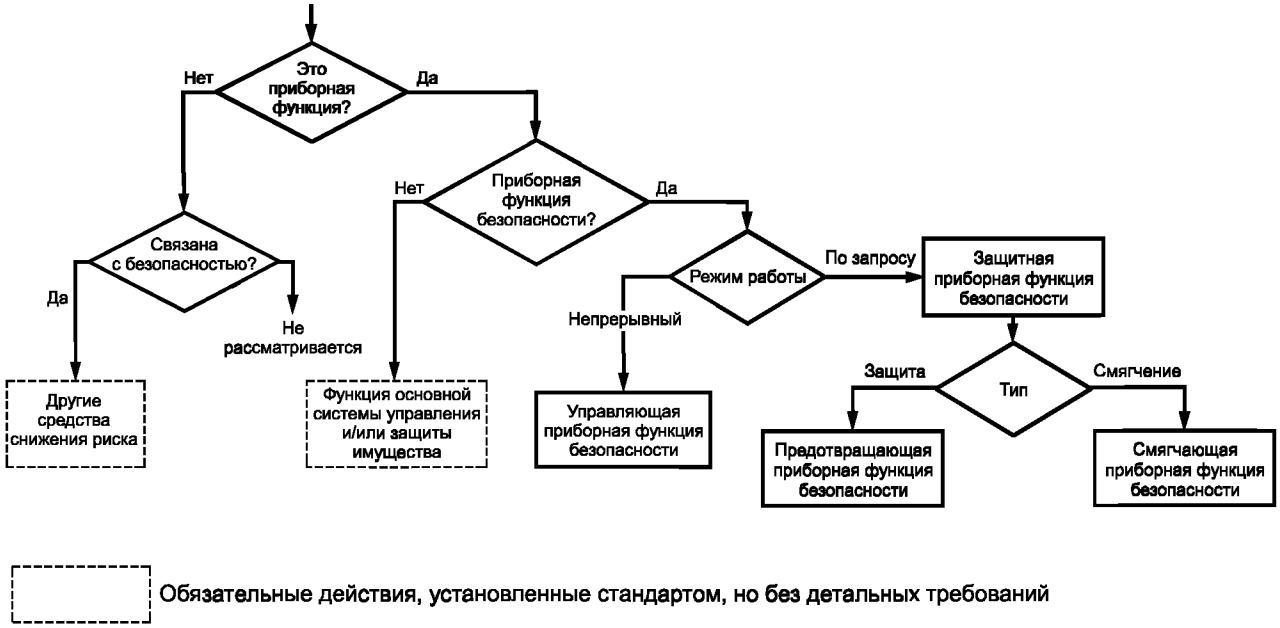


Рисунок 4 — Соотношение между приборными функциями безопасности и иными функциями

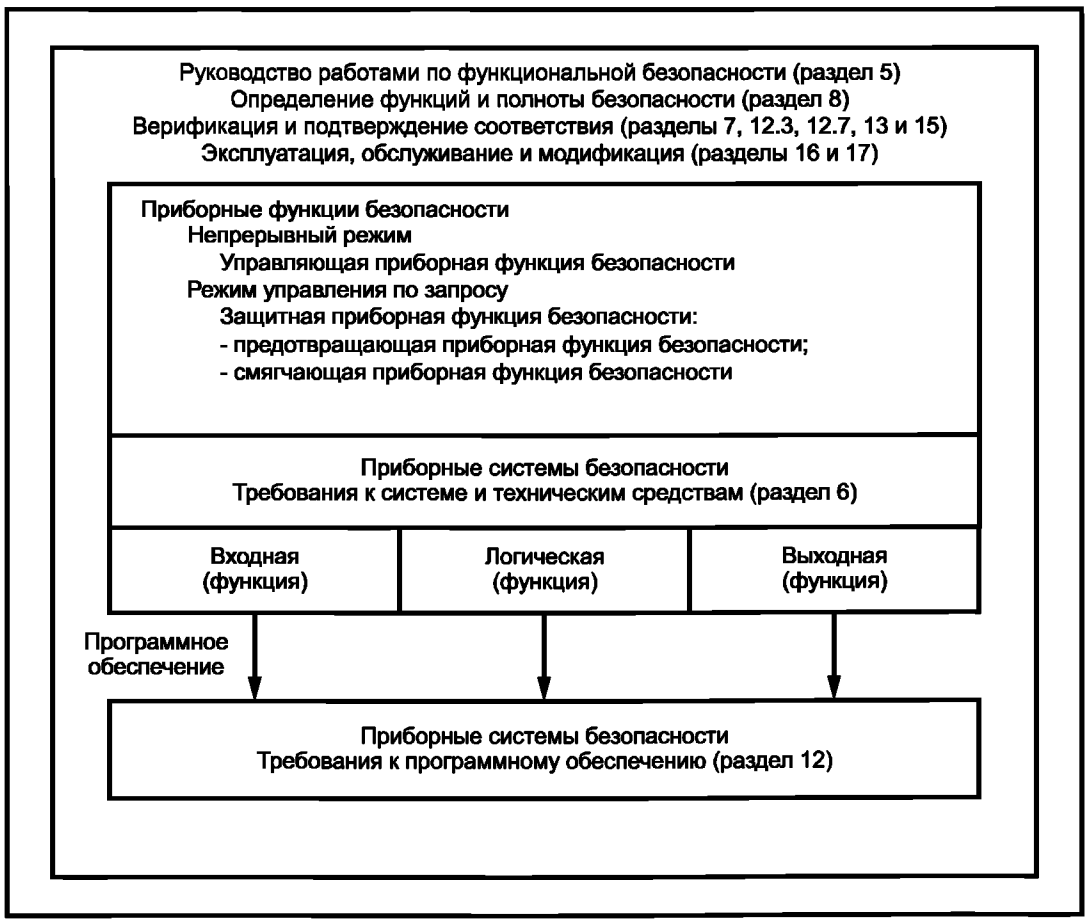


Рисунок 5 — Соотношение между системой, техническими средствами и программным обеспечением в соответствии с МЭК 61511-1

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

МЭК 60654-1:1993 Оборудование контрольно-измерительное для промышленных процессов. Условия работы. Часть 1. Климатические условия (IEC 60654-1:1993, Industrial process measurement and control equipment — Operating conditions — Part 1: Climatic conditions)

МЭК 60654-3:1998 Оборудование контрольно-измерительное для технологических процессов в промышленности. Часть 3. Механические воздействия (IEC 60654-3:1998, Industrial process measurement and control equipment — Operating conditions — Part 3: Mechanical influences)

МЭК 61326-1:2005 Электрооборудование для измерения, управления и лабораторного использования. Требования к электромагнитной совместимости (IEC 61326-1:2005, Electrical equipment for measurements, control laboratory use — EMC requirements)

МЭК 61508-2:2000 Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 2. Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью (IEC 61508-2:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems)

МЭК 61508-3:1998 Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 3. Требования к программному обеспечению (IEC 61508-3:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements)

МЭК 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью Часть 4. Определения и сокращения (IEC 61508-4:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4:1998, Definitions and abbreviations)

МЭК 61511-2:2003 Безопасность функциональная. Приборные системы безопасности для технологических процессов в промышленности. Часть 2. Руководящие указания к применению IEC 61511-1 (IEC 61511-2:2003, Functional safety — Safety instrumented systems for process industry sector — Part 2: Guidelines in the application of IEC 61511-1)

3 Сокращения, термины и определения

3.1 Сокращения

Сокращения, используемые в МЭК 61511, представлены в таблице 1.

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)
ANSI	—	Американский национальный институт стандартов (American National Standards Institute)
ISA	—	(Общество по приборам, системам и автоматизации) (Instrumentation, System and Automation Society)
FTA	АДО	Анализ дерева ошибок
HRA	АНП	Анализ надежности персонала
H&RA	ООР	Оценка опасности и риска
PFD	ВОНЗ	Вероятность отказа при наличии запроса
PFD_{avg}	$ВОНЗ_{ср}$	Средняя вероятность отказа при наличии запроса
SFF	ДБО	Доля безопасных отказов
HFT	ДЧО	Допустимое число отказов оборудования
FAT	ЗПИ	Заводские приемочные испытания
ISO	ИСО	Международная организация по стандартизации
MooN	М из N	М из N (см. 3.2.45)

Окончание таблицы 1

Сокращение (англ.)	Сокращение (рус.)	Полное название
IEC	МЭК	Международная электротехническая комиссия
IEV	МЭС	Международный электротехнический словарь
NP	НП	Непрограммируемый(ая, ое)
BPCS	ОСУП	Основная система управления процессом
SAT	ПИМ	Приемочные испытания на месте
PLC	ПЛК	Программируемый логический контроллер
S/W	ПО	Программное обеспечение
SIS	ПСБ	Приборная система безопасности
SIF	ПФБ	Приборная функция безопасности
PE	ПЭ	Программируемая электроника
PES	ПЭС	Программируемая электронная система
DC	ОД	Охват диагностикой
SRS	СТБ	Спецификация требований по безопасности
H/W	ТС	Технические средства
SIL	УПБ	Уровень полноты безопасности
FPL	ФЯП	Фиксированный язык программирования
HMI	ЧМИ	Человекомашинный интерфейс
E/E/PE	Э/Э/ПЭ	Электрическая или электронная, или программируемая электронная
E/E/PES	Э/Э/ПЭС	Электрическая или электронная, или программируемая электронная система
EMC	ЭМС	Электромагнитная совместимость
LVL	ЯОИ	Язык программирования с ограниченной изменчивостью
FVL	ЯПИ	Язык программирования с полной изменчивостью

3.2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.2.1 **архитектура** (architecture): Организация элементов аппаратных средств и/или ПО в системе. Например:

- организация (структура) подсистем в ПСБ;
- внутренняя структура подсистемы ПСБ;
- организация (структура) ПО.

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

3.2.2 **защита имущества** (asset protection): Функция, предусмотренная проектом системы в целях предотвращения имущественных потерь.

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, и которая выполняет функции безопасности ПСБ, имеющие номинальный УПБ, равный и выше 1.

Примечание — См. А.2 (приложение А).

3.2.4 **канал системы безопасности** (safety system channel): Элемент или группа элементов, независимо выполняющий(ая) определенную функцию.

Примечания

1 Элементами канала могут быть модули ввода/вывода, логическая система (см. 3.2.40), датчики, исполнительные устройства.

2 Двухканальная (или дуальная) конфигурация — это такая конфигурация, при которой два канала независимо выполняют одну и ту же функцию.

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

3.2.5 **кодирование** (coding): Процесс разработки, написания и тестирования программных кодов для решения проблемы или обработки данных в системе безопасности.

3.2.6

3.2.6.1 **отказ по общей причине** (common cause failure): Отказ, который является результатом одного или нескольких событий, вызывающих одновременные отказы двух и более отдельных каналов в многоканальной системе и приводящих к отказу системы.

3.2.6.2 **отказ общего типа** (common mode failure): Одинаковый отказ двух и более каналов, приводящий к одному и тому же неправильному результату.

3.2.7 **компонент системы безопасности** (safety system component): Одна из частей системы, подсистемы или устройства, выполняющая определенную функцию.

3.2.8 **конфигурация системы безопасности** (safety system configuration): Организация элементов аппаратных средств и/или ПО в системе безопасности, позволяющая реализовать управление изменениями в этих элементах и обеспечить соблюдение их преемственности и прослеживаемости на протяжении всего жизненного цикла.

3.2.9 **управление конфигурацией системы безопасности** (safety system configuration management): Порядок определения компонентов системы, включающей компоненты аппаратных средств и ПО, обеспечивающий управление изменениями в этих компонентах и соблюдение их преемственности и прослеживаемости на протяжении всего жизненного цикла.

3.2.10 **система управления системы безопасности** (safety system 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 устройства ввода и исполнительные устройства и может быть либо ОСУП, либо ПСБ, либо их комбинацией.

3.2.11 **опасный отказ системы безопасности** (safety system dangerous failure): Отказ, который потенциально может перевести систему, связанную с безопасностью, в опасное или неработоспособное состояние.

Примечание — Реализуется или нет такая возможность, может зависеть от архитектуры канала системы; в многоканальных системах с каналами, предназначенными для повышения безопасности, менее вероятно, что опасные отказы оборудования приведут к переходу в общее опасное или неработоспособное состояние.

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 $P(A + B) > P(A) \times P(B)$, где $P(z)$ — вероятность события z.

2 См. в 9.5 пример зависимого отказа между слоями защиты.

3 Зависимый отказ включает в себя отказ по общей причине (см. 3.2.6).

3.2.13 **обнаруженный** (detected, revealed, overt): Вид отказа, выявляемого диагностическими проверками или при нормальном функционировании.

Примечание — Относится к отказам аппаратных средств или ошибкам ПО.

3.2.14 **устройство системы безопасности** (safety system device): Функциональная единица аппаратных средств или ПО либо совместно аппаратно-программных средств, способная выполнять определенную задачу.

Примечание — Например, внешнее устройство; оборудование, подсоединенное к терминалам ввода-вывода ПСБ; такое оборудование включает в себя соединительные провода, датчики, исполнительные элементы, логические устройства и те средства интерфейса оператора, которые подсоединены к терминалам ввода-вывода ПСБ.

3.2.15 **охват диагностикой**; ОД (diagnostic coverage; DC): Отношение интенсивности обнаруженных отказов, выявляемых в результате диагностических проверок, к общей интенсивности отказов компонента или подсистемы без учета ошибок, выявленных при проверочных испытаниях.

Примечания

1 Если известна интенсивность всех отказов ($\lambda_{\text{total failure rate}}$), то это отношение используется для вычисления интенсивностей обнаруженных ($\lambda_{\text{detected}}$) и необнаруженных ($\lambda_{\text{undected}}$) отказов по формулам: $\lambda_{\text{detected}}$ = = ОД × $\lambda_{\text{total failure rate}}$ и $\lambda_{\text{undected}}$ = (1 – ОД) × $\lambda_{\text{total failure rate}}$.

2 Охват диагностикой применяется к компонентам или подсистемам ПСБ. Например, охват диагностикой обычно определяется для датчиков, исполнительных или логических устройств.

3 На опасных объектах охват диагностикой обычно применяется для характеристики безопасных и опасных отказов какого-либо компонента или подсистемы. Например, охват диагностикой для опасных отказов компонента или подсистемы определяется как ОД = $\lambda_{DD}/\lambda_{DT}$, где λ_{DD} — интенсивность выявленных опасных отказов и λ_{DT} — общая интенсивность опасных отказов.

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

Примечание — Разнообразие может быть достигнуто с помощью различных физических методов и различных проектных подходов.

3.2.17 **электрическая/электронная/программируемая электронная система**; Э/Э/ПЭС (electrical/electronic/programmable electronic system; E/E/PES): Система, основанная на применении электрического (Э)/электронного (Э)/программируемого электронного (ПЭ) принципа действия.

Примечание — Данный термин предназначен для обозначения всех и любых устройств или систем, действующих на основе электричества, и может охватывать:

- электромеханические устройства (электрические);
- полупроводниковые непрограммируемые электронные устройства (электронные);
- электронные устройства, основанные на компьютерных технологиях (программируемые электронные); см. 3.2.55.

3.2.18 **ошибка** (error): Расхождение между вычисленным, наблюдаемым или измеренным значением или условием и его истинным, проектным или теоретически правильным значением или условием.

Примечание — Это определение (исключая примечания) соответствует [1].

3.2.19 **внешнее средство уменьшения риска** (external risk reduction facilities): Средство, предназначенное для уменьшения или ослабления рисков, существующее отдельно от ПСБ и отличное от нее.

Примечания

1 Дренажная система, пожарная стена, дамба (насыпь) относятся к внешним средствам уменьшения риска.

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

3.2.20 **отказ** (failure): Прекращение способности функциональной единицы выполнять требуемую функцию.

Примечания

1 Это определение (исключая настоящие примечания) соответствует [2].

2 Дополнительные пояснения см. в МЭК 61508-4.

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

4 Отказы могут быть случайными или систематическими (см. 3.2.62 и 3.2.85).

3.2.21 **сбой** (fault): Ненормальный режим, который может привести к снижению или потере способности функциональной единицы выполнять требуемую функцию.

Примечание — В [1] «сбой» определяется как состояние, характеризуемое неспособностью выполнить необходимую функцию, исключая периоды предупредительного обслуживания и других плановых действий или случаи нехватки внешних ресурсов [2].

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

3.2.23 **отказоустойчивость функциональной единицы** (functional unit fault tolerance): Способность функциональной единицы продолжать выполнять требуемую функцию при наличии сбоев или ошибок.

Примечание — Определение, приведенное в [1], относится только к отказам подкомпонентов. См. примечание к термину «неисправность» в пункте 3.2.21 [2].

3.2.24 **исполнительное устройство** (final element): Часть ПСБ, которая выполняет физические действия, необходимые для достижения безопасного состояния.

Примечание — Исполнительными устройствами могут служить клапаны, переключатели, двигатели, включая их дополнительные элементы (например, соленоидный клапан или усилитель), если он участвует в выполнении функции безопасности ПСБ.

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

3.2.26 **оценка функциональной безопасности** (functional safety assessment): Изучение фактов, позволяющее судить о функциональной безопасности, достигаемой с помощью одного или более слоев защиты.

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

3.2.27 **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 оценки функциональной безопасности.

3.2.28 **функциональная единица системы безопасности** (safety system functional unit): Совокупность средств технического и/или программного обеспечения, способная достигать заданную цель [2].

Примечание — В [1] вместо термина «функциональная единица» использован более общий термин «объект». Иногда «объект» может включать в себя людей.

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

Примечания

1 Данный термин относится к отказам, проявляющимся в опасном режиме, то есть к тем отказам функции безопасности ПСБ, которые снижают ее полноту безопасности. Данная ситуация характеризуется двумя параметрами: суммарной интенсивностью опасных отказов и вероятностью отказа при выполнении запроса.

2 См. 3.2.86.

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

3.2.30 **вред** (harm): Физическое повреждение или ущерб здоровью человека, причиненный как прямо, так и косвенно в результате повреждения имущества или ухудшения окружающей среды.

Примечание — Данное определение соответствует [3].

3.2.31 **опасность** (hazard): Потенциальный источник вреда [3].

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).

3.2.32 **ошибка человека** (human error, mistake): Действие или бездействие человека, которое может привести к непредусмотренному результату.

Примечание — Данное определение соответствует [2] и отличается от приведенного в [1] добавлением слов «или бездействие».

3.2.33 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.

3.2.34 **независимое подразделение** (independent department): Отдельное подразделение, не связанное с подразделениями, отвечающими за работы, выполняемые в течение определенной стадии жизненного цикла безопасности, которое осуществляет оценку или подтверждение соответствия функциональной безопасности.

3.2.35 **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, которая осуществляет оценку или подтверждение соответствия функциональной безопасности.

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

3.2.37 **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.

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

Примечание — В промышленных процессах системы, оснащенные измерительными средствами, обычно состоят из датчиков технологических параметров (например, давления, расхода, температуры), логических устройств или управляющих систем (например, программируемых контроллеров, распределенных систем управления) и исполнительных устройств (например, управляющих клапанов). В конкретных случаях системы, оснащенные измерительными средствами, могут считаться ПСБ (см. 3.2.72).

3.2.39 **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.

Примечание — Дополнительные указания см. в [4] и [5].

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

Примечания

1 В МЭК 61511 применены следующие термины для логических систем:

- электрические логические системы — для систем с электромеханическим принципом действия;
- электронные логические системы — для систем с электронным принципом действия;
- программируемые электронные логические системы — для систем с программируемым электронным принципом действия.

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

3.2.40.1 **конфигурируемое логическое устройство безопасности** (safety configured logic solver): Промышленное программируемое электронное логическое устройство общего назначения, которое может быть специально сконфигурировано для применения в целях обеспечения безопасности в соответствии с 11.5.

3.2.41 **интерфейс обслуживающего (технического) персонала** (maintenance/engineering interface): Совокупность технических средств и ПО, обеспечивающая возможность правильного обслуживания (выполнения) изменений ПСБ.

Примечание — Такой интерфейс может включать в свой состав инструкции и диагностические средства, которые можно найти в составе ПО, терминалы программирования с соответствующими протоколами связи, средства диагностики, индикаторы, устройства обхода, контрольные приборы и калибровочные устройства.

3.2.42 **ослабление опасного события** (mitigation of a hazardous event): Действие, снижающее тяжесть последствия(й) опасного события.

Примечание — Например, аварийное снижение давления при обнаружении огня или утечки газа.

3.2.43 **режим работы функции безопасности приборной системы безопасности** (safety instrumented function mode of operation): Способ, в соответствии с которым выполняется функция безопасности ПСБ.

3.2.43.1 **режим работы по запросу функции безопасности приборной системы безопасности** (demand mode safety instrumented function): Режим работы, при котором определенное действие (например, закрывание клапана) выполняется в ответ на появление заданных условий процесса или другого запроса, а потенциальная опасность в случае опасного отказа функции безопасности ПСБ возникает только при наличии отказа в процессе или в ОСУП.

3.2.43.2 **непрерывный режим работы функции безопасности приборной системы безопасности** (continuous mode safety instrumented function): Режим работы, при котором в случае опасного отказа функции безопасности ПСБ потенциальная опасность возникает даже без последующих отказов до тех пор, пока не предприняты действия для предотвращения этой опасности.

Примечания

1 Непрерывный режим работы характерен для тех функций безопасности ПСБ, которые реализуют непрерывный контроль над поддержанием функциональной безопасности.

2 В режиме по запросу, когда частота запросов более чем один раз в год, частота опасного события будет не более чем частота опасного отказа функции безопасности ПСБ. В этом случае будет правильно применять непрерывный режим работы.

3 Целевые меры отказов для функций безопасности ПСБ, работающих в режиме низкой частоты запросов, а также в режиме непрерывной работы, определены в таблицах 3 и 4.

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

3.2.44 **модуль** (module): Модульная сборка компонентов оборудования, выполняющая конкретную функцию технических средств (например, модуль цифрового ввода, модуль аналогового вывода), либо повторно используемая прикладная программа (может быть подпрограммой либо множеством программ), поддерживающая определенную функцию (например, часть вычислительной программы), выполняющая конкретную функцию.

Примечания

1 В соответствии с [4] модуль ПО является функцией или функциональным блоком.

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

3.2.45 **M из N** (MooN): Приборная система безопасности или ее часть, выполненная из N независимых каналов, соединенных так, что M каналов достаточно для выполнения функции безопасности ПСБ.

3.2.46 **необходимое снижение риска** (necessary risk reduction): Уменьшение риска, которое требуется для того, чтобы быть уверенным, что риск снижен до приемлемого уровня.

3.2.47 **непрограммируемая система**; НП-система (non-programmable; NP system): Система, основанная на некомпьютерных технологиях, то есть система, принцип действия которой не основан на использовании программируемой электроники или ПО.

3.2.48 **интерфейс оператора** (operator interface): Средство или совокупность средств, обеспечивающее(их) обмен информацией между оператором(ами) и ПСБ.

Примечание — Например, электронно-лучевые трубки, световые индикаторы, кнопки, сирены, устройства аварийной сигнализации. Интерфейс оператора иногда называют интерфейсом человек-машина.

3.2.49 **связанная с безопасностью система, основанная на применении других технологий** (other technology safety-related system): Система, связанная с безопасностью, основанная на применении технологии, отличающейся от электрической, электронной или программируемой электронной технологии.

Примечание — Примером системы, связанной с безопасностью и основанной на применении других технологий, является перепускной клапан. Другими примерами могут служить гидравлические и пневматические системы.

3.2.50 **выходная функция** (output function): Функция, состоящая в управлении процессом и его соответствующим оборудованием в соответствии с информацией, поступающей на исполнительное устройство от логического устройства.

3.2.51 **стадия жизненного цикла безопасности** (safety life cycle phase): Интервал внутри жизненного цикла безопасности, в течение которого выполняются действия, описанные в настоящем стандарте.

3.2.52 **предотвращение опасного события** (prevention of a hazardous event): Действие, снижающее частоту появления опасных событий.

3.2.53 **предшествующее применение** (prior use): Документированная оценка предшествующего опыта применения данного компонента для доказательства того, что он подходит для применения в ПСБ.

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

Примечания

1 Риск в этом 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 [6]. Основной целью определения риска процесса является установление значения риска без учета слоев защиты.

3 Оценка такого риска включает в себя влияние соответствующего человеческого фактора.

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

3.2.55 **программируемая электроника**; ПЭ (programmable electronic; PE): Электронные компоненты или устройства, формирующие часть ПЭС и основанные на использовании компьютерных технологий. Этот термин охватывает как технические, так и программные компоненты, включая устройства ввода и вывода.

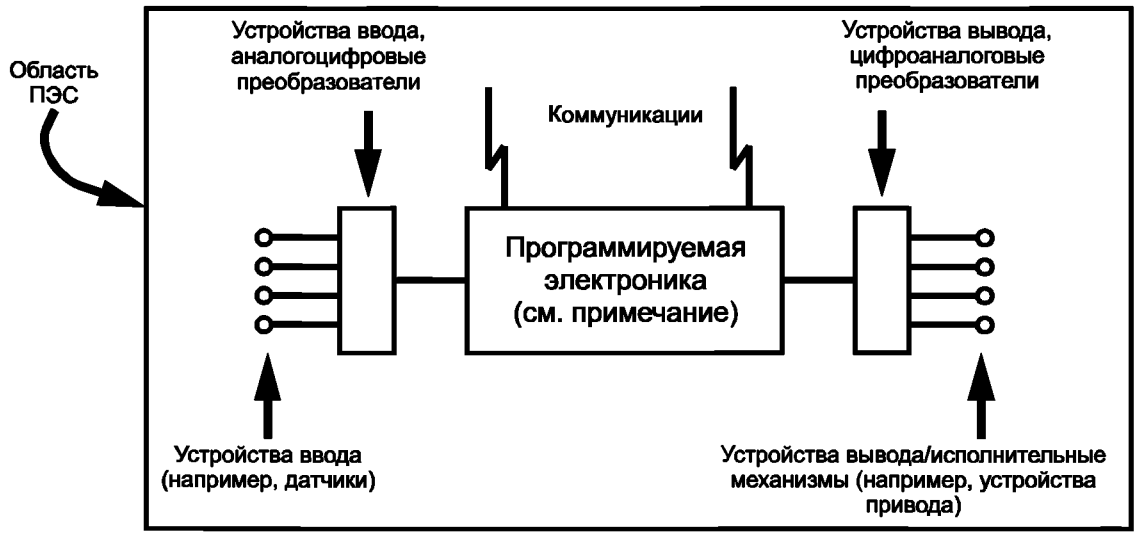
Примечания

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

- датчики с развитой логикой и исполнительные элементы;
- программируемая электроника логической системы, включающая:
- программируемые устройства управления;
- 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.

3.2.56 **программируемая электронная система**; ПЭС (programmable electronic system; PES): Система для управления, защиты или контроля, основанная на применении одного или нескольких программируемых электронных устройств, включая все элементы системы, такие, как источники питания, датчики и другие устройства ввода, шины данных и другие линии связи, устройства привода и другие выходные устройства (см. рисунок 6).



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

Рисунок 6 — Программируемая электронная система (ПЭС): структура и терминология

3.2.57 **программирование системы безопасности** (safety system programming): Процесс разработки, написания и тестирования множества инструкций для решения проблемы или обработки данных в системе безопасности.

Примечание — В настоящем стандарте программирование обычно связано с ПЭ.

3.2.58 **контрольная проверка** (proof test): Испытание, проводимое для выявления в ПСБ ранее не обнаруженных отказов так, чтобы при необходимости систему можно было вернуть к ее предусмотренным функциональным возможностям.

3.2.59 **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).

3.2.60 **проверено в эксплуатации** (proven-in-use): Ситуация, при которой документированной оценкой показано, что существуют соответствующие, основанные на предшествующем опыте применения доказательства того, что данный компонент подходит для применения в ПСБ (см. «предшествующее применение компонентов» в 11.5).

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

3.2.61 **качество системы безопасности** (safety system quality): Совокупность характеристик реальной системы безопасности, которая отражает ее способность удовлетворять установленные и подразумеваемые потребности.

Примечание — Более подробно см. в [7].

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

Примечания

1 Существует много механизмов ухудшения характеристик, действующих с различной интенсивностью в различных компонентах. 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 Основное различие между случайными отказами аппаратных средств и систематическими отказами (см. 3.2.85) состоит в том, что интенсивность отказов системы (или другие подобные характеристики таких отказов), связанная со случайными отказами аппаратных средств, может быть прогнозируема с достаточной степенью точности, но систематические отказы по своей природе не могут быть предсказаны точно. Это означает, что интенсивность отказов системы, вызванных случайными отказами аппаратных средств, может быть оценена количественно с достаточной степенью точности, тогда как систематические отказы нельзя оценить количественно статистическим методом, поскольку события, приводящие к таким отказам, не могут быть предсказаны.

3.2.63 **избыточность** (redundancy): Использование нескольких элементов или систем для выполнения одной и той же функции. Избыточность может быть реализована путем использования идентичных элементов (однородное резервирование) или разнообразных элементов (разнородное резервирование).

Примечания

1 Примерами избыточности являются дублирование функциональных компонентов и добавление битов четности.

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

3 Определение в [1] является менее полным, чем в [2].

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

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

Примечание — Дальнейшее обсуждение этого понятия см. в разделе 8.

3.2.65 **безопасный отказ** (safe failure): Отказ, который потенциально не способен перевести ПСБ в опасное состояние или в состояние отказа при выполнении функции.

Примечания

1 Реализуется ли такая потенциальная способность, может зависеть от архитектуры канала системы.

2 Другие названия, используемые для безопасного отказа, — мешающий отказ, ложный отказ или отказ, не нарушающий работоспособность других элементов (системы).

3.2.65.1 **доля безопасных отказов** (safe failure fraction): Часть общей интенсивности случайных отказов технического средства, приходящаяся на отказы, приводящие к безопасным или обнаруженным опасным отказам системы.

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

Примечания

1 При переходе от потенциально опасного состояния к конечному, безопасному состоянию процесс может проходить через несколько промежуточных безопасных состояний. 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.

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

3.2.67 **безопасность** (safety): Отсутствие неприемлемого риска.

Примечание — Настоящее определение соответствует [3].

3.2.68 **функция безопасности** (safety function): Функция, реализуемая ПСБ, системой, связанной с безопасностью, основанной на других технологиях, или внешними средствами снижения риска, которая предназначена для достижения или поддержания безопасного состояния процесса применительно к определенному опасному событию.

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

3.2.69 **функция управления приборной системы безопасности** (safety instrumented control function): Функция безопасности приборной системы безопасности с заданным УПБ, которая выполняется в непрерывном режиме и предназначена для предотвращения появления опасного состояния и/или ослабления его последствий.

3.2.70 **система управления приборной системы безопасности** (safety instrumented control system): Система управления, используемая для выполнения одной или более функций управления приборной системы безопасности.

Примечание — Системы управления приборной системы безопасности редко реализуются внутри процесса. Если такие системы встречаются, то их необходимо рассматривать как специальный случай и разрабатывать на индивидуальной основе. Требования настоящего стандарта применимы к таким системам, но для того, чтобы продемонстрировать, что система способна удовлетворять требованиям безопасности, может потребоваться более подробный анализ.

3.2.71 **функция безопасности приборной системы безопасности**; ФБПСБ (safety instrumented function; SIF): Функция безопасности с определенным уровнем полноты безопасности, необходимым для обеспечения функциональной безопасности, которая может быть либо функцией защиты, либо функцией управления.

3.2.72 **приборная система безопасности**; ПСБ (safety instrumented system; SIS): Система контроля и управления, которая используется для выполнения одной или нескольких функций безопасности и состоит из одного или нескольких датчиков, из одного или нескольких логических устройств и из одного или нескольких исполнительных элементов. Пример см. на рисунке 7.

Примечания

1 ПСБ может выполнять функции безопасности и/или функции защиты.

2 Производители и поставщики устройств ПСБ должны ссылаться на раздел 1, перечисления от a) до d) включительно.

3 ПСБ может содержать или не содержать в себе ПО.

4 См. А.2 (приложение А).

5 В случаях, когда действие человека является частью действия ПСБ, в спецификации требований к безопасности должны быть определены готовность действий оператора и их надежность и включены в расчеты характеристик ПСБ. Указания по отражению надежности, готовности и подготовленности оператора в расчетах УПБ см. в МЭК 61511-2.

Пример архитектуры ПСБ и ПФБ с различными устройствами

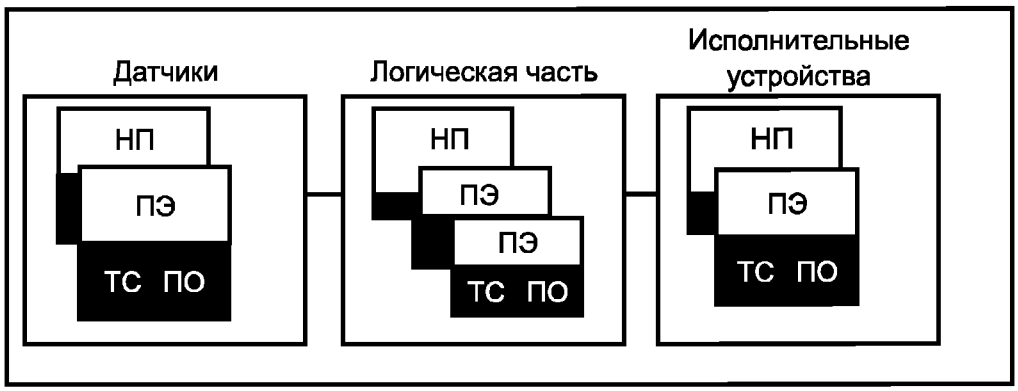


Рисунок 7 — Пример структуры ПСБ

3.2.73 **полнота безопасности** (safety integrity): Средняя вероятность того, что ПСБ удовлетворительно выполняет требуемые функции безопасности ПСБ при всех заданных условиях и в течение заданного периода времени.

Примечания

1 Чем выше уровень полноты безопасности, тем ниже вероятность того, что требуемая функция безопасности ПСБ будет выполнена.

2 Существуют четыре уровня полноты безопасности для функций безопасности ПСБ.

3 При определении полноты безопасности следует учитывать все случаи отказов (как случайных отказов аппаратных средств, так 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 интенсивность опасных отказов или вероятность срабатывания функции безопасности ПСБ при наличии запроса. Однако полнота безопасности ПСБ также зависит от многих факторов, которые нельзя точно определить количественно, но можно рассмотреть качественно.

4 Полнота безопасности системы включает в себя полноту безопасности технических средств и полноту безопасности по отношению к систематическим отказам.

3.2.74 **уровень полноты безопасности**; УПБ (safety integrity level; SIL): Дискретный уровень (принимающий одно из четырех возможных значений), определяющий требования к полноте безопасности для функций безопасности ПСБ, который ставится в соответствие приборным системам безопасности. Уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности, уровень, равный 1, отвечает наименьшей полноте безопасности.

Примечания

1 Целевые меры отказов для УПБ определены в таблицах 3 и 4.

2 Допускается использование нескольких систем с более низким УПБ для удовлетворения требований функции с более высоким уровня (например, совместное применение систем с УПБ 2 и УПБ 1 для выполнения функции с УПБ 3).

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

3.2.75 **спецификация требований к полноте безопасности** (safety integrity requirements specification): Спецификация, содержащая требования к полноте безопасности для функций безопасности ПСБ, которые должны быть выполнены этими системами.

Примечания

1 Данная спецификация представляет собой часть (относящуюся к полноте безопасности) спецификации требований к безопасности (см. 3.2.78).

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

3.2.76 **жизненный цикл систем безопасности** (safety lifecycle): Необходимые процессы, относящиеся к реализации функции(й) безопасности ПСБ, проходящие 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 настоящего стандарта.

2 Модель жизненного цикла безопасности, используемая в МЭК 61511, приведена на рисунке 8.

3.2.77 **руководство по безопасности** (safety manual): Руководство, определяющее, как могут быть безопасно применены устройства, подсистемы или системы.

Примечание — Руководство по безопасности может быть самостоятельным документом, учебным руководством, руководством по программированию, стандартом или включенным в документ(ы) пользователя, определяющий(ие) ограничения применимости.

3.2.78 **спецификация требований к безопасности** (safety requirements specification): Спецификация, содержащая все требования к функциям безопасности ПСБ, которые должны быть выполнены ПСБ.

3.2.79 **программное обеспечение безопасности** (safety software): Программное обеспечение приборной системы безопасности, включающее прикладное, встроенное или сервисное программное обеспечение.

3.2.80 **датчик системы безопасности** (safety system sensor): Устройство или совокупность устройств системы безопасности, выполняющие измерение условий протекания процесса.

Примечание — Например передатчик, преобразователь, переключатель процессов, переключатель направлений.

3.2.81 **программное обеспечение**; ПО (software; S/W): Продукт интеллектуальной деятельности, включающий программы, процедуры, данные, правила и любую связанную с ними документацию, относящиеся к функционированию системы обработки данных.

Примечания

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

2 Данное определение без примечания 1 отличается от приведенного в [8], а полное определение отличается от приведенного в [9] добавлением слова «данные».

3.2.81.1 Языки программирования в подсистемах ПСБ

3.2.81.1.1 **фиксированный язык программирования**; ФЯП (fixed program language; FPL): Тип языка программирования, в котором пользователь ограничен выбором нескольких параметров, таких как диапазон датчика давления, настройки аварийной сигнализации, сетевые адреса.

Примечание — Типичными примерами устройств с ФЯП являются интеллектуальный датчик (например, датчик давления), интеллектуальный клапан, контроллер последовательности событий, цифровой блок аварийной сигнализации, небольшие системы логической обработки данных.

3.2.81.1.2 **язык программирования с ограниченной изменчивостью**; ЯОИ, (limited variability language; LVL): Тип языка программирования, специально созданного для специалистов, работающих с процессами, который позволяет объединять предварительно определенные, специфические для предметной области библиотечные функции для выполнения спецификаций требований к безопасности и обеспечить близкое соответствие программ с функциями, требуемыми для данного применения.

Примечания

1 Типичные примеры ЯОИ приведены в [4] и включают в себя языки многоступенчатых диаграмм, диаграмм функциональных блоков, диаграмм функциональных последовательностей.

2 Типичными примерами систем, использующих ЯОИ, являются стандартные программируемые логические контроллеры (например, ПЛК для управления горелкой).

3.2.81.1.3 **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 системы, широко используемые компьютерами.

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

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

3.2.81.2 Типы ПО (software program type)

3.2.81.2.1 **прикладное программное обеспечение** (application software): Специальное программное обеспечение для применений пользователей, содержащее в общем случае логические предложения, условия, ограничения и выражения, управляющие вводом, выводом, вычислениями, решениями, необходимые для выполнения требований функциональной безопасности приборных систем безопасности. См. 3.2.81.1.1, ФЯП, и 3.2.81.1.2, ЯОИ.

3.2.81.2.2 **встроенное программное обеспечение** (embedded software): Программное обеспечение, являющееся частью системы, поставляемой производителем, и которое запрещено модифицировать конечным пользователям.

Примечание — Встроенное программное обеспечение называют также мягким обеспечением или системным программным обеспечением. См. 3.2.81.1.3, ЯПИ.

3.2.81.2.3 **сервисное программное обеспечение** (utility software): Программные инструменты для создания, модификации и документирования прикладных программ.

Примечание — Такие программные инструменты для ПСБ не требуются.

3.2.82 **жизненный цикл ПО** (software lifecycle): Процессы, происходящие в течение периода времени, который начинается с появления общей концепции ПО и заканчивается, когда ПО окончательно перестает эксплуатироваться.

Примечания

1 Обычно жизненный цикл ПО включает в себя стадии разработки требований, разработки ПО, тестирования, интеграции, установки, а также проведения модификаций.

2 ПО не может подвергаться обслуживанию, скорее оно подлежит модификации.

3.2.83 **подсистема безопасности** (safety subsystem): Элемент системы, связанной с безопасностью.

3.2.84 **система безопасности** (safety system): Совокупность связанных с безопасностью элементов, которые взаимодействуют в соответствии с проектом, в котором элементом системы может быть другая система, называемая подсистемой; система может быть управляющей системой или управляемой системой и включать аппаратные средства, ПО и средства взаимодействия с человеком.

Примечания

1 Человек может быть частью системы.

2 Это определение отличается от приведенного в [10].

3 Система включает датчики, логические устройства, исполнительные элементы, средства коммуникации и вспомогательное оборудование, принадлежащее ПСБ (например, кабели, кабельные каналы, источники электропитания).

3.2.85 **систематический отказ (системы безопасности)** (systematic failure): Отказ, детерминированно связанный с некоторой причиной, которая может быть устранена только путем модификации проекта либо рабочих операций, процедур, документации, либо других факторов.

Примечания

1 Корректирующее сопровождение без модификации обычно не устраняет причину отказа.

2 Систематический отказ может быть воспроизведен имитацией причины отказа.

3 Настоящее определение (вплоть до примечания 2) соответствует [1].

4 Примерами источников систематических отказов являются ошибки человека, внесенные:

- в спецификации требований к безопасности;
- при проектировании, изготовлении, установке или эксплуатации технических средств;
- при проектировании и/или реализации ПО.

3.2.86 **полнота безопасности по отношению к систематическим отказам** (systematic safety integrity): Составляющая полноты безопасности функции безопасности приборной системы безопасности, связанная с систематическими отказами (см. 3.2.73, примечание 3) опасного вида.

Примечания

1 Обычно полноту безопасности по отношению к систематическим отказам нельзя описать количественно (в отличие от полноты безопасности технических средств).

2 См. также 3.2.29.

3.2.87 **целевая мера отказов** (target failure measure): Заданное значение вероятности опасных отказов, которое должно быть достигнуто в соответствии с требованиями к полноте безопасности, определяемое:

- либо как средняя вероятность отказа при выполнении проектируемой функции при наличии запроса (для режима работы с низкой частотой запросов);
- либо как частота опасных отказов выполнения ФБПСБ в час (для режима с высокой частотой запросов или непрерывным запросом).

Примечание — Количественные оценки для целевых мер отказов даны в таблицах 3 и 4.

3.2.88 **шаблон ПО** (software template): Структурированная неспециализированная часть ПО, которую можно легко изменять для выполнения специальных функций, сохраняя исходную структуру.

Примечания

1 Например, шаблон интерактивного экрана управляет изображением потоков в процессе на экранах приложений, но не отражает специфики представляемых данных. Программист может воспользоваться общим шаблоном и выполнить специальные корректировки (настройки), создав новый экран для конкретных пользователей.

2 Иногда используется термин «шаблон ПО». Обычно он относится к алгоритму или совокупности алгоритмов, которые должны быть запрограммированы для выполнения необходимой функции или множества функций и собраны так, чтобы они могли быть использованы во многих различных случаях. В контексте [4] — это программа, которая может быть выбрана для многих приложений.

3.2.89 **приемлемый риск** (tolerable risk): Риск, который приемлем при данных обстоятельствах на основании существующих в текущий период времени ценностей в обществе [3].

Примечание — См. [6].

3.2.90 **необнаруженный** (undetected, unrevealed, covert): Вид сбоев в аппаратных средствах и в ПО, не выявляемых с помощью диагностических проверок либо в ходе нормальной работы.

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

3.2.91 **подтверждение соответствия** (validation): Действия, демонстрирующие, что функция(и) безопасности ПСБ и приборная(ые) система(ы) безопасности, рассматриваемые после установки, во всех отношениях удовлетворяют спецификации требований к безопасности.

3.2.92 **верификация** (verification): Действия, демонстрирующие для каждой стадии соответствующего жизненного цикла безопасности путем анализа и/или тестирования, что при определенных входах (входных данных) выходы (результаты) удовлетворяют во всех отношениях целям и требованиям соответствующей стадии.

Примечание — Процесс верификации включает в себя:

- просмотр выходных результатов (документов, относящихся ко всем стадиям жизненного цикла безопасности) для того, чтобы убедиться в соответствии целям и требованиям соответствующей стадии с учетом конкретных входных данных для этой стадии;
- проверку проектов;
- тестирование разработанной продукции для того, чтобы убедиться, что она выполнена в соответствии с их спецификациями;
- комплексные (интегральные) испытания, при которых различные части систем объединяются шаг за шагом в единую систему, проводимые путем выполнения испытаний на воздействие окружающей среды для того, чтобы убедиться в том, что все части работают вместе заданным образом в соответствии со спецификацией.

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

Примечания

1 Сторожевое устройство подтверждает, что программная система работает корректно, путем регулярного перезапуска внешнего устройства (например, аппаратного электронного таймера сторожевого устройства) с помощью программно-управляемого выходного устройства.

2 Сторожевое устройство может быть использовано для обесточивания группы выходов безопасности при обнаружении опасных отказов для перевода процессов в безопасное состояние. Сторожевое устройство используется для увеличения охвата диагностикой программируемой электроники логического устройства в реальном времени (см. 3.2.15 и 3.2.40).

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

Примечание — Данный раздел 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 Основные требования

5.2.1.1 Политику и стратегию обеспечения безопасности следует определять совместно для оценки ее достижимости и связывать с организацией.

5.2.1.2 Система руководства работами по безопасности должна быть организована так, чтобы быть уверенным в том, что ПСБ, если их используют, способны приводить и/или поддерживать процесс в безопасном состоянии.

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 безопасности (включая при необходимости лицензирующие и надзорные органы), и необходимо проинформировать их о возложенной на них ответственности.

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

Примечание — При рассмотрении компетенции лиц, подразделений, организаций и других структур, участвующих в реализации жизненного цикла безопасности, следует проверить, как минимум, 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 безопасности;

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

g) понимание потенциально возможных последствий события;

h) уровень полноты безопасности ПСБ;

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

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

Чтобы определить действия, которые необходимо выполнить, а также лиц, подразделения, организации или другие структуры, ответственные за выполнение этих действий, следует составить план безопасности. При необходимости такое планирование следует обновлять в процессе полного жизненного цикла безопасности (см. раздел 6).

Примечание — Результаты планирования безопасности могут быть оформлены:

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

5.2.5 Реализация и контроль

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

- анализа опасностей и оценки рисков;
- оценки и аудита работ;
- действий по верификации;
- действий по подтверждению соответствия;
- 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 безопасности, должен передавать изделия или услуги как специально предназначенные для этой организации и иметь систему управления качеством. При этом следует установить процедуры проверки адекватности такой системы.

5.2.5.3 Должны быть реализованы процедуры, предназначенные для оценки выполнения ПСБ требований ее безопасности, включая следующие процедуры для:

- обнаружения и предотвращения систематических отказов, которые могут нарушить безопасность;
- оценки того, согласуется ли интенсивность опасных отказов ПСБ с принятой при проектировании.

Примечания

1 Опасные отказы обнаруживаются посредством контрольных испытаний, диагностических тестов или отказов срабатывания при наличии запроса.

2 Следует рассмотреть процедуры, определяющие необходимые корректирующие действия, которые должны предприниматься, если интенсивности отказов окажутся выше значений, принятых при проектировании;

- оценки интенсивности запросов на срабатывание функции безопасности ПСБ в реальных условиях, чтобы проверить предположения, сделанные в ходе оценки риска, при определении требований к уровню полноты безопасности.

5.2.6 Оценка, аудит и проверки

5.2.6.1 Оценка функциональной безопасности

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

5.2.6.1.2 В состав команды специалистов, проводящих оценку, должен входить по крайней мере один старший компетентный специалист, не участвовавший в проектировании.

Примечания

1 Если команда специалистов, проводящих оценку, велика, следует рассмотреть вопрос о привлечении в ее состав более чем одного старшего компетентного специалиста, не участвовавшего в проектировании.

2 При планировании оценки функциональной безопасности необходимо рассмотреть:

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

5.2.6.1.3 В ходе планирования безопасности следует определить те стадии жизненного цикла безопасности, на которых необходимо выполнять действия по оценке функциональной безопасности.

Примечания

1 Если после модификации или периодически в процессе функционирования будут выявлены новые источники опасности, может оказаться необходимым провести дополнительные действия по оценке функциональной безопасности.

2 Действия по оценке функциональной безопасности должны быть выполнены на следующих стадиях жизненного цикла безопасности (см. рисунок 8):

Стадия 1. После выполнения оценки опасностей и рисков следует определить необходимые слои защиты и разработать спецификацию требований к безопасности.

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 всех действий по оценке функциональной безопасности должны зависеть от конкретных обстоятельств. Факторы, влияющие на эти решения, обычно включают:

- объем проекта;
- уровень его сложности;
- уровень полноты безопасности;
- продолжительность проекта;
- последствия в случае отказа;
- уровень стандартизации проектных решений;
- нормативные требования безопасности;
- предшествующий опыт выполнения подобных проектов.

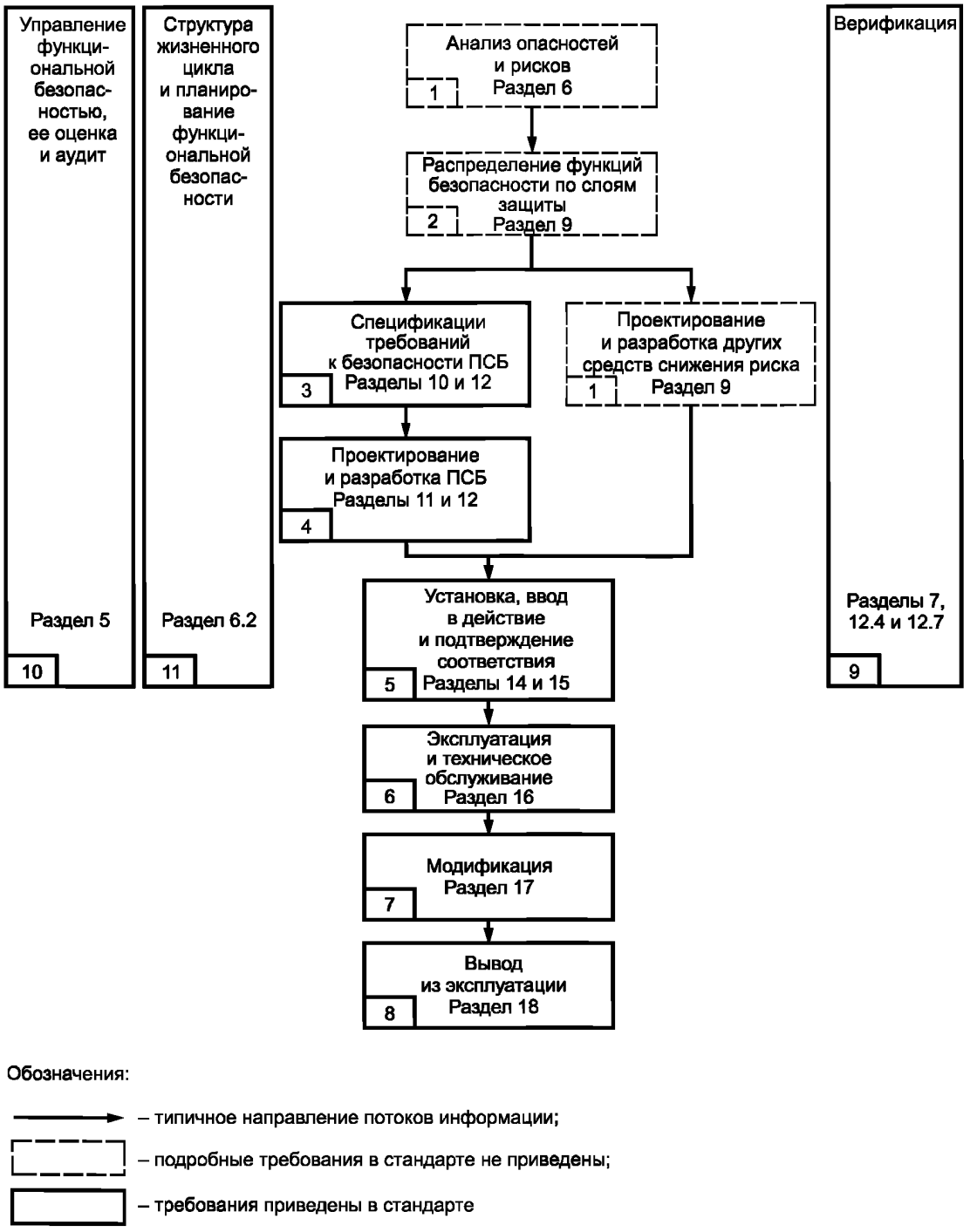


Рисунок 8 — Стадии жизненного цикла безопасности и стадии оценки функциональной безопасности ПСБ

5.2.6.1.4 По крайней мере должна быть предпринята одна попытка оценки функциональной безопасности. Такая оценка функциональной безопасности должна быть выполнена для того, чтобы быть уверенным, что опасности, возникающие в процессе и соответствующем оборудовании, находятся под должным управлением. Как минимум, оценивание следует выполнить перед определением имеющихся опасностей (т. е. на стадии 3). Команда специалистов, проводящих оценку, до возникновения выявленных опасностей должна подтвердить, что:

- оценка опасностей и рисков выполнена (см. 8.1);
- рекомендации, являющиеся результатом оценки 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 предыдущего анализа безопасности, выполнены;
- ПСБ спроектирована, создана и установлена в соответствии со спецификацией требований безопасности, 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 проведено и действия по подтверждению соответствия были выполнены;
- обучение персонала было выполнено и вся необходимая информация о ПСБ обслуживающему и оперативному персоналу предоставлена;
- планы или стратегии проведения последующих работ по оцениванию функциональной безопасности имеются.

5.2.6.1.5 Инструментальные средства разработки и изготовления, используемые для любого действия, выполняемого на любой стадии жизненного цикла безопасности, сами должны быть подвергнуты оценке функциональной безопасности.

Примечания

1 Глубина оценивания таких средств должна зависеть от их влияния на достигаемую безопасность.

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

3 Оценка функциональной безопасности инструментальных средств включает в себя, но не ограничивается проверкой прослеживаемости калибровочных эталонов, истории эксплуатации и журнала дефектов.

5.2.6.1.6 Результаты оценки функциональной безопасности должны быть доступными вместе с любыми рекомендациями, вытекающими из этой оценки.

5.2.6.1.7 Участники команды специалистов, проводящих оценку функциональной безопасности, должны иметь доступ по их запросу ко всей информации, относящейся к этой работе.

5.2.6.2 Аудит и проверка

5.2.6.2.1 Следует определить и выполнить процедуры для того, чтобы контролировать соответствие с требованиями, включая:

- частоту проведения аудита;
- степень независимости исполнителей действий по аудиту от лиц, подразделений, организаций и иных структур, выполняющих работы;
- регистрацию и последующие действия.

5.2.6.2.2 Должны быть установлены процедуры управления внесением изменений, включая их инициирование, документирование, проверку, внедрение и утверждение изменений в ПСБ, отличающиеся от замены на такое же (т. е. то же на то же).

5.2.7 Управление конфигурацией ПСБ

5.2.7.1 Требования

5.2.7.1.1 Должны быть установлены процедуры управления конфигурацией ПСБ, выполняемые в течение всех стадий жизненного цикла безопасности системы и ее ПО; в частности, должны быть определены:

- стадии, на которых следует проводить формальный контроль конфигурации;
- процедуры, применяемые для определения индивидуальных особенностей всех компонентов изделия (его аппаратных средств и ПО);
- процедуры для предотвращения использования компонентов, не имеющих разрешения.

6 Требования к жизненному циклу безопасности

6.1 Цели

Цели данного раздела следующие:

- определить стадии и установить требования к действиям жизненного цикла безопасности;
- упорядочить технические действия в жизненный цикл безопасности;
- убедиться, что существует (или разрабатывается) адекватный план, который дает уверенность в том, что ПСБ отвечает требованиям безопасности.

Примечание — Общий подход, принятый в настоящем стандарте, показан на рисунках 8, 10 и 11. Необходимо подчеркнуть, что этот подход приведен для иллюстрации и служит только для того, чтобы показать действия типичного жизненного цикла безопасности от появления начального замысла до вывода из эксплуатации.

6.2 Требования

6.2.1 Жизненный цикл безопасности, предусмотренный требованиями настоящего стандарта, должен быть определен в процессе планирования работ по безопасности.

6.2.2 Для каждой стадии жизненного цикла безопасности должны быть определены входы, выходы, а также действия по верификации правильности ее выполнения (см. таблицу 2).

6.2.3 Для всех стадий жизненного цикла безопасности необходимо выполнять планирование безопасности для определения критериев, способов, показателей и процедур, чтобы:

- обеспечить выполнение требований безопасности ПСБ (и к функциям, и к полноте безопасности) для всех соответствующих состояний процесса;
- обеспечить правильный монтаж и приемку ПСБ;
- обеспечить полноту безопасности функции безопасности ПСБ после ее установки на объекте;
- поддерживать полноту безопасности в процессе функционирования ПСБ (например, проверочные испытания, анализ отказов);
- управлять опасностями процесса в ходе технического обслуживания ПСБ.

7 Верификация

7.1 Цель

Цель данного раздела состоит в том, чтобы продемонстрировать с помощью рассмотрения, анализа и/или испытаний, что требуемые выходные результаты соответствующих стадий (рисунок 8) жизненного цикла безопасности удовлетворяют установленным требованиям, определенным с помощью планирования верификации.

Таблица 2 — Обзор жизненного цикла безопасности ПСБ

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 8)	Цели	Требования. Номер раздела, подраздела	Входы	Выходы
1 Анализ опасностей и рисков	Определить опасности и опасные события процесса и связанного с ним оборудования. Определить последовательность событий, приводящих к опасным событиям. Определить риски процесса, связанные с опасным событием. Определить требования по снижению риска и к функциям безопасности для достижения необходимого сокращения риска	8	Проект процесса, его размещение, состав персонала, заданная безопасность	Описания опасностей, требуемой(ых) функции(й) безопасности и соответствующего снижения риска

Окончание таблицы 2

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 8)	Цели	Требования. Номер раздела, подраздела	Входы	Выходы
2 Распределение функций безопасности по слоям защиты	Распределить функции безопасности по уровням защиты и для каждой функции безопасности ПСБ, назначить уровень полноты безопасности	9	Описание необходимой(ых) функции (й) безопасности и соответствующих требований к полноте безопасности	Описание распределения требований к безопасности (см. раздел 9)
3 Спецификация требований к безопасности ПСБ	Установить для каждой ПСБ требования к функциям безопасности и их полноте безопасности, необходимые для достижения требуемой функциональной безопасности	10	Описание распределения требований к безопасности (см. раздел 9)	Требования к безопасности ПСБ. Требования к безопасности ПО
4 Проектирование и разработка ПСБ	Спроектировать ПСБ, отвечающую требованиям к функциям безопасности ПСБ и к полноте безопасности	11 и 12.4	Требования к безопасности ПСБ. Требования к безопасности программного обеспечения	Проект ПСБ, отвечающий требованиям к безопасности. План тестирования ПСБ в целом
5 Установка, ввод в действие и подтверждение соответствия безопасности ПСБ	Собрать и испытать ПСБ. Проверить соответствие ПСБ требованиям безопасности в части требуемых функций безопасности и требуемой полноты безопасности	12.3, 14, 15	Проект ПСБ. План тестирования ПСБ в целом. Требования к безопасности ПСБ. План подтверждения соответствия безопасности ПСБ	Полное функционирование ПСБ в соответствии с ее проектом. Результаты комплексных испытаний. 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	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 уровня безопасности	17	Скорректированные требования по безопасности ПСБ	Результаты модификации ПСБ
8 Снятие с эксплуатации	Обеспечить правильную проверку, организацию работ и сохранность ПСБ	18	Информация о процессе и требованиях к его безопасности	ПСБ, выведенная из обслуживания
9 Верификация ПСБ	Провести испытания и оценить результаты конкретной стадии, чтобы обеспечить правильность и соответствие изделий исходным для данной стадии регламентирующим документам	7, 12.7	План верификации ПСБ на каждой стадии	Результаты верификации ПСБ на каждой стадии
10 Оценка функциональной безопасности	Обследовать ПСБ и дать заключение о достигнутой функциональной безопасности	5	Планирование оценки функциональной безопасности ПСБ. Требования к безопасности ПСБ	Результаты оценки функциональной безопасности ПСБ

7.1.1 Требования

План верификации должен определять все действия, необходимые для каждой стадии (рисунок 8) жизненного цикла безопасности. План верификации должен соответствовать настоящему стандарту, включая следующие требования:

- действия по верификации;
- процедуры, показатели и способы, которые будут использованы для верификации, включая внедрение и утверждение итоговых рекомендаций;
- время выполнения указанных действий;
- определение отдельных лиц, подразделений и организаций, несущих ответственность за выполнение этих действий, включая уровни их независимости;
- определение объектов, подлежащих верификации;
- определение информации, используемой при выполнении верификации;
- способы преодоления несоответствий;
- средства поддержки анализа.

7.1.1.1 Верификация должна быть выполнена согласно плану верификации.

7.1.1.2 Результаты процесса верификации должны быть доступны.

Примечания

1 Выбор способов и показателей проведения верификации и степени независимости ее исполнителей зависит от ряда факторов, включая степень сложности, новизну проекта, новизну технологии, требуемый уровень полноты безопасности.

2 Примерами некоторых действий по верификации являются: анализ проекта, применение программных средств и способов верификации, включая средства автоматизированного проектирования.

8 Анализ опасностей и рисков процесса

8.1 Цели

Цели требований данного 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 функциями безопасности ПСБ (см. раздел 9).

Примечания

1 Раздел 8 настоящего стандарта 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 функций безопасности ПСБ.

2 Если это практически достижимо, процессы следует проектировать как изначально безопасные. В тех случаях, когда это невозможно, может оказаться необходимым введение в проект таких способов снижения риска, как механические системы защиты и ПСБ. Такие системы могут действовать самостоятельно или в комбинации друг с другом.

3 Типовые методы снижения риска, используемые в промышленных процессах на предприятиях, показаны на рисунке 9 (без отражения иерархии).

8.2 Требования

8.2.1 Для процесса и связанного с ним оборудования (например, ОСУП) следует провести анализ опасностей и риска, в результате выполнения которого:

- должны быть получены описания каждого определенного опасного события и влияющих на него факторов (включая ошибки человека);
- должно быть проведено описание последствий и правдоподобности события;
- должны быть рассмотрены условия, такие как условия нормальной работы, запуска, останова, обслуживания, запуска процесса, аварийного останова;

- должны быть установлены требования по дополнительному снижению риска, необходимому для достижения требуемой безопасности;

- должно быть проведено 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 вероятные интенсивности запросов и интенсивности отказов оборудования, а также любые сведения об ограничениях условий работы и вмешательстве человека;

- должно быть принято распределение функций безопасности по слоям защиты (см. раздел 9), учитывающее возможное снижение эффективности защиты, вызванное отказом по общей причине, возможным как между разными слоями защиты, так и между этим слоями и ОСУП (см. примечание 1);

- должны быть определены те функции безопасности, которые реализуются как функции безопасности ПСБ (см. раздел 9).

Примечания

1 При определении требований к полноте безопасности необходимо учесть влияние общих причин на системы, которые генерируют запросы, и системы защиты, разработанные, чтобы реагировать на эти запросы. Например, запросы могут возникнуть в результате отказа в системе управления, а оборудование, используемое в системе защиты, аналогично или идентично оборудованию, используемому в системе управления. В таких случаях на запрос, вызванный отказом оборудования в системе управления, 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 системы защиты еще не будет выполнена. Однако при определении соответствия проекта процесса и слоев защиты требованиям необходимо рассмотреть отказы по общей причине.

2 Примеры способов, которые могут быть использованы при установлении требований к УПБ приборных функций безопасности, приведены в [6].

8.2.2 Интенсивность опасных отказов ОСУП (не подпадающих под действие МЭК 61511), которая определяет потребность в слое защиты, не следует принимать больше чем 10^{-5} в час.

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

Примечания

1 Перечисленные выше требования не означают, что риск и заданное снижение риска должны быть оценены в количественных величинах. Допустимо также применение графических подходов (см. [6]).

2 Степень необходимого снижения риска зависит от особенностей применения и требований национального законодательства. Во многих странах принят следующий принцип: дополнительные меры по сокращению риска необходимо применять, пока их стоимость не становится непропорциональной достигнутому сокращению риска.

9 Распределение функций безопасности по слоям защиты

9.1 Цели

Цели требований данного раздела следующие:

- распределить функции безопасности по слоям защиты;
- определить необходимые функции безопасности ПСБ;
- определить для каждой функции безопасности ПСБ соответствующий УПБ.

Примечание — В процессе размещения следует учитывать другие отраслевые стандарты или нормы.

9.2 Требования к процессу распределения

9.2.1 Процесс распределения должен обеспечить:

- распределение функций безопасности по определенным слоям защиты в целях предотвращения, управления или уменьшения опасностей, возникающих в процессе и в его соответствующем оборудовании;

- распределение целевых сокращений риска по функциям безопасности ПСБ.

Примечание — Приоритеты в процессе размещения могут быть определены требованиями законодательства или другими отраслевыми нормами.

9.2.2 Требуемый УПБ функции безопасности ПСБ должен быть определен с учетом требуемого снижения риска, которое должно быть достигнуто с помощью этой функции.

Примечание — См. руководящие указания в [6].

9.2.3 Для каждой функции безопасности ПСБ, выполняемой в режиме по запросу, требуемый УПБ следует установить в соответствии с таблицей 3 или 4. Если используют таблицу 4, то при определении УПБ ни длительность контрольных испытаний, ни интенсивность запросов не следует применять.

9.2.4 Для каждой функции безопасности ПСБ, выполняемой в непрерывном режиме, требуемый УПБ следует устанавливать в соответствии с таблицей 4.

Таблица 3 — Уровни полноты безопасности: вероятность отказа по запросу

Режим работы по запросу		
Уровень полноты безопасности (УБП)	Целевая средняя вероятность отказа выполнения функции по запросу	Целевое сокращение риска
4	$\geq 10^{-5} — < 10^{-4}$	> 10 000 — ≤ 100 000
3	$\geq 10^{-4} — < 10^{-3}$	> 1 000 — ≤ 10 000
2	$\geq 10^{-3} — < 10^{-2}$	> 100 — ≤ 1 000
1	$\geq 10^{-2} — < 10^{-1}$	> 10 — ≤ 100

Таблица 4 — Уровни полноты безопасности: частота опасных отказов функции безопасности ПСБ

Непрерывный режим работы	
Уровень полноты безопасности (УБП)	Целевая частота опасных отказов функции безопасности ПСБ (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 в 3.2.43.

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

3 Требуемая целевая частота опасных отказов в час функции безопасности ПСБ в режиме непрерывных запросов определяется путем рассмотрения риска (в единицах интенсивности опасных событий), вызванного отказами функции безопасности ПСБ, выполняемой в непрерывном режиме, совместно с интенсивностью отказов другого оборудования, которое приводит к такому же риску, с учетом вкладов от других уровней защиты.

4 Возможно использовать несколько систем с более низким УПБ, чтобы удовлетворить потребность в функции безопасности с более высоким УПБ (например, совместно использовать системы с УПБ 2 и УПБ 1, чтобы удовлетворить потребность в функции безопасности с УПБ 3).

9.3 Дополнительные требования для уровня полноты безопасности 4

9.3.1 ПСБ не следует поручать функций безопасности с более высоким УПБ, чем соответствующий УПБ 4. Приложения, в которых требуется использование одиночной функции безопасности ПСБ с УПБ 4, редки в промышленных процессах. Подобных случаев, если это практически возможно, следует избегать из-за трудности достижения и поддержания столь высокого качества функционирования на всем жизненном цикле безопасности. Кроме того, такие системы потребуют высокой компетентности от всех специалистов, принимающих участие в работах на всем жизненном цикле безопасности.

Если по результатам анализа УПБ 4 был определен для функции безопасности ПСБ, необходимо рассмотреть возможность таких изменений в проекте процесса, которые повышают внутреннюю безопасность или вводят дополнительные слои защиты. Такие изменения, возможно, смогут понизить требования к УПБ, предъявляемой к функции безопасности ПСБ.

9.3.2 Реализация функции безопасности ПСБ с УПБ 4 допустима, если только выполняются или критерий a), или критерии b) и c) вместе, которые представлены ниже:

a) с помощью комбинации соответствующих аналитических методов и тестированием явно показано, что целевая мера отказов полноты безопасности выполняется;

b) существует большой эксплуатационный опыт применения компонентов, используемых для выполнения функции безопасности ПСБ.

Примечание — Такой опыт должен быть получен при аналогичных условиях окружающей среды и, как минимум, компоненты должны использоваться в системе, имеющей сопоставимый уровень сложности;

c) существуют обширные данные об отказах технических средств, полученные для компонентов, используемых для выполнения функции безопасности ПСБ, и позволяющие достаточно достоверно утверждать, что показатели отказов этих средств соответствуют заявленным.

Примечание — Эти данные должны быть применимы для предложенных условий окружающей среды, случая применения и уровня сложности.

9.4 Требования к основной системе управления процессом как к слою защиты

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



Рисунок 9 — Типовые методы снижения риска, используемые в промышленных процессах на предприятиях

9.4.2 Коэффициент снижения риска для ОСУП (который не подпадает под действие МЭК 61511 или МЭК 61508), применяемой в качестве уровня защиты, должен быть ниже 10.

Примечание — При рассмотрении снижения риска, которое можно доверить ОСУП, следует уделить внимание тому факту, что любые части ОСУП могут также быть источниками нежелательных событий.

9.4.3 Если коэффициент снижения риска с помощью ОСУП оказывается больше 10, ее следует разрабатывать в соответствии с требованиями настоящего стандарта.

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

9.5.1 Должен быть проанализирован проект слоев защиты для того, чтобы обеспечить достаточно низкую вероятность появления отказов по общей причине, отказов общего вида и зависимых отказов для слоев защиты и ОСУП по сравнению с общим уровнем требований к полноте безопасности слоев защиты. Оценка может быть дана в количественном или качественном виде.

Примечание — Определение зависимого отказа см. в 3.2.12.

9.5.2 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 (например, может ли закупоривание предохранительного клапана вызвать такие же проблемы, что и засорение датчика в ПСБ).

10 Спецификация требований к безопасности ПСБ

10.1 Цель

Целью данного раздела является спецификация требований для функции(й) безопасности ПСБ.

10.2 Основные требования

10.2.1 Требования безопасности должны быть установлены в результате распределения функций безопасности ПСБ и определены в ходе планирования безопасности.

Примечание — 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 теми, кто обычно пользуется ими на любой стадии жизненного цикла.

10.3 Требования к безопасности ПСБ

10.3.1 Эти требования должны быть достаточны для проектирования ПСБ и должны включать:
- описание всех функций безопасности ПСБ, необходимых для достижения требуемой функциональной безопасности;
- требования для определения и учета отказов по общей причине;
- определение безопасного состояния процесса для каждой установленной функции безопасности ПСБ;
- определение любых таких по отдельности безопасных состояний процесса, которые, если совпадают во времени, создают опасность (например, переполнение аварийной памяти, повторяющийся перезапуск системы);
- принятые источники запросов и интенсивность запросов на срабатывание функции безопасности ПСБ;
- требование к интервалу времени между тестовыми испытаниями;
- требования к быстродействию срабатывания ПСБ, необходимому для перевода процесса в безопасное состояние;
- УПБ и режим выполнения (по запросу/непрерывный) для каждой функции безопасности ПСБ;
- описание измерений параметров процесса в ПСБ и их особых точек;
- описание выходных воздействий, выполняемых ПСБ, и критериев их успешного выполнения (например, требования к плотности отсечных клапанов);
- функциональные отношения между входами и выходами процесса, включая логику, математические функции и любые необходимые рекомендации;
- требования для останова в ручном режиме;
- требования, связанные с включением или выключением питания;
- требования к установке ПСБ в исходное состояние после ее отключения;
- максимально допустимая интенсивность ложных срабатываний;

- режимы отказов и желательная реакция 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 определение функций безопасности ПСБ, работающих в каждом режиме;
- требования к прикладному ПО безопасности в соответствии с 12.2.2;
- требования к отменам/задержкам/пропускам, включая указания, как их следует устранять;
- спецификацию любого действия, необходимого для достижения или поддержки безопасного состояния в случае ошибки(ок), обнаруженной ПСБ. Любое такое действие должно быть установлено с учетом всех соответствующих человеческих факторов;
- среднее время ремонта, достижимое для данной ПСБ, с учетом времени прибытия, обнаружения, получения запасных частей, обслуживания, а также внешних ограничений;
- установление опасных комбинаций выходных состояний ПСБ, которые необходимо предотвратить;
- предельные значения всех условий окружающей среды, с которыми может столкнуться ПСБ. Это может потребовать рассмотрения следующих параметров: температура, влажность, загрязненность, заземление, электромагнитные и радиочастотные помехи, удары/вибрации, электростатические разряды, классификация электрических зон, наводнение, молния и другие факторы;
- установление нормальных и аномальных режимов работы как для установки в целом (например, пуск установки), так и для отдельных эксплуатационных процедур (например, обслуживание, калибровка и/или ремонт датчика). Для поддержки этих режимов работы могут потребоваться дополнительные функции безопасности ПСБ;
- определение требований, предъявляемых к любой функции безопасности ПСБ, необходимой для того, чтобы перенести наиболее крупные инциденты (например, требуемое время сохранения работоспособности клапана в случае пожара).

Примечание – ПСБ может выполнять функции, не связанные с безопасностью, чтобы обеспечить правильный останов или быстрый запуск. Но такие функции должны быть отделены от функций безопасности ПСБ.

10.3.2 Перечень требований безопасности, предъявляемых к ПО, следует устанавливать исходя из общего перечня требований безопасности и выбранной архитектуры ПСБ.

11 Проектирование и разработка ПСБ

11.1 Цель

Целью данного раздела является спецификация требований для проектирования одной или нескольких ПСБ, выполняющей(их) функцию(и) безопасности и удовлетворяющей(их) указанному(ым) уровню(ям) полноты безопасности.

11.2 Основные требования

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

11.2.2 Если ПСБ должна осуществлять и функцию(и) безопасности ПСБ, и функцию(и), не связанную(ые) с безопасностью, то все аппаратные средства и ПО, которые могут негативно повлиять на любую функцию безопасности ПСБ при нормальных условиях и в случае сбоя, должны рассматриваться как часть ПСБ и быть выполнены в соответствии с требованиями самого высокого УПБ.

Примечания

1 Везде, где практически возможно, функции безопасности ПСБ должны быть отделены (адекватно независимы) от функций ПСБ, не связанных с безопасностью.

2 Адекватная независимость означает, что ни отказ любых не связанных с безопасностью функций, ни программный доступ к не связанным с безопасностью функциям ПО не приводят к опасному отказу функций безопасности ПСБ.

11.2.3 Если ПСБ должна выполнять функции безопасности ПСБ с различными УПБ, тогда общедоступные или общие аппаратные средства и ПО должны соответствовать самому высокому УПБ, если нельзя будет показать, что функции безопасности ПСБ с более низким УПБ не могут негативно влиять на функции безопасности ПСБ с более высокими УПБ.

11.2.4 Если не предполагается квалифицировать ОСУП как удовлетворяющую настоящему стандарту, то она должна быть спроектирована так, чтобы ОСУП была отделена и независима до такой степени, чтобы не нарушалась функциональная полнота ПСБ.

Примечания

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

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

11.2.5 В процессе проектирования ПСБ должны быть реализованы требования по оперативности, обслуживаемости и проверяемости, чтобы облегчить выполнение в проекте требований к человеческому фактору (например, использование байпаса при испытаниях и аварийной сигнализации, если он включен).

Примечание — Средства обслуживания и проверок следует спроектировать так, чтобы свести к минимуму, насколько это практически возможно, вероятность опасных отказов, возникающих от их использования.

11.2.6 Проект ПСБ должен учитывать возможности и ограничения человека и задачи, поручаемые операторам и обслуживающему персоналу. Проект всех человекомашинных интерфейсов должен быть рассчитан на применение положительного практического опыта и реального уровня тренированности и обученности, получаемого операторами.

11.2.7 ПСБ должна быть спроектирована так, чтобы, как только она перевела процесс в безопасное состояние, процесс оставался в безопасном состоянии до начала его переустановки в исходное состояние или до другого события, установленного в спецификациях требований к безопасности.

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 спецификациях требований по безопасности.

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

11.2.10 Любое устройство, использующееся для выполнения части функции безопасности ПСБ, не должно использоваться для целей основного управления в тех случаях, когда отказ этого устройства приведет к отказу функции основной системы управления, который порождает запрос на срабатывание функции безопасности ПСБ, если только не 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 на функцию, выполняемую ПСБ, то появляется новый риск. Величина дополнительного риска зависит от интенсивности опасных отказов общего оборудования, так как если в общем оборудовании 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 используемого оборудования достаточно низка. В качестве примеров такого оборудования, общего с ОСУП, часто рассматривают датчики и клапаны.

11.2.11 В подсистемах, для которых потеря электропитания выводит их из безопасного состояния, должны быть выполнены все следующие требования и предприняты действия, указанные в 11.3:

- обнаружить потерю целостности цепи (например, контроль разрыва цепи);
- обеспечить непрерывность работы источника электропитания, используя дополнительный источник электропитания (например, резервную батарею, источники бесперебойного питания);
- обнаружить потерю электропитания в подсистеме.

11.3 Требования к поведению системы при обнаружении отказа

11.3.1 Обнаружение опасного отказа (диагностическими тестами, контрольными проверками или любыми другими средствами) в любой подсистеме, в которой допустим единичный аппаратный отказ, должно приводить к одному из следующих результатов:

a) к конкретному действию, направленному на достижение или поддержание безопасного состояния (см. примечание); или

b) к продолжению безопасного выполнения процесса на все время, пока дефектная часть не будет отремонтирована. Если ремонт дефектной части не будет завершен за среднее время восстановления,

принятое в расчете вероятности случайных отказов технических средств, то должно быть выполнено определенное действие, направленное на достижение или поддержание безопасного состояния (см. примечание).

В тех случаях, когда указанные выше действия зависят от определенных действий оператора, выполняемых в ответ на предупредительную сигнализацию (например, открывание или закрывание клапана), такая сигнализация должна рассматриваться как часть ПСБ (т. е. должна быть независимой от ОСУП).

В тех случаях, когда указанные выше действия заключаются в подаче оператором заявки обслуживающему персоналу отремонтировать неисправную систему в ответ на сигнализацию результата диагностики, такая сигнализация может быть частью ОСУП, но для нее должны быть выполнены соответствующие проверочные испытания и процедуры управления изменениями, как и для ПСБ.

Примечание — Указанное действие (реакция на сбой), необходимое для достижения или поддержания безопасного состояния, должно быть установлено в требованиях к безопасности (см. 10.3). Оно может заключаться, например, в безопасном завершении процесса или его неисправной части для снижения риска на дефектной подсистеме или в другом конкретном запланированном действии, ослабляющем последствия сбоя.

11.3.2 Обнаружение опасного отказа (диагностическим тестом, контрольными проверками или любыми другими средствами) в любой подсистеме, не имеющей резервирования, функция безопасности которой является полностью зависимой (см. примечание 1), должно, если подсистема выполняет только функцию(и) безопасности ПСБ в режиме запроса, завершаться или:

a) конкретным действием для достижения и поддержания безопасного состояния, или

b) восстановлением дефектной подсистемы в течение среднего времени восстановления, принятого при расчете вероятности случайных отказов аппаратных средств. В течение этого времени безопасность процесса должна непрерывно обеспечиваться дополнительными мерами и ограничениями. Снижение риска, обеспечиваемое этими мерами и ограничениями, должно быть по крайней мере равным снижению риска, обеспечиваемому ПСБ в отсутствие любых отказов. Такие дополнительные меры и ограничения должны быть определены в процедурах эксплуатации и технического обслуживания ПСБ. Если восстановление за установленное среднее время восстановления не завершается, следует выполнить определенное действие, направленное на достижение или поддержание безопасного состояния (см. примечание 2).

В тех случаях, когда указанные выше действия зависят от определенных действий оператора, выполняемых в ответ на предупредительную сигнализацию (например, открывание или закрывание клапана), такая сигнализация должна рассматриваться как часть ПСБ (т. е. должна быть независимой от ОСУП).

В тех случаях, когда указанные выше действия заключаются в подаче оператором заявки обслуживающему персоналу отремонтировать неисправную систему в ответ на сигнализацию результата диагностики, такая сигнализация может быть частью ОСУП, но для нее должны быть выполнены соответствующие проверочные испытания и процедуры управления изменениями, как и для ПСБ.

Примечания

1 Предполагается, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы приводит к отказу функции безопасности рассматриваемой ПСБ, и функция безопасности ПСБ не была распределена между другими слоями защиты.

2 Указанное действие (реакция на сбой), необходимое для достижения или поддержания безопасного состояния, должно быть установлено в требованиях к безопасности (см. 10.3). Оно может заключаться, например, в безопасном завершении процесса или его неисправной части для снижения риска на дефектной подсистеме или в другом конкретном запланированном действии, ослабляющем последствия сбоя.

11.3.3 Обнаружение опасного сбоя (диагностическим тестом, контрольными проверками или любыми другими средствами) в любой подсистеме, не имеющей резервирования, в которой функция безопасности является зависимой (см. примечание 1), в случае подсистемы, выполняющей любую функцию(и) безопасности ПСБ, действующей(их) в режиме с высокой частотой запросов или в непрерывном режиме (см. примечание 2), должно приводить к определенному действию, направленному на достижение или поддержание безопасного состояния.

Указанное действие (реакция на сбой), необходимое для достижения или поддержания безопасного состояния, должно быть установлено в требованиях к безопасности. Оно может заключаться, например, в безопасном завершении процесса или его неисправной части для снижения риска на дефектной подсистеме или в другом конкретном запланированном действии, ослабляющем последствия сбоя. Суммарное время обнаружения сбоя и выполнения такого действия должно быть меньше, чем время появления опасного события.

В тех случаях, когда указанные выше действия зависят от определенных действий оператора, выполняемых в ответ на предупредительную сигнализацию (например, открывание или закрывание клапана), такая сигнализация должна рассматриваться как часть ПСБ (т. е. должна быть независимой от ОСУП).

В тех случаях, когда указанные выше действия заключаются в подаче оператором заявки обслуживающему персоналу отремонтировать неисправную систему в ответ на сигнализацию результата диагностики, такая сигнализация может быть частью ОСУП, но для нее должны быть выполнены соответствующие проверочные испытания и процедуры управления изменениями, как и для ПСБ.

Примечания

1 Предполагается, что функция безопасности полностью зависит от подсистемы, если отказ подсистемы приводит к отказу функции безопасности, рассматриваемой приборной системы безопасности, и функция безопасности ПСБ не была распределена между другими слоями защиты (см. раздел 9).

2 Если имеется вероятность, что некоторая комбинация состояний выходов подсистемы может стать непосредственной причиной опасного события, то обнаружение опасных отказов в подсистеме необходимо рассматривать как для функции безопасности ПСБ, действующей в непрерывном режиме.

11.4 Требования к отказоустойчивости аппаратных средств

11.4.1 Для функций безопасности ПСБ датчики, логические устройства и исполнительные элементы должны иметь минимальную аппаратную отказоустойчивость.

Примечания

1 Аппаратная отказоустойчивость — способность компонента или подсистемы продолжать выполнять требуемую функцию безопасности ПСБ при наличии в нем(й) одного или более опасных отказов. Аппаратная отказоустойчивость, равная единице, означает, что существуют, например, два устройства и что структура такова, что опасный отказ одного из двух компонентов не препятствует выполнению действий по безопасности.

2 Минимальное допустимое число отказов оборудования определяется для того, чтобы сократить влияние возможных недостатков в проекте функция безопасности ПСБ, которые могут возникнуть из-за ряда допущений, принятых в ходе разработки, вместе с неопределенностью в интенсивности отказов компонентов или подсистем, применяемых в различных процессах.

3 Важно отметить, что требования отказоустойчивости аппаратных средств представлены для компонента или подсистемы с минимальный избыточностью. В зависимости от специфики применения, интенсивности отказов и интервала между контрольными проверками компонента может потребоваться дополнительная избыточность, обеспечивающая выполнение данной ПСБ требований по УПБ, в соответствии с 11.9.

11.4.2 Минимальная отказоустойчивость аппаратных средств логических устройств с программируемой электроникой представлена в таблице 5.

Таблица 5 — Минимальное допустимое число отказов для программируемой электроники логических устройств

УПБ	Минимальное допустимое число отказов		
	ДБО < 60 %	60 % ≤ ДБО ≤ 90 %	ДБО > 90 %
1	1	0	0
2	2	1	0
3	3	2	1
4	Применяются специальные требования (см. МЭК 61508)		

11.4.3 Все подсистемы (например, датчики, исполнительные элементы, непрограммируемые логические устройства), кроме логических устройств с ПЭ, должны иметь минимальную отказоустойчивость аппаратных средств, как показано в таблице 6, и при этом обеспечить выявление отказов преимущественного вида, происходящих в безопасном состоянии, или опасных отказов (см. 11.3), иначе отказоустойчивость должна быть увеличена на единицу.

Примечание — Чтобы установить, относятся ли отказы в безопасном состоянии к преимущественному виду, необходимо рассмотреть каждый из следующих пунктов:

- соединение процесса и данного устройства;
- использование диагностической информации устройства для подтверждения соответствия сигнала от процесса;
- использование естественно (внутренне) безопасного поведения устройства (например, обнуление сигнала или потерю питания, приводящие к переходу в безопасное состояние).

11.4.4 Для всех подсистем (например, датчики, исполнительные элементы, непрограммируемые логические устройства), исключая логические устройства с ПЭ, минимальная отказоустойчивость, установленная по таблице 6, может быть уменьшена на единицу, если используемое устройство выполнено с соблюдением всех следующих пунктов:

- аппаратные средства устройства выбраны на основе предшествующего опыта использования (см. 11.5.3);
- устройство имеет настройки только таких параметров, которые зависят от процесса (например, диапазон измерения, прямая или обратная шкала);
- настройки параметров устройства, зависящих от процесса, защищены, например использованием перемычки или пароля;
- к уровню безопасности функции предъявляются требования ниже, чем УПБ 4.

Таблица 6 — Минимальное допустимое число отказов для датчиков, исполнительных элементов и логических устройств с непрограммируемой электроникой

УПБ	Минимальное допустимое число отказов для аппаратных средств (см. 11.4.3 и 11.4.4)
1	0
2	1
3	2
4	Применяются специальные требования (см. МЭК 61508)

11.4.5 Могут быть использованы иные требования к отказоустойчивости при условии, что обеспечено проведение оценки в соответствии с требованиями МЭК 61508-2 (таблицы 2 и 3).

11.5 Требования к выбору компонентов и подсистем

11.5.1 Цели

11.5.1.1 Первая цель требований данного подраздела состоит в том, чтобы установить требования для выбора компонентов или подсистем, которые должны быть использованы в ПСБ.

11.5.1.2 Вторая цель требований данного подраздела состоит в том, чтобы установить требования к интеграции компонентов или подсистем в структуру ПСБ.

11.5.1.3 Третья цель требований данного подраздела состоит в том, чтобы определить критерии пригодности компонентов и подсистем в терминах соответствующих функций безопасности ПСБ и полноты безопасности.

11.5.2 Общие требования

11.5.2.1 Компоненты и подсистемы, выбираемые для использования в ПСБ для приложений со значениями УПБ от 1 до 3, должны либо соответствовать требованиям МЭК 61508-2 и МЭК 61508-3, либо в противном случае отвечать требованиям 11.4 и 11.5.3 — 11.5.6 (когда это целесообразно).

11.5.2.2 Компоненты и подсистемы, выбираемые для использования в ПСБ для приложений со значением УПБ 4, должны соответствовать требованиям МЭК 61508-2 и МЭК 61508-3 (когда это целесообразно).

11.5.2.3 Пригодность выбранных компонентов и подсистем должна быть продемонстрирована с помощью анализа:

- документации изготовителей аппаратных средств и встроенного ПО;
- выбора подходящего прикладного языка и инструментальных средств (см. 12.4.4), если это необходимо.

11.5.2.4 Компоненты и подсистемы должны соответствовать перечню требований к безопасности ПСБ.

Примечание — При выборе компонентов и подсистем применяют все соответствующие требования настоящего стандарта, включая архитектурные ограничения, к целостности аппаратных средств, поведению при обнаружении сбоя и прикладному ПО.

11.5.3 Требования для выбора компонентов и подсистем на основе опыта их предшествующего применения

11.5.3.1 Необходимо располагать доказательствами того, что компоненты и подсистемы пригодны для использования в составе ПСБ.

Примечания

1 Для внешних элементов может существовать обширный опыт их работы в безопасных или небезопасных приложениях. Это может быть использовано как основание для доказательства.

2 Уровень подробности доказательства следует выбирать в соответствии со сложностью рассматриваемого компонента или подсистемы и при вероятности отказов, необходимой для достижения требуемого УПБ функции безопасности ПСБ.

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 характеристик компонентов или подсистем;
- демонстрацию функционирования компонентов или подсистем в аналогичных рабочих условиях и окружающей среде.

Примечание — Внешние устройства (например, датчики и исполнительные элементы) выполняют заданные функции, которые в системах безопасности и в системах, не связанных с безопасностью, обычно идентичны, что означает, что устройство будет работать подобным способом в обоих типах приложений. Поэтому рассмотрение функционирования таких устройств в составе систем, не связанных с безопасностью, также может считаться выполнением данного требования;

- объем опыта эксплуатации.

Примечание — 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;
- в журнал включают только подходящие случаи применения.

11.5.4 Требования к выбору программируемых на ФЯП компонентов и подсистем (например, внешних устройств) на основе опыта их применения

11.5.4.1 Применимы требования, установленные в 11.5.2 и 11.5.3.

11.5.4.2 При доказательстве пригодности следует выявить неиспользуемые характеристики компонентов и подсистем и установить, что они едва ли могут порождать опасность при выполнении требуемых функций безопасности ПСБ.

11.5.4.3 Для доказательства пригодности конкретной конфигурации и конкретных условий работы аппаратных средств и ПО следует рассмотреть:

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

11.5.4.4 Для приложений с УПБ 3 должна быть выполнена формальная оценка устройства, использующего ФЯП (в соответствии с 5.2.6.1), 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.

11.5.4.5 В случаях применения с УПБ 3 должно быть разработано руководство по безопасности, содержащее ограничения на функционирование, обслуживание и обнаружение неисправностей, а также типовые конфигурации и предполагаемые условия работы устройства, использующего ФЯП.

11.5.5 Требования к выбору компонентов и подсистем, использующих ЯОИ (например, логических устройств), на основе опыта их применения

11.5.5.1 Приведенные ниже требования предъявляют только к логическим устройствам с программируемой электроникой, используемым в ПСБ, предназначенных для выполнения функций безопасности с УПБ 1 и УПБ 2.

11.5.5.2 Применяют требования, установленные в 11.5.4.

11.5.5.3 Если существует какое-либо различие между условиями работы и окружающей среды компонента или подсистемы, использованных ранее, и условиями работы и окружающей среды компонента или подсистемы, применяемых в ПСБ, тогда 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 ошибок в ПСБ достаточно мала.

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

- УБП функции безопасности ПСБ;
- сложность и функциональные возможности компонента или подсистемы.

Примечание — Дополнительные руководящие указания см. в МЭК 61511-2.

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

- понимание того, какие отказы относятся к опасным видам;
- применение способов конфигурации, учитывающих установленные виды отказов;
- использование встроенного ПО, имеющего хорошую историю применения на опасных объектах;
- защита против несанкционированных или непреднамеренных изменений.

Примечание — Конфигурируемые логические устройства безопасности с ПЭ представляют собой программируемые электронные устройства общего назначения в промышленном исполнении, которые специально конфигурируются для применения на опасных объектах.

11.5.5.6 В случаях применения с УПБ 2 формальную оценку любого логического устройства с ПЭ, проводимую в соответствии с 5.2.6.1, следует выполнить так, чтобы показать, что:

- данное 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 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;
- защита кодов от изменений или обнаружение отказов с помощью оперативного мониторинга;
- программирование выявления отказов или разнотипное программирование;
- проверка диапазонов переменных или проверка 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 методов искусственного интеллекта, ни средств динамического изменения;
- документально оформленное выполнение проверки с введением неисправностей.

11.5.5.7 Для приложений с УПБ 2 необходимо располагать руководством по безопасности, содержащим ограничения на функционирование, обслуживание и обнаружение неисправностей, а также охватывающим типовые конфигурации и предполагаемые условия работы логического устройства с ПЭ.

11.5.6 Требования к выбору компонентов и подсистем, использующих ЯПИ (например, логических устройств)

11.5.6.1 Если в приложениях использован ЯПИ, то логические устройства с ПЭ должны соответствовать требованиям МЭК 61508-2 и МЭК 61508-3.

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 процессе или окружающей 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 Для обеспечения энергоснабжения цепей входа/выхода дискретных сигналов следует применять метод, гарантирующий целостность цепи и источника электропитания.

Примечание — Примером применения такого метода является контроль разрыва цепи, при котором вспомогательное устройство непрерывно контролирует целостность цепи, но при этом само не способно повлиять на значения сигналов входа/выхода.

11.6.3 Каждое отдельное внешнее устройство должно иметь свою собственную специально выделенную связь с системой ввода-вывода, кроме следующих случаев:

- несколько дискретных датчиков подсоединено последовательно к одному входу и все датчики контролируют одно и то же условие процесса (например, перегрузку двигателя);
- несколько исполнительных элементов подсоединено к одному выходу.

Примечание — Два клапана, подключенные к одному выходу, должны одновременно изменять свое состояние для всех функций безопасности ПСБ, использующих эти два клапана;

- для общей безопасной работы применяют цифровую шину, отвечающую требованиям полноты безопасности ПСБ.

11.6.4 Память интеллектуальных датчиков должна быть защищена от записи, чтобы предотвратить неосторожные изменения от удаленных источников, кроме тех случаев, когда проверка безопасности позволяет чтение/запись. Эта проверка должна учитывать человеческие факторы, такие, как неправильное выполнение процедур.

11.7 Интерфейсы

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

- интерфейсы оператора;
- интерфейсы обслуживания/разработки;
- коммуникационные интерфейсы.

11.7.1 Требования к интерфейсу оператора

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

11.7.1.2 При разработке ПСБ следует свести к минимуму необходимость выбора оператором опций и способов обхода системы при действующем объекте. 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 повторного подтверждения.

11.7.1.3 Доступ к переключателям линий обхода должен быть защищен ключами или паролями, чтобы предотвратить несанкционированное использование этой возможности.

11.7.1.4 Информация о состоянии ПСБ, которая важна для поддержки УПБ, 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.

11.7.1.5 Проект интерфейса оператора ПСБ должен быть таким, чтобы предотвратить изменения прикладного ПО ПСБ. Если информацию, связанную с безопасностью, необходимо передавать из ОСУП в ПСБ, то следует использовать средства, обеспечивающие селективную запись из ОСУП в специальные переменные ПСБ. Должны быть использованы такое оборудование и процедуры, которые позволяли бы подтвердить, что надлежащая селективная передача и прием (ПСБ) были выполнены надлежащим образом и отсутствует угроза функциональной безопасности ПСБ.

Примечания

1 Если опции или блокировки выбирают из ОСУП и загружают в ПСБ, то отказы в ОСУП могут повлиять на способность ПСБ работать по запросу. В таких случаях сама ОСУП станет системой, связанной с безопасностью.

2 В групповых производственных процессах ПСБ может быть применена для выбора различных настроек или логических функций в зависимости от используемых спецификаций. В этих случаях интерфейс оператора может быть использован для выполнения такого выбора.

3 Передача неточной информации из ОСУП в ПСБ не должна приводить к ухудшению безопасности.

11.7.2 Требования к интерфейсу обслуживания/разработки

11.7.2.1 Проект интерфейса обслуживания/разработки программируемой электроники ПСБ должен гарантировать, что любой отказ такого интерфейса не должен неблагоприятно влиять на способность ПСБ удерживать процесс в безопасном состоянии. Для этого может потребоваться отсоединить интерфейс обслуживания/разработки (например, панели программирования) от действующей ПСБ.

11.7.2.2 Интерфейс обслуживания/разработки должен обеспечивать выполнение следующих функций ПСБ с защитой доступа к каждой из них:

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

Примечание — Требования к ПО применяют только для ПСБ, использующих программируемую электронику.

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

11.7.2.4 Предоставление и отключение доступа для чтения-записи должны быть выполнены только в процессе конфигурирования или программирования, используя интерфейс обслуживания/разработки с соответствующим документированием и мерами по безопасности.

11.7.3 Требования к коммуникационным интерфейсам

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

11.7.3.2 ПСБ должна быть способна обмениваться информацией с ОСУП и периферийными устройствами без какого-либо воздействия на функции безопасности ПСБ.

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

11.7.3.4 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 для проведения испытаний при необнаруженных отказах.

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

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

11.8.4 Принудительная установка входов и выходов программируемой электроники ПСБ не должна использоваться в:

- прикладном ПО;
- 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 или отключении тревожной сигнализации должно быть сделано объявление в установленном порядке.

11.9 Вероятность отказа функции безопасности ПСБ

11.9.1 Вероятность отказа при наличии запроса для каждой функции безопасности ПСБ должна быть равной или меньше целевой меры отказов, установленной в спецификациях требований к безопасности. Это должно быть проверено расчетом.

Примечания

1 Для функций безопасности ПСБ, выполняемых в режиме по запросу, целевая мера отказов должна быть выражена в терминах средней вероятности отказа выполнения по запросу предусмотренной функции безопасности, как установлено УПБ функции безопасности ПСБ (см. таблицу 3).

2 Для функции безопасности ПСБ, выполняемой в режиме с непрерывным запросом, целевая мера отказов будет выражена в терминах средней вероятности опасного отказа в час, как установлено УПБ функции безопасности ПСБ (см. таблицу 4).

3 Необходимо количественно определить вероятности отказа отдельно для каждой функции безопасности ПСБ, так как им могут быть свойственны различные виды отказов компонентов и архитектура ПСБ (в части резервирования) также может быть различной.

4 Целевая мера отказов может быть установлена в виде величины средней вероятности отказа по запросу, или интенсивности опасных отказов, полученной из качественного анализа, или из установленного диапазона, связанного с УПБ, если он был определен количественным методом.

11.9.2 Расчетная вероятность отказов каждой функции безопасности ПСБ, вызванных отказами аппаратных средств, должна учитывать:

a) архитектуру ПСБ в части, связанной с выполнением каждой рассматриваемой функции безопасности ПСБ;

b) оценку интенсивности отказов каждой подсистемы, вызванных случайными неисправностями технических средств любого вида, которые приводят к опасному отказу ПСБ, но выявляются с помощью диагностических проверок;

c) оценку интенсивности отказов каждой подсистемы, вызванных случайными неисправностями технических средств любого вида, которые приводят к опасному отказу ПСБ, но не выявляются с помощью диагностических проверок.

Примечание — Оценки интенсивностей отказов подсистем могут быть определены из количественного анализа видов отказов при проектировании с использованием данных об отказах компонентов или подсистем из известного источника в промышленности или из опыта предшествующего использования подсистемы в таких же условиях, что и в предполагаемом случае применения; при этом продолжительность предшествующего использования должна быть достаточной для того, чтобы подтвердить объявленные на основе статистики интенсивности отказов при односторонней доверительной вероятности не ниже 70 %;

d) чувствительность ПСБ к отказам по общей причине;

e) охват диагностикой для любого периодического диагностического испытания (определяется согласно МЭК 61511-2) и связанные с ним диагностический интервал и надежность диагностических средств;

f) интервалы времени, через которые проводят проверочные испытания;

g) время восстановления для выявленных отказов;

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

i) оценку интенсивности опасных отказов при выполнении любых действий человека, способных вызвать опасный отказ ПСБ (как обнаруживаемый, так и не обнаруживаемый диагностическими проверками);

j) чувствительность к электромагнитным возмущениям (например, согласно МЭК 61326-1);

k) чувствительность к климатическим и механическим условиям эксплуатации (например, согласно МЭК 60654-1 и МЭК 60654-3).

Примечания

1 Среди множества возможных методов моделирования наиболее подходящий метод выбирает аналитик. Доступные методы включают в себя (см. [11], приложение В):

- моделирование поведения;
- анализ последовательности причин отказа;
- анализ дерева ошибок;
- модели Маркова;
- блок-схемы надежности.

2 Диагностический интервал и последующее время ремонта вместе составляют среднее время восстановления, рассматриваемое в модели надежности [1].

12 Требования к прикладному ПО, включая критерии выбора сервисного ПО

Настоящий раздел рассматривает:

a) три типа ПО:

- прикладное ПО (ППО);
- сервисное ПО, то есть программные инструментальные средства, использующиеся для разработки и проверки ППО;
- встроенное ПО, то есть ПО, поставляемое как часть программируемой электроники;

b) три типа языков разработки ПО:

- фиксированные языки программирования (ФЯП);
- языки программирования с ограниченной изменчивостью (ЯОИ);
- языки программирования с полной изменчивостью (ЯПИ).

Настоящий стандарт распространяется на прикладное ПО, разработанное на ЯОИ или ЯПИ. Все перечисленные ниже требования применяют для разработки и модификации прикладного ПО при уровне полноты безопасности до УПБ 3, поэтому настоящий стандарт не делает различия между УПБ 1, УПБ 2 и УПБ 3.

Разработку и модификацию прикладного ПО, выполненную с использованием ЯОИ или ЯПИ, для случаев до УПБ 3 следует выполнять в соответствии с требованиями настоящего стандарта. Разработку и модификацию прикладного ПО при УПБ 4 следует выполнять в соответствии с требованиями МЭК 61508. Разработку и модификацию прикладных программ на ФЯП также следует выполнять в соответствии с МЭК 61508.

Сервисное ПО (вместе с руководством изготовителя, содержащим указания по его безопасному применению) выбирают и применяют в соответствии с требованиями 12.4.4. Выбор встроенного ПО следует выполнять в соответствии с требованиями 11.5.

12.1 Требования к жизненному циклу безопасности прикладного ПО

12.1.1 Цели

12.1.1.1 Целями настоящего подраздела являются:

- определить действия, которые требуются при разработке прикладного ПО для каждой программируемой подсистемы ПСБ;

- установить, как следует выбирать, контролировать и применять сервисное ПО, применяемое при разработке прикладного ПО;

- обеспечить наличие плана, достаточного для того, чтобы гарантировать выполнение целей функциональной безопасности, поручаемых прикладным программам.

Примечание — На рисунке 10 представлена область применения требований раздела 12 в жизненном цикле безопасности ППО.

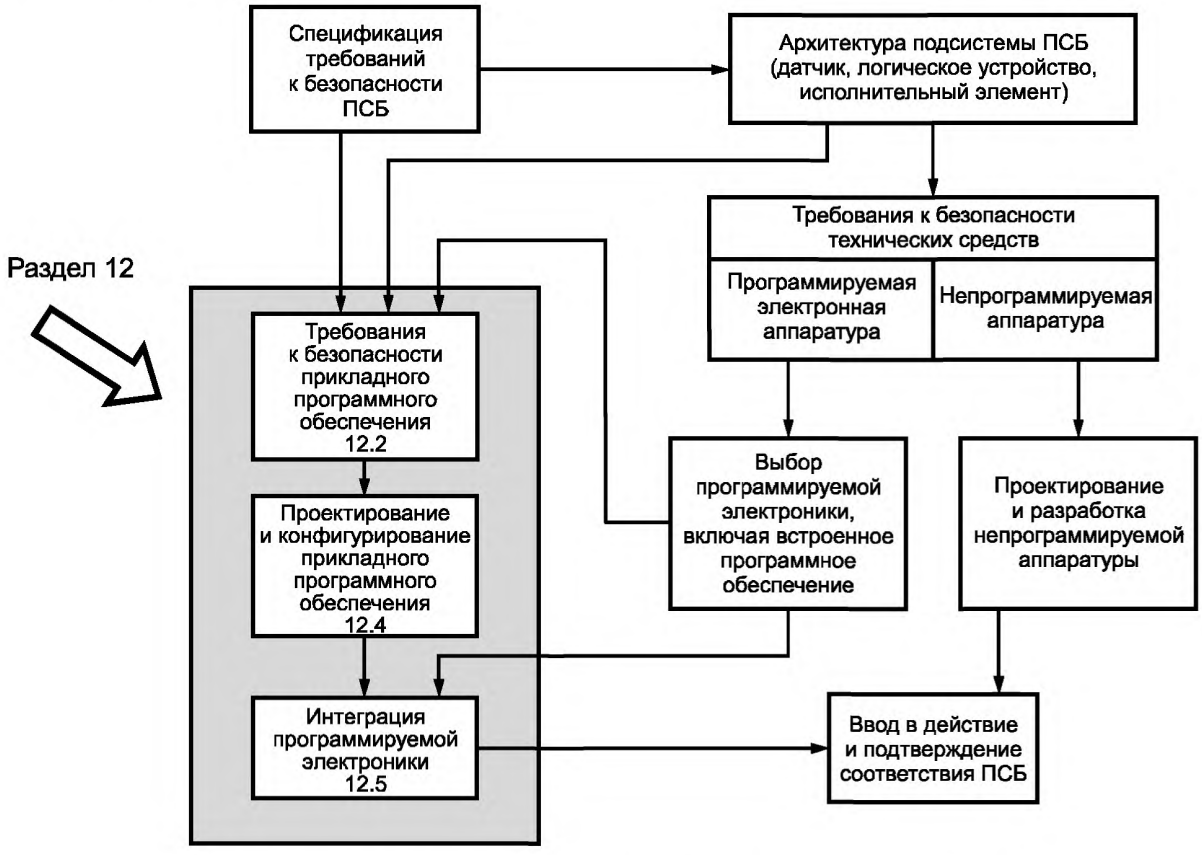


Рисунок 10 — Жизненный цикл безопасности прикладного ПО и его связь с жизненным циклом безопасности ПСБ

12.1.2 Требования

12.1.2.1 Жизненный цикл безопасности разрабатываемого ППО, отвечающего требованиям данного подраздела, должен устанавливаться в ходе планирования безопасности и должен быть интегрирован в жизненный цикл безопасности ПСБ.

12.1.2.2 Каждая стадия жизненного цикла безопасности ППО должна быть определена в терминах ее элементарных действий, целей, требуемой входной информации и выходных результатов, требований проверки (см. 12.7) и уровня ответственности (см. таблицу 7 и рисунок 11).

Примечания

1 При условии обеспечения соответствия жизненного цикла безопасности ППО требованиям таблицы 7 допускается выбирать глубину, число и объем работ каждой стадии V-образной модели (см. рисунок 12) с учетом полноты безопасности и сложности проекта ППО.

2 Тип используемого языка программирования (ФЯП, ЯОИ, ЯПИ) и близость языка к прикладным функциям могут влиять на широту охвата стадий V-образной модели.

3 Спецификации требований к безопасности ППО могут быть включены как часть в спецификации требований к безопасности ПСБ.

4 План подтверждения соответствия ППО может быть включен как часть в полный план подтверждения соответствия ПСБ в целом или ее подсистемы.

12.1.2.3 ПЭ устройство, которое обеспечивает выполнение прикладных программ, должно соответствовать УПБ, требуемому от каждой функции безопасности ПСБ, которую оно обслуживает.

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

- минимизировать риск появления ошибок в ППО;
- выявить и устранить ошибки, которые уже существуют в ПО;
- обеспечить, чтобы ошибки, остающиеся в ПО, не приводили к недопустимым результатам;
- обеспечить возможность обслуживания ПО в течение всего жизненного цикла ПСБ;
- продемонстрировать, что ПО обладает требуемым уровнем качества.

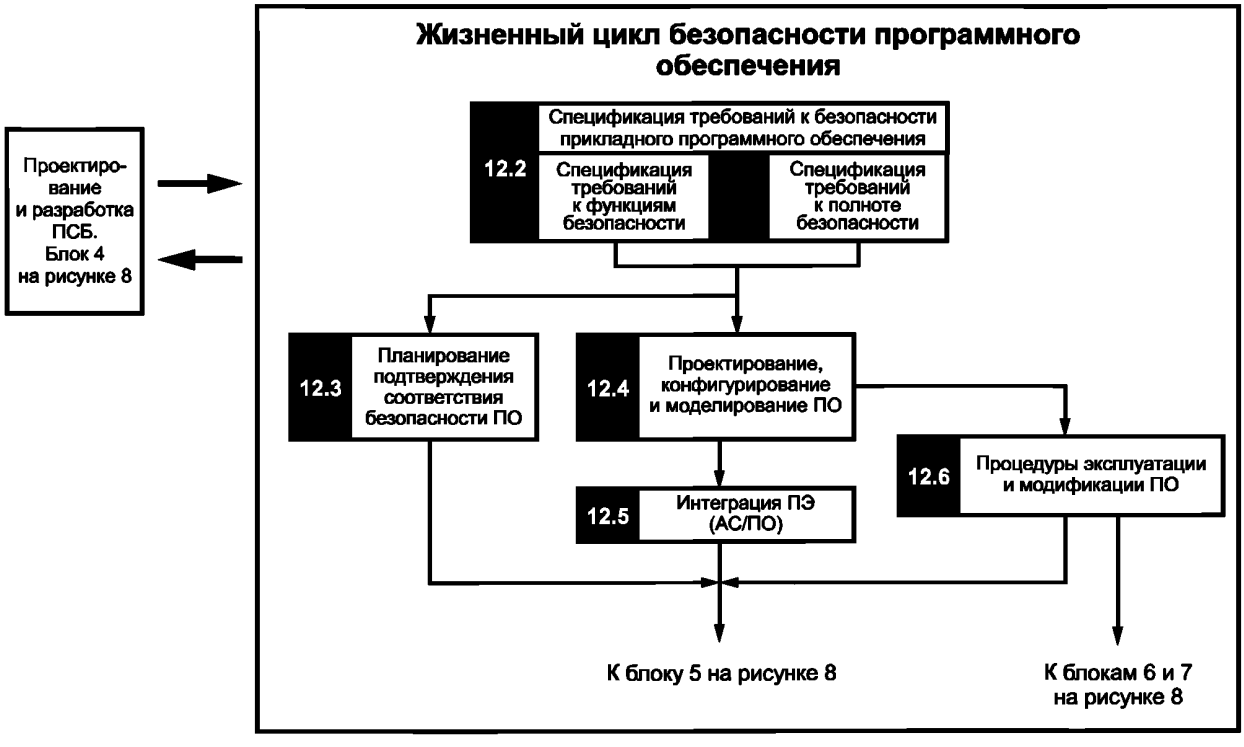
Примечание — Выбор методов и средств должен зависеть от конкретных обстоятельств. Факторы, влияющие на принимаемые при этом решения, обычно включают в себя:

- объем ПО;
- степень сложности;
- уровень полноты безопасности ПСБ;
- последствие в случае отказа;
- степень стандартизации элементов проекта.

12.1.2.5 Каждая стадия жизненного цикла безопасности ППО подлежит проверке (см. 12.7), результаты которой должны быть доступны (см. раздел 19).

12.1.2.6 Если на какой-либо стадии жизненного цикла безопасности ППО возникает необходимость внести изменение, относящееся к более ранней фазе жизненного цикла, то и эта, и последующие фазы подлежат проверке, и если в них также требуются изменения, то эти фазы также должны быть повторно выполнены и повторно проверены.

12.1.2.7 ППО, аппаратные средства ПСБ, а также встроенное ПО и сервисное ПО (инструментальные средства) подлежат процедурам управления конфигурацией (см. 5.2.7).



АС — аппаратные средства; ПО — программное обеспечение; ПЭ — программируемая электроника

Рисунок 11 — Жизненный цикл безопасности прикладного ПО (стадия реализации)



Рисунок 12 — Жизненный цикл разработки ПО (V-образная модель)

12.1.2.8 Испытания следует планировать. При этом должны быть рассмотрены следующие позиции:

- стратегия интеграции ПО и аппаратных средств;
- обстоятельства и результаты испытаний;
- типы проводимых испытаний;
- окружающие условия, включая инструментальные средства, вспомогательные программы и описание конфигурации при испытаниях;
- критерии, по которым оценивается выполнение испытаний;
- физические условия (например, заводские или стендовые);
- зависимости от внешних функций;
- готовность персонала;
- несоответствия.

Таблица 7 — Обзор жизненного цикла безопасности ППО

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 11)	Цели	Требования. Номер раздела, подраздела	Требуемая информация	Требуемые результаты
12.2 Спецификация требований к безопасности ППО	Установить требования к ПО каждой функции безопасности ПСБ, необходимой для реализации требуемых функций безопасности ПСБ. Установить требования к полноте безопасности ПО для каждой функции безопасности ПСБ, распределенной для данной ПСБ	12.2.2	Спецификация требований к безопасности ПСБ. Руководства по безопасности выбранных ПСБ. Архитектура ПСБ	Спецификация требований к безопасности ППО ПСБ. Информация о верификации
12.3 Планирование подтверждения соответствия безопасности ППО	Разработать план подтверждения соответствия ППО	12.3.2	Спецификация требований к безопасности ППО ПСБ	План подтверждения соответствия безопасности ППО ПСБ. Информация о верификации

Продолжение таблицы 7

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 11)	Цели	Требования. Номер раздела, подраздела	Требуемая информация	Требуемые результаты
12.4 Проектирование и разработка ППО	Архитектура. Создать архитектуру ПО, отвечающую установленным требованиям к безопасности ПО. Проверить и оценить требования, предъявляемые к ПО структурой аппаратных средств ПСБ	12.4.3	Спецификация требований к безопасности ППО ПСБ. Руководства по проектированию архитектуры аппаратных средств ПСБ	Описание проекта архитектуры, например, разделение ППО на подсистемы для соответствующих процессов и УПБ, например, выделение общих модулей в ППО, таких как управление насосом или клапаном. Архитектура ППО и спецификация требований к совместным испытаниям подсистем. Информация о верификации
	Инструментальные средства поддержки и языки программирования. Определить подходящий набор сервисного ПО для конфигурации, библиотек, управления, моделирования и испытания для всего жизненного цикла безопасности ПО. Установить процедуры разработки ППО	12.4.4	Спецификация требований к безопасности ППО ПСБ. Описание проекта архитектуры. Руководства по ПСБ. Руководство по безопасности выбранных логических устройств ПСБ	Список процедур для использования сервисного ПО
	Разработка ППО и прикладных модулей. Создать ППО, выполняющее установленные требования к безопасности ПО	12.4.5	Описание проекта архитектуры. Список инструкций и процедур выбранной ПЭС для использования сервисного ПО	1 Программа ППО (например, функциональные блок-схемы, ступенчатая логика). 2 Прикладные программы моделирования и совместных испытаний. 3 Спецификация специальных требований к безопасности ППО. 4 Информация о верификации
12.4 Разработка ППО на ЯПИ	Разработка и испытание программы (только на ЯПИ). Создать ЯПИ, удовлетворяющий установленным требованиям к безопасности ПО	12.4.6 и 12.4.7	Специальные требования к безопасности ППО	См. МЭК 61508-3

Окончание таблицы 7

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 11)	Цели	Требования. Номер раздела, подраздела	Требуемая информация	Требуемые результаты
12.4 Проектирование и разработка ППО	Испытание ППО, с тем чтобы: 1 Проверить выполнение требований по безопасности ПО. 2 Показать, что все прикладные программы систем и подсистем взаимодействуют правильно, выполняют свои намеченные функции и не выполняют ненамеченных функций. Может быть объединена со следующей стадией (12.5) для улучшения зоны проверок	12.4.6, 12.4.7 и 12.7	Спецификация требований к моделированию поведения ППО и совместным испытаниям (тестирование структуры). Спецификация требований к совместным испытаниям архитектуры ПО	1 Результаты испытаний ПО. 2 Испытанная и проверенная система ПО. 3 Информация о верификации
12.5 Интеграция ПЭ (технические средства и ПО)	Интегрировать ПО в ПЭ аппаратных средств	12.5.2	Спецификация требований к совместным испытаниям ПО и технических средств	Результаты совместных испытаний ПО и технических средств. Проверенные технические средства и ПО
12.3 Подтверждение соответствия безопасности ПСБ	Провести подтверждение соответствия ПСБ, включая безопасность ППО, требованиям безопасности	12.3	Планы подтверждения соответствия безопасности ПО и ПСБ	Результаты подтверждения соответствия ПО и ПСБ

12.2 Спецификация требований к безопасности ППО

Примечание — Данная стадия представлена блоком 12.2 на рисунке 11.

12.2.1 Цель

12.2.1.1 Цель данного подраздела состоит в том, чтобы обеспечить составление перечня требований к безопасности ППО для каждой программируемой подсистемы ПСБ, необходимой для реализации требуемых функций безопасности ПСБ, согласованного с архитектурой ПСБ.

Примечание — На рисунке 13 представлено отношение между структурой аппаратных средств и архитектурой ПО.

Архитектура программируемой подсистемы ПСБ		
Структура аппаратных средств	Архитектура ПО (включает встроенное ПО и ППО)	
Общие и зависимые от приложений характеристики аппаратных средств Примеры: - диагностические тесты; - резервные процессоры; - дублированные платы ввода/вывода	Встроенное ПО	Прикладное ПО
	Примеры: - коммуникационные драйверы; - программы обработки отказов; - управляющие программы	Примеры: - функции ввода/вывода; - созданные функции (например, проверка датчиков, если эта функция не выполняется встроенной программой)

Рисунок 13 — Отношение между структурой аппаратных средств и архитектурой ПО ПСБ

12.2.2 Требования

12.2.2.1 Должна быть разработана спецификация требований к безопасности ППО.

Примечания

1 Структура ПСБ обычно включает в себя структуры трех подсистем: датчиков, логического устройства и исполнительных элементов. Кроме того, подсистемы могут иметь резервные устройства, позволяющие достичь требуемого уровня полноты.

2 Структура аппаратных средств ПСБ с резервными датчиками может сопровождаться дополнительными требованиями к логической части ПСБ (например, реализация логики «один из двух»).

3 Не следует повторять требования к безопасности ПО подсистемы ПСБ, ранее установленные для системы в целом (см. раздел 10).

4 В спецификации требований по безопасности ПО следует определить минимальные функциональные возможности ПО ПЭ, а также ограничивать выбор любых функций, выполнение которых могло бы приводить к опасным условиям.

12.2.2.2 Входная информация для составления спецификации требований к безопасности ПО для каждой подсистемы ПСБ должна включать:

a) установленные требования к безопасности функции безопасности ПСБ;

b) требования, вытекающие из архитектуры ПСБ;

c) любые требования по планированию безопасности (см. раздел 5).

Примечания

1 Эта входная информация должна быть доступна разработчикам ППО.

2 Данное требование не означает, что недопустимы итерации между разработчиком структуры ПСБ, организацией, отвечающей за конфигурацию устройств, и разработчиком ППО. По мере того как требования к безопасности ППО и его возможная структура (см. 12.4.3) приобретают большую определенность, они могут влиять на структуру аппаратных средств ПСБ, вследствие чего становится важным тесное взаимодействие между разработчиками структуры ПСБ, поставщиками подсистемы ПСБ и разработчиками ППО (см. рисунок 5).

12.2.2.3 Спецификация требований к безопасности ППО должна быть достаточно подробной для того, чтобы можно было разработать и реализовать его в соответствии с требуемой полнотой безопасности, а также оценить достигнутую функциональную безопасность. При этом должны быть рассмотрены следующие вопросы:

- функции, поддерживаемые ППО;
- производительность и время реакции;
- интерфейсы с оборудованием и оператором и их удобство использования;
- все соответствующие режимы работы процесса, установленные в спецификации требований к безопасности ПСБ;
- действия, предпринимаемые при получении сигналов о нежелательных значениях переменных процесса, таких как значение сигнала датчика вне рабочего диапазона, обнаруженный разрыв цепи, обнаруженное короткое замыкание;
- проверочные и диагностические испытания внешних устройств (например, датчиков и исполнительных элементов);
- самоконтроль ПО (включая, например, программно-управляемые устройства контроля и проверки диапазона данных);
- мониторинг других устройств в ПСБ (например, датчиков и исполнительных элементов);
- возможность проведения периодических проверок функций безопасности ПСБ без останова процесса;
- ссылки на входные документы (например, на спецификацию функции безопасности ПСБ, конфигурацию или архитектуру ПСБ, требования к полноте безопасности аппаратных средств ПСБ).

12.2.2.4 Разработчик ППО должен критически рассмотреть всю информацию, приведенную в спецификации, чтобы убедиться, что требования однозначны, непротиворечивы и понятны. Любые недостатки установленных требований к безопасности должны быть определены и сообщены разработчику подсистемы ПСБ.

12.2.2.5 Установленные требования к безопасности ПО должны быть сформулированы и структурированы так, чтобы они:

- были ясны тем, кто пользуется данным документом на каждой из стадий жизненного цикла безопасности ПСБ; это относится и к терминологии, и к описаниям, которые должны быть однозначны и понятны операторам предприятий, специалистам по эксплуатации, а также прикладным программистам;

- были пригодны для верификации, испытаний и изменений;
- имели прослеживаемую связь со спецификацией требований к безопасности ПСБ.

12.2.2.6 Спецификация требований к безопасности ППО должна давать информацию, позволяющую выбрать подходящее оборудование. Для этого необходимо рассмотреть:

- функции, дающие возможность достичь или сохранить безопасное состояние процесса;
- функции, связанные с выявлением ошибок в любой подсистеме ПСБ, оповещением о них и управлением ими;
- функции, связанные с проведением периодических испытаний функций безопасности ПСБ на действующем процессе;
- функции, связанные с проведением периодических испытаний функций безопасности ПСБ на остановленном процессе;
- функции, дающие возможность проводить безопасную модификацию ПСБ;
- интерфейсы с функциями, не связанными с безопасностью;
- производительность и время реакции;
- уровни полноты безопасности для каждой из указанных выше функций.

Примечания

1 В зависимости от свойств выбранной подсистемы ПСБ некоторые из этих функций могут быть частью системного ПО.

2 Интерфейсы включают средства для модификации как в режиме действующего процесса, так и на остановленном процессе.

12.3 Планирование подтверждения соответствия безопасности ППО

Примечание — Данная стадия представлена блоком 12.3 на рисунке 11.

12.3.1 Цель

12.3.1.1 Цель требований данного подраздела состоит в том, чтобы обеспечить составление плана подтверждения соответствия безопасности ППО.

12.3.2 Требования

12.3.2.1 Планирование подтверждения соответствия ППО следует проводить в соответствии с требованиями, представленными в разделе 15.

12.4 Проектирование и разработка ППО

Примечание — Данная стадия представлена блоком 12.4 на рисунке 11.

12.4.1 Цели

12.4.1.1 Первая цель требований данного подраздела состоит в том, чтобы создать такую архитектуру ППО, которая была бы совместима со структурой технических средств и выполняла установленные требования к безопасности ПО (см. 12.2).

12.4.1.2 Вторая цель требований данного подраздела состоит в том, чтобы критически рассмотреть и оценить требования, предъявляемые к ПО со стороны структуры технических средств и встроенного ПО ПСБ. Они включают побочные для безопасности влияния поведения аппаратных средств и/или ПО ПСБ, особенности конфигурации технических средств ПСБ, допустимого числа отказов ПСБ и взаимовлияния аппаратных средств ПСБ и архитектуры встроенного ПО с ППО.

12.4.1.3 Третья цель требований данного подраздела состоит в том, чтобы выбрать подходящий набор инструментальных средств (включая сервисное ПО) для разработки ППО.

12.4.1.4 Четвертая цель требований данного подраздела состоит в том, чтобы спроектировать и реализовать или выбрать такое ППО, которое соответствовало бы требованиям безопасности ПО (см. 12.2), т. е. позволяло бы проводить его анализ, верификацию и давало возможность его безопасной модификации.

12.4.1.5 Пятая цель требований данного подраздела состоит в проверке выполнения требований к безопасности ПО (в отношении установленных функций безопасности ПО ПСБ).

12.4.2 Общие требования

12.4.2.1 Разработку, испытание, верификацию и подтверждение соответствия прикладных программ, написанных на языке с полной изменчивостью, следует проводить в соответствии с МЭК 61508-3.

12.4.2.2 Метод проектирования должен быть совместим со средствами разработки и ограничениями, принятыми для применяемой подсистемы ПСБ.

Примечание — Ограничения на применение подсистемы ПСБ, необходимые для соответствия с МЭК 61511, следует устанавливать в руководстве по безопасности оборудования.

12.4.2.3 Выбранный метод проектирования и прикладной язык (ЯОИ или ЯПИ) должны обладать свойствами, которые помогают:

a) добиться независимости, модульности и других свойств, влияющих на сложность; везде, где возможно, ПО должно строиться на базе хорошо проверенных программных модулей, которые могут включать пользовательские библиотечные функции и четко определенные правила для организации связей между программными модулями;

b) получить выражения для:

- функциональной зависимости, в идеале в виде логического описания или алгоритма функции;
- информационного потока между модулями прикладных функций;
- требований программирования;
- гарантий того, что функции безопасности ПСБ всегда выполняются за установленные интервалы времени;
- отсутствия неопределенного поведения;
- гарантий того, что элементы внутренних данных безошибочно продублированы, все используемые типы данных определены и осуществляется соответствующее действие, если данные находятся вне диапазона или потеряны;
- проектных допущений и их обусловленности;

c) добиться, чтобы разработчики и другие лица, которым необходимо знать проект, понимали как прикладные функции, так и сведения об ограничениях используемых технологий;

d) провести проверку и подтверждение соответствия, в том числе для кодов ППО, прикладных функций, интерфейсов с ПСБ, а также специфических особенностей конфигураций технического обеспечения ПСБ;

e) обеспечить свойства, облегчающие внесение изменений в ППО. Такие свойства включают модульность, прослеживаемость и документированность.

12.4.2.4 Созданный проект должен:

a) предусматривать проверки полноты данных и обоснованности проверок.

Примечание — Например, сквозные проверки каналов связи, проверки диапазонов значений входных данных датчика, проверки диапазонов значений данных входных и выходных параметров прикладных функций;

b) быть прослеживаемым при анализе требований;

c) быть проверяемым;

d) обладать способностью к безопасной модификации;

e) сводить к минимуму сложность и объем ППО функции безопасности ПСБ.

12.4.2.5 Если ППО применяется для выполнения функций безопасности ПСБ, имеющих различные УПБ, или функций, не связанных с безопасностью, то следует считать, что все ПО должно быть разработано как принадлежащее к самому высокому УПБ, кроме тех случаев, когда в проекте может быть показано, что функции безопасности ПСБ, имеющие различные УПБ, являются независимыми. Обоснование независимости должно быть документально оформлено. Для каждой функции безопасности ПСБ с требуемым от нее УПБ должно быть определено, является она независимой или нет.

Примечания

1 МЭК 61511-2 определяет, как проектировать и разрабатывать ППО, когда ПСБ должна выполнять функции, как связанные, так и не связанные с безопасностью.

2 МЭК 61511-2 определяет, как проектировать и разрабатывать ППО, когда ПСБ должна выполнять функции безопасности с различными УБП.

12.4.2.6 Если в проекте предусмотрено использование ранее разработанных библиотечных функций ППО, то должно быть обосновано, что они удовлетворяют спецификации требований к безопасности ППО (см. 12.2). Обоснованность должна базироваться на:

- соответствии требованиям МЭК 61508-3, если используется ЯПИ; или
- соответствии требованиям МЭК 61511, если используется ФЯП или ЯОИ; или

- доказательстве удовлетворительного функционирования в аналогичном случае применения, для которого было продемонстрировано, что оно имеет аналогичную функциональность, или для него были применены такие же процедуры проверки и подтверждения соответствия, как и для вновь разрабатываемого ПО (см. 11.5.4 и 11.5.5).

Примечание — Такое обоснование может быть разработано в процессе планирования безопасности (см. раздел 6).

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

a) о правообладателе (например, компания, авторы);

b) описание;

c) о прослеживаемости при анализе прикладных функциональных требований;

d) об используемых логических соглашениях;

e) об используемых стандартных библиотечных функциях;

f) о входных и выходных данных;

g) об управлении конфигурацией, включая историю изменений.

12.4.3 Требования к архитектуре ППО

12.4.3.1 Проект архитектуры ППО должен базироваться на спецификации требований к безопасности ПСБ и учитывать ограничения на структуру ПСБ. Этот проект должен быть согласован также с требованиями проекта выбранной подсистемы, набором ее средств и руководством по безопасности.

Примечания

1 Архитектура ПО определяет основные компоненты и подсистемы системного и ППО, их взаимосвязь, способ реализации необходимых характеристик и, в частности, полноты безопасности. Примерами модулей системного ПО являются операционные системы, базы данных, подсистемы передачи данных. Примеры модулей ППО включают программные реализации прикладных функций, реплицированные по всему предприятию.

2 Архитектура ППО должна определяться также структурой подсистем ПСБ, получаемых от поставщика.

12.4.3.2 Описание проекта архитектуры ППО должно:

a) обеспечивать исчерпывающее описание внутренней структуры и функционирования подсистем ПСБ и их компонентов;

b) включать спецификацию всех установленных компонентов (технических и программных) и описание соединений и взаимовлияний между ними;

c) устанавливать программные модули, включенные в подсистему ПСБ, но не используемые ни одной функцией безопасности ПСБ;

d) описывать порядок логической обработки данных подсистемами ввода-вывода и функциональные возможности логического устройства, включая любые временные ограничения;

e) устанавливать все функции ПСБ, не связанные с безопасностью, и обеспечивать, чтобы они не могли повлиять на правильное выполнение любой функции безопасности ПСБ.

Примечание — Особенно важно, чтобы документация по архитектуре ПО была актуальна и полна в отношении подсистем ПСБ.

12.4.3.3 Должен быть установлен набор методов и средств, применяемых для разработки ППО, а также должен быть обоснован их выбор.

Примечание — Такие методы и средства должны быть направлены на то, чтобы обеспечить:

- предсказуемость поведения подсистемы ПСБ;

- отказоустойчивость (согласованную с аппаратными средствами) и предотвращение отказов, в том числе за счет резервирования и разнообразия.

12.4.3.4 Методы и средства, применяемые при проектировании ППО, должны быть согласованы со всеми ограничениями, установленными в руководстве по безопасности подсистемы ПСБ.

12.4.3.5 Свойства, используемые для поддержания полноты безопасности всех данных, должны быть описаны и обоснованы. Такие данные могут включать входные и выходные данные установки, коммуникационные данные, эксплуатационные данные, данные обслуживания и данные, хранящиеся во внутренних базах данных.

Примечание — Между структурами аппаратных средств и архитектурами ПО существует итерационное взаимодействие (см. рисунок 11), поэтому спецификацию совместных испытаний ПЭ технических средств и ПО необходимо обсудить с разработчиком аппаратных средств (см. 12.5).

12.4.4 Требования к средствам поддержки, руководству пользователя и прикладным языкам

12.4.4.1 Должен быть выбран подходящий набор инструментальных средств, включающий подмножество языка прикладного программирования, средства управления конфигурацией, моделирования, средства испытаний и, при необходимости, средства измерений при автоматических проверках.

12.4.4.2 Следует рассмотреть пригодность соответствующих средств (необязательно тех, которые применялись при первоначальной разработке системы) для удовлетворения потребностей соответствующих служб в течение всего жизненного цикла ПСБ.

Примечание — Выбор средств разработки зависит от характера работ по созданию ППО, встроенного ПО и программной архитектуры (см. 12.4.3).

12.4.4.3 Следует установить подходящий набор процедур применения инструментальных средств, учитывающих ограничения руководства по безопасности, известные слабые места, способные привести к появлению ошибок в ППО, и любые ограничения зоны ранее проведенных проверки и подтверждения соответствия.

12.4.4.4 Выбранный прикладной язык должен:

- использовать транслятор/компилятор, пригодность которого для данного случая должна быть оценена;
- быть полностью и однозначно определен либо ограничен однозначно определенными функциями;
- соответствовать характеристикам данного случая применения;
- обладать свойствами, облегчающими выявление программных ошибок; и
- поддерживать свойства, соответствующие выбранному методу проектирования.

12.4.4.5 Если требования 12.4.4.4 не могут быть выполнены, то при описании проекта архитектуры ППО (см. 12.4.3) следует документально оформить обоснование использования применяемого языка программирования. В обосновании должны быть подробно рассмотрены пригодность языка программирования, а также дополнительные мероприятия, направленные на смягчение установленных его недостатков.

12.4.4.6 Процедуры применения прикладного языка должны быть хорошо проверены практикой программирования, недопустимо использовать небезопасные особенности языка (например, неустановленные характеристики, неструктурированные разработки), следует определять проверки на наличие ошибок в конфигурации и устанавливать процедуры документирования прикладной программы.

12.4.4.7 Руководство по безопасности должно охватывать следующие вопросы (при их уместности):

a) применение диагностики для выполнения функций безопасности;

b) перечень сертифицированных или верифицированных библиотек безопасности;

c) логику обязательных проверок и остановов системы;

d) применение контрольных устройств;

e) требования и ограничения на средства и языки программирования;

f) уровни полноты безопасности, для которых подходит данное устройство или система.

12.4.4.8 Пригодность используемых инструментальных средств должна быть проверена.

12.4.5 Требования к разработке ППО

12.4.5.1 Чтобы начать детальное проектирование ППО, необходимо располагать следующей информацией:

a) спецификациями требований к безопасности ПО (см. 12.2);

b) описанием проекта архитектуры ППО (см. 12.4.3), включающим в себя логику прикладной задачи и функции, обеспечивающие отказоустойчивость, перечень входных и выходных данных, применяемые общие программные модули и инструментальные средства их поддержки, а также процедуры программирования ППО.

12.4.5.2 ППО следует создавать с использованием структурных методов, чтобы обеспечить:

- модульность функций;
- проверяемость функций (включая отказоустойчивость) и внутренней структуры;
- способность к безопасной модификации;
- прослеживаемость для анализа и объяснения прикладных функций и связанных с ними ограничений.

Примечание — Везде, где возможно, следует применять проверенное ПО.

12.4.5.3 Проект каждого прикладного модуля должен быть рассчитан на здравый смысл, предусматривая в том числе:

- проверку правдоподобности каждой входной переменной, включая любые глобальные переменные, используемые для обеспечения входных данных;
- полное определение интерфейсов входа и выхода;
- проверку конфигурации системы, включая наличие и доступность предполагаемых технических и программных модулей.

12.4.5.4 Следует точно определить проект каждого прикладного программного модуля и применяемые к нему структурные проверки.

12.4.5.5 ППО должно:

- быть читаемым, понятным и проверяемым;
- удовлетворять всем соответствующим принципам проектирования;
- удовлетворять всем соответствующим требованиям, установленным при планировании безопасности (см. 5.2.4).

12.4.5.6 ППО следует подвергнуть критическому рассмотрению, чтобы убедиться в его соответствии принятому проекту, принципам проектирования и требованиям планирования подтверждения соответствия безопасности.

Примечание — Критическое рассмотрение ППО включает в себя такие приемы, как инспектирование программ, прогоны и формальный анализ. Оно должно сочетаться с моделированием и испытаниями, обеспечивающими уверенность в том, что модули ППО удовлетворяют соответствующей спецификации.

12.4.6 Требования к проверкам модулей ППО

Примечание — Проверка модуля ППО на соответствие его спецификации представляет собой работу по верификации (см. также 12.7). Она является комбинацией критического рассмотрения и структурной проверки, обеспечивающей уверенность в том, что модуль прикладной программы удовлетворяет перечню предъявляемых к нему требований, т. е. верифицирован.

12.4.6.1 Должны быть проверены все конфигурации системы между ее входами и выходами путем рассмотрения, моделирования и испытаний так, чтобы подтвердить, что входные и выходные данные корректно отображают логику применения.

12.4.6.2 Каждый модуль ППО должен проверяться путем рассмотрения, моделирования и испытаний так, чтобы определить, что предполагаемая функция выполняется правильно, а непредполагаемые функции не выполняются.

Тесты должны соответствовать конкретному проверяемому модулю и выполнять проверку:

- всех моделируемых ситуаций области применения;
- границ диапазона данных;
- временных эффектов, вызванных последовательностью исполнения;
- правильности выполнения последовательности.

12.4.6.3 Результаты проверок модулей ППО должны быть доступны.

12.4.7 Требования к комплексным испытаниям ППО

Примечание — Испытание на правильность интеграции ППО является работой по его верификации (см. 12.7).

12.4.7.1 Испытания ППО должны показать, что при выполнении предполагаемых функций все модули ППО и другие его компоненты или подсистемы правильно взаимодействуют друг с другом и с системным встроенным ПО.

Примечание — Проверки следует проводить так, чтобы подтвердить, что ПО не выполняет непреднамеренных функций, которые подвергают риску невыполнения требований по безопасности.

12.4.7.2 Результаты комплексных испытаний ППО должны быть доступны и содержать:

a) результаты испытаний; и

b) сведения о том, выполнены ли цели и критерии проведения испытаний.

Если происходили отказы, следует включить в отчет сведения об их причинах.

12.4.7.3 При интеграции ППО все модификации ПО должны быть объектом анализа влияния на безопасность, который должен определить:

a) все программные модули, затрагиваемые изменениями; и

b) необходимость проведения повторной верификации и перепроектирования (см. 12.6).

12.5 Интеграция ППО с подсистемой ПСБ

Примечание — Данная стадия представлена блоком 12.5 на рисунке 11.

12.5.1 Цель

12.5.1.1 Цель данного подпункта состоит в том, чтобы продемонстрировать, что ППО, выполняемое на аппаратных средствах и встроенном ПО подсистемы ПСБ, соответствует спецификации требований к безопасности ПО.

Примечание — В зависимости от характера приложения эти проверки могут сочетаться с проверками, описанными в 12.4.7.

12.5.2 Требования

12.5.2.1 Интеграционные испытания должны быть определены на самой ранней стадии жизненного цикла безопасности ПО, на которой это возможно, что позволит убедиться в совместимости ППО с аппаратными средствами и платформой встроенного ПО и в выполняемости функциональных и других требований по безопасности.

Примечания

1 На основе ранее полученного опыта объем испытаний может быть сокращен.

2 При выполнении испытаний необходимо обратить внимание на следующие вопросы:

- разделение ППО на интегрируемые наборы программ;
- тестовые примеры и тестовые данные;
- типы проводимых испытаний;
- окружающие условия, испытательные средства, конфигурацию и программы;
- критерий, по которому оценивается результат проведения испытаний;
- процедуры проведения корректирующих действий при появлении отказа в ходе испытаний.

12.5.2.2 Любые модификации или изменения, проводимые в процессе испытаний, должны подвергаться тщательному анализу на безопасность, чтобы определить:

a) все программные модули, затрагиваемые изменениями; и

b) необходимость проведения повторной верификации (см. 12.7).

12.5.2.3 Должна быть доступна следующая информация об испытаниях:

a) конфигурация испытываемой системы;

b) конфигурация системы, поддерживающей испытание (средства испытаний и внешние функциональные блоки);

c) участвующий персонал;

d) описания задач и содержание испытаний;

e) результаты испытаний;

f) сведения о выполнении цели и критериев оценки завершенности испытаний; и

g) если был отказ, то сведения о его причине, анализ отказа и отчеты об исправлении отказа, включая повторные испытания и повторную верификацию (см. 12.5.2.2).

12.6 Процедуры модификации ПО на ФЯП и ЯОИ

Примечание — Необходимость в модификации появляется на стадии эксплуатации ПО.

12.6.1 Цель

12.6.1.1 Цель требований данного подраздела состоит в обеспечении того, чтобы после внесения модификаций ПО продолжало удовлетворять требованиям безопасности.

12.6.2 Требования к модификации

12.6.2.1 Модификации следует проводить в соответствии с 5.2.6.2.2, 5.2.7 и разделом 17 с учетом следующих дополнительных требований:

a) перед проведением модификации следует выполнить анализ влияния модификации на безопасность процесса и на состояние разрабатываемого ПО и использовать результаты такого анализа для управления модификацией;

b) для данной модификации должно быть проведено планирование безопасности и повторной верификации;

c) модификации и повторные верификации следует проводить в соответствии с планом;

d) должны быть рассмотрены плановые условия, необходимые в течение проведения модификации и испытаний;

e) следует собрать всю документацию, влияющую на модификацию;

f) должны быть доступны детальные сведения (например, расписание) о всех действиях по модификации ПСБ.

12.7 Верификация ППО

12.7.1 Цели

12.7.1.1 Первая цель данного подраздела состоит в том, чтобы показать, что информация является удовлетворительной.

12.7.1.2 Вторая цель данного подраздела состоит в том, чтобы продемонстрировать, что выходные результаты прикладной программы для каждой стадии жизненного цикла безопасности ППО соответствуют установленным требованиям.

12.7.2 Требования

12.7.2.1 В соответствии с разделом 7 для каждой стадии жизненного цикла ППО следует провести планирование верификации.

12.7.2.2 Результаты каждой стадии подлежат верификации на:

a) адекватность выходных данных конкретной стадии жизненного цикла требованиям для этой стадии;

b) адекватность полноты проверок, инспекций и/или испытаний, проведенных на данной стадии;

c) совместимость между выходными результатами, полученными на различных фазах жизненного цикла;

d) корректность данных.

12.7.2.3 Верификация должна также обладать:

a) пригодностью для испытаний;

b) удобочитаемостью;

c) прослеживаемостью.

Примечания

1 Формат данных для прикладной программы следует верифицировать на:

- полноту;
- внутреннюю согласованность;
- защищенность от несанкционированного изменения;
- соответствие функциональным требованиям.

2 Данные прикладной программы необходимо верифицировать на:

- соответствие структурам данных;
- полноту;
- совместимость с используемым системным ПО (например, последовательность выполнения, время выполнения);
- правильность значений данных;
- выполнение действий в пределах известных границ безопасности.

3 Модифицируемые параметры следует верифицировать, чтобы защитить их от:

- неверных и неопределенных начальных значений;
- ошибочных значений;
- несанкционированных изменений;
- искажения данных.

4 Коммуникационные интерфейсы, интерфейсы процессов и связанное с ними ПО должны быть верифицированы на наличие возможности:

- обнаружения отказов;
- защиты от повреждения сообщений;
- подтверждения соответствия данных.

12.7.2.4 Функции, не связанные с безопасностью, и интерфейсы процесса, объединенные с сигналами и функциями, связанными с безопасностью, должны быть верифицированы на:

- отсутствие взаимного влияния с функциями безопасности;
- защищенность от появления взаимного влияния с функциями безопасности в случае отказа функций, не связанных с безопасностью.

13 Заводские приемочные испытания

Примечание — Данный раздел является справочным.

13.1 Цель

13.1.1 Цель заводских приемочных испытаний (ЗПИ) состоит в том, чтобы проверить, что логическое устройство вместе с соответствующим ПО удовлетворяет требованиям, установленным в спецификации требований к безопасности. Путем испытаний логического устройства с соответствующим ПО, проведенных перед их установкой на объекте, можно легко выявить и скорректировать ошибки.

Примечание — ЗПИ иногда называются комплексными или интеграционными испытаниями и могут быть частью подтверждения соответствия.

13.2 Рекомендации

13.2.1 Необходимость проведения ЗПИ следует определить на стадии проектирования.

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 устанавливаются:

- типы проводимых испытаний, в том числе: функциональные испытания системы как «черного ящика» (т. е. испытания по методу, при котором система рассматривается в виде «черного ящика», без явного использования знания о ее внутренней структуре. План испытаний по методу «черного ящика» обычно концентрирует внимание на требованиях к испытуемым функциям. Аналогами испытаний по методу «черного ящика» являются поведенческие и функциональные испытания, а также испытания методом непрозрачного или закрытого ящика); оценочные испытания (синхронизации, безотказности и готовности, полноты, целевых значений и ограничений безопасности); общетехнические испытания (включая ЭМС, испытания в нормальных и стрессовых условиях); проверки интерфейсов; испытания в режимах отказов и/или деградации; особые или исключительные испытания; проверки применимости инструкций по эксплуатации и обслуживанию ПСБ;
- постановка задачи, описание и данные испытаний.

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

- зависимость от других систем и/или интерфейсов;
- условия и средства проведения испытаний;
- конфигурация логического устройства;
- критерий принятия решения о прохождении испытаний;
- процедуры корректирующих действий при появлении отказа в процессе испытаний;
- компетентность персонала, выполняющего испытание;
- физическое размещение.

Примечание — Для испытаний, которые не могут быть физически продемонстрированы, обычно допускается привести формальные аргументы, доказывающие, что ПСБ отвечает требованиям, заданиям 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;
- функцию безопасности ПСБ и эксплуатационную характеристику, проверяемую в данном испытании;

- подробную процедуру 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:

a) степень их влияния на каждую функцию безопасности ПСБ; и

b) объем повторных испытаний, 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 ПСБ

14.1 Цели

14.1.1 Цели требований данного 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.

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 компоненты 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. 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.

14.2.4 Следует вести соответствующие записи мероприятий по вводу в действие ПСБ, фиксируя результаты проверок, 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 ПСБ

15.1 Цель

15.1.1 Цель требований данного раздела состоит в том, чтобы путем осмотра и испытаний можно было проверить, что установленная и введенная в эксплуатацию ПСБ и связанные с ней функции безопасности соответствуют требованиям, установленным в спецификации требований к безопасности.

Примечание — Иногда подтверждение соответствия называют приемо-сдаточными испытаниями на объекте.

15.2 Требования

15.2.1 Планирование подтверждения соответствия ПСБ должно определить все действия, требуемые для проведения подтверждения соответствия, среди которых должны быть:

- действия, связанные с подтверждением соответствия всех ПСБ спецификации требований к безопасности, включая установку 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;
- разумно предвидимых ненормальных условий, например установленных в ходе анализа риска;
- процедуры, меры и методики, используемые для подтверждения соответствия;
- 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).

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

15.2.2 Планирование подтверждения соответствия дополнительно для ППО безопасности должно включать следующее:

a) идентификацию ПО безопасности, для которого должна быть проведена процедура подтверждения соответствия, для каждого режима работы процесса до начала ввода в действие;

b) техническую стратегию для подтверждения соответствия ПО, которая должна содержать информацию о:

- ручных и автоматических методах;
- статических и динамических методах;
- аналитических и статистических методах;

c) меры (методики) и процедуры, соответствующие перечислению b), которые должны использоваться для подтверждения того, что каждая функция безопасности ПСБ соответствует установленным требованиям для функций безопасности ПО ПСБ (см. 12.2) и установленным требованиям для полноты безопасности ПО (см. 12.2);

d) условия окружающей среды, при которых проводят испытания на подтверждение соответствия (например, средства калибровки и испытательное оборудование);

e) критерии положительного/отрицательного результата выполнения подтверждения соответствия ПО должны включать:

- необходимые для процесса и оператора входные сигналы, включая их последовательность и значения;
- предполагаемые выходные сигналы, включая их последовательность и значения, и
- другие критерии приемки, например использование памяти, временные допуски и допуски значений;

f) политику и процедуры, используемые для оценки результатов подтверждения соответствия, в частности при оценке отказов.

Примечание — Эти требования основаны на общих требованиях 12.2.

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 функций безопасности ПСБ должно проводиться в соответствии с планом подтверждения соответствия ПСБ. Действия, связанные с подтверждением соответствия, должны включать, но этим не ограничиваться, подтверждение того, что:

- ПСБ работает в обычных и необычных режимах (например, при пуске или останове) так, как это установлено в спецификации требований по безопасности;
- 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;
- датчики, логические устройства и исполнительные элементы, включая все каналы с резервированием, работают в соответствии со спецификацией требований по безопасности.

Примечание — Если центральная (логическая) часть системы проходила ЗПИ, как это описано в разделе 13, то можно доверять результатам ЗПИ;

- документация на ПСБ соответствует установленной системе;
- функция безопасности ПСБ при недопустимых значениях переменных процесса (например, при значениях вне заданного диапазона) выполняется, как и было установлено;
- последовательность останова выполняется правильно;
- ПСБ обеспечивает выдачу правильных сообщений и их правильное представление на дисплее;
- вычисления, порученные ПСБ, выполняются правильно;
- функции установки ПСБ в исходное состояние выполняются так, как установлено в спецификации требований к безопасности;
- функции резерва (обхода) выполняются правильно;
- пусковые перенастройки ведутся правильно;
- системы ручного останова работают правильно;
- интервалы времени между тестовыми испытаниями зафиксированы в документации на процедуры обслуживания;
- функции сигнализации результатов диагностики выполняются, как это требуется;
- 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;
- устойчивость к электромагнитным помехам соответствует спецификации требований по безопасности (см. 10.3).

15.2.5 Подтверждение соответствия ПО должно показывать, что все установленные требования по его безопасности (см. 12.2) выполняются правильно и что ПО не ставит под угрозу выполнение требований безопасности в условиях сбоя в ПСБ, при режимах с деградацией или путем выполнения функций, не установленных в спецификации. Информация о действиях по подтверждению соответствия должна быть доступной.

15.2.6 Должна быть выпущена соответствующая информация о результатах подтверждения соответствия ПСБ требованиям безопасности, в которой указаны:

- использованная версия плана проведения подтверждения соответствия ПСБ;
- испытуемая (или оцениваемая) функция безопасности 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 комплексных (интеграционных) испытаний;
- испытуемая версия аппаратных средств и ПО ПСБ;
- любое несоответствие между ожидаемыми и действительными результатами;
- проведенный анализ и принятые решения по вопросу, следует ли при обнаружении расхождений продолжать испытания или выпустить запрос на изменение.

15.2.7 При наличии расхождений между ожидаемыми и реальными результатами проводится анализ и принимается решение о том, следует ли продолжать проверку или подготовить запрос на изменение и вернуться к более ранней стадии жизненного цикла разработки. Это решение должно быть документально оформлено и включено в состав результатов подтверждения соответствия безопасности ПО.

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

- все резервные функции (например, выполняемые программируемой электронной логической частью и комплексом ПЭ датчиков и отключенные аварийно) 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 принудительные воздействия должны быть устранены и при необходимости все возможности принудительных воздействий должны быть устранены.

16 Эксплуатация и техническое обслуживание ПСБ

16.1 Цели

16.1.1 Целями требований данного раздела являются:

- обеспечить для каждой функции безопасности ПСБ поддержание требуемого УПБ в процессе эксплуатации и технического обслуживания системы;
- эксплуатировать и выполнять техническое обслуживание ПСБ так, чтобы поддерживать проектную функциональную безопасность.

16.2 Требования

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

- штатные и нештатные действия по эксплуатации;
- проверочные испытания, превентивные и аварийные действия по техническому обслуживанию;
- процедуры, меры и методики, используемые при эксплуатации и техническом обслуживании;
- проверка допустимости процедур эксплуатации и технического обслуживания;
- лица, подразделения и организации, ответственные за эти действия.

16.2.2 Процедуры эксплуатации и технического обслуживания должны быть разработаны согласно соответствующему плану безопасности и обеспечивать следующие сведения:

- штатные действия, которые необходимо выполнять, чтобы поддерживать функциональную безопасность ПСБ на проектном уровне (например, соблюдение установленных при определении УПБ интервалов между проверочными испытаниями);
- необходимые действия и ограничения для предотвращения опасных состояний и/или уменьшения последствий опасных событий во время технического обслуживания или эксплуатации (например, дополнительные шаги по ослаблению опасности, когда система блокируется для выполнения тестирования или технического обслуживания);
- информацию (которая должна поддерживаться) по интенсивности отказов системы и запросов на срабатывание ПСБ;
- информацию (которая должна поддерживаться), хранящую результаты аудитов и испытаний ПСБ;
- процедуры технического обслуживания, которые должны быть выполнены после отказов и ошибок, происшедших 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 отслеживания включают:

- процедуры регистрации отказов;
- процедуры анализа систематических отказов;

- обеспечение того, что испытательное оборудование, используемое при нормальном техническом обслуживании, откалибровано и обслуживается правильно.

16.2.3 Эксплуатацию и техническое обслуживание следует проводить в соответствии с установленными процедурами.

16.2.4 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);
- знание об опасности, от которой защищает ПСБ;
- действие всех перепускных ключей и обстоятельства, при которых такие ключи должны использоваться;
- действие каждого из ключей ручного останова и пуска, а также когда такие ключи должны применяться.

Примечание — В состав таких ключей могут входить «настройка системы» и «перезапуск системы»;

- ожидаемую реакцию при срабатывании любых диагностических сигналов тревоги (например, оператором должно быть предпринято правильное действие при любом аварийном сигнале, обозначающем, что в ПСБ появилась проблема).

16.2.5 Обслуживающий персонал должен быть подготовлен настолько, как это требуется для обеспечения функционирования ПСБ (включая ее аппаратные средства и ПО) с заданной полнотой.

16.2.6 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:

- действия, выполняемые при запросе на срабатывание системы;
- отказы оборудования, входящего в ту часть ПСБ, которая используется в ходе штатных проверок или выполнения реального запроса;
- причины запросов;
- причины ошибочных срабатываний.

Примечание — Очень важно, чтобы были проанализированы все несоответствия между ожидаемым и реальным поведением. Этот анализ не следует путать с мониторингом запросов, приходящих при штатном функционировании.

16.2.7 Процедуры эксплуатации и обслуживания в случае необходимости могут потребовать повторного проведения:

- аудита функциональной безопасности;
- испытаний ПСБ.

16.2.8 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 учетом запаса надежности.

16.3 Проверочные испытания и осмотр

16.3.1 Проверочные испытания

16.3.1.1 Для обнаружения необнаруженных отказов следует, используя документально оформленные процедуры (см. 16.2.8), проводить периодические проверочные испытания, препятствующие ПСБ действовать в соответствии со спецификацией требований по безопасности.

16.3.1.2 Все компоненты ПСБ должны быть проверены, включая датчики, логическое устройство и исполнительные элементы (например, клапаны останова и двигатели).

16.3.1.3 Частота проведения проверочных испытаний должна быть определена путем расчета средней частоты отказов при наличии запроса.

Примечание — Различные части ПСБ могут потребовать различных интервалов испытаний, например, логическому устройству может потребоваться интервал, отличающийся от испытательного интервала для датчиков или исполнительных элементов.

16.3.1.4 Любые отклонения, обнаруженные в ходе проверочных испытаний, должны быть устранены безопасным способом и своевременно.

16.3.1.5 Через некоторый период времени, определяемый пользователем, частоту испытаний следует вычислять заново с учетом различных факторов, включая накопленные данные испытаний, опыт эксплуатации, старение технических средств и надежность ПО.

16.3.1.6 Любое изменение в логике приложения требует проведения полных проверочных испытаний. Исключения из этого правила допускаются, только если будут проведены соответствующий критический анализ и частичные испытания, подтверждающие, что изменения введены правильно.

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).

16.3.3 Документальное оформление проверочных испытаний и осмотров

Пользователь должен выполнять отчеты, удостоверяющие, что проверочные испытания и осмотры были выполнены в соответствии с требованиями. Эти отчеты должны включать, как минимум, следующую информацию:

a) описание выполненных испытаний и осмотров;

b) даты испытаний и осмотров;

c) фамилии лиц, выполнявших испытания и осмотры;

d) порядковый номер или другой уникальный идентификатор испытуемой системы (например, номер цикла, сигнала, оборудования и номер функции безопасности ПСБ);

e) результаты испытаний и осмотра (например, «как создано» или «как оставлено»).

17 Модификация ПСБ

17.1 Цели

17.1.1 Цели требований данного раздела:

- обеспечить, чтобы проведение модификаций любой ПСБ было спланировано правильно, 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 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 безопасности, затронутой модификацией.

17.2.4 Работы по модификации не должны начинаться без надлежащего разрешения.

17.2.5 Для всех изменений ПСБ должна быть сформирована соответствующая информация, включающая:

- описание модификации или изменения;
- причину изменения;

- установленные опасности, на которые могут повлиять изменения;
- анализ влияния работ по модификации ПСБ;
- все разрешения, требуемые для проведения изменений;
- испытания, проверяющие, что изменения проведены правильно, и ПСБ выполняет свои функции в соответствии с требованиями;
- соответствующую хронологию конфигурации;
- испытания, проверяющие, что изменения не повлияли неблагоприятно на элементы ПСБ, которые не подлежали модификации.

17.2.6 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 ПСБ

18.1 Цели

18.1.1 Целями требований данного раздела являются:

- обеспечить проведение соответствующего критического анализа и получение необходимого разрешения перед тем, как любая ПСБ будет выведена из эксплуатации; а также
- обеспечить сохранение работоспособности требуемых функций безопасности ПСБ в период выполнения действий по выводу из эксплуатации.

18.2 Требования

18.2.1 До выполнения вывода из эксплуатации любой 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 потенциально возможные опасности.

18.2.3 Должен быть проведен анализ того, как предполагаемый вывод системы из эксплуатации влияет на функциональную безопасность. Получаемая при этом оценка должна включать дополнительные сведения об опасности и риске, достаточные для того, чтобы определить тот охват и ту глубину, на которые необходимо повторить соответствующие этапы жизненного цикла безопасности. 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 безопасности, чтобы повторно применить соответствующие требования настоящего стандарта, включая повторное проведение проверки и подтверждения соответствия.

18.2.5 Работы по выводу из эксплуатации не должны начинаться до получения надлежащего разрешения.

19 Требования к информации и документации

19.1 Цели

19.1.1 Целями требований данного раздела являются:

- обеспечить наличие соответствующей документированной информации, позволяющей успешно выполнить все стадии жизненного цикла; и
- обеспечить наличие соответствующей документированной информации, позволяющей успешно выполнить действия по проверке, подтверждению соответствия и функциональной безопасности.

Примечания

1 Примеры структуры документации см. в [12], приложение А, и более подробно — в [13].

2 Документация может быть доступна в разных формах (например, на бумаге, пленке или ином носителе информации, допускающем отображение на экране или дисплее).

19.2 Требования

19.2.1 Документация, требования к которой установлены в настоящем стандарте, должна быть доступной.

19.2.2 Документация должна:

- описывать установку, систему или оборудование и их применение;
- быть точной;
- быть понятной;
- соответствовать цели, для которой она предназначена; и
- быть доступна и поддерживаться.

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 проверяемой на соответствие требованиям настоящего стандарта.

19.2.6 Документация должна иметь номер изменения (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 информационной схемы управления.

19.2.9 Должна поддерживаться текущая версия документации, содержащая следующее:

a) результаты оценки опасностей и рисков и связанные с ней допущения;

b) описание оборудования, выполняющего функции безопасности 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) информацию о результатах проектирования ПСБ, его реализации, проверки и подтверждения соответствия.

Примечание — Более подробные требования к информации приведены в разделах 14 и 15.

Приложение А
(справочное)

Различия между стандартами

Настоящее приложение представляет основные различия между МЭК 61511 и МЭК 61508.

МЭК 61511 имеет некоторые расхождения с МЭК 61508. Эти расхождения представлены в А.1 и А.2 настоящего приложения и базируются на сравнении данной версии МЭК 61511 с МЭК 61508.

А.1 Организационные различия

МЭК 61508	МЭК 61511	Пояснения
Часть 1	Часть 1	МЭК 61508-1, МЭК 61508-2, МЭК 61508-3 и МЭК 61508-4 объединены в МЭК 61511-1
Часть 2	Часть 1	Включена в МЭК 61511-1
Часть 3	Часть 1	Включена в МЭК 61511-1
Часть 4	Часть 1	Включена в МЭК 61511-1
Часть 5	Часть 3	Включена в МЭК 61511-3
Часть 6	Часть 2	Указания к МЭК 61511-1
Часть 7	Все части	Информативные ссылки даны в каждой части в виде приложений (при необходимости)

А.2 Терминология

МЭК 61508-4	МЭК 61511-1	Пояснения
Э/Э/ПЭ система, связанная с безопасностью	ПСБ	МЭК 61508 касается Э/Э/ПЭ систем, связанных с безопасностью, тогда как МЭК 61511 касается приборных систем безопасности
ПЭС	ПСБ	В МЭК 61508 система, включающая датчики и исполнительные устройства, называется «ПЭС», тогда как в МЭК 61511 используется термин «ПСБ»
Система управления процессом	Основная система управления процессом	«Основная система управления процессом» — термин, широко принятый в перерабатывающих отраслях
УО	Процесс	В МЭК 61508 применяется термин «управляемое оборудование» (УО), тогда как в МЭК 61511 — термин «процесс»
Функция безопасности	Функция безопасности приборной системы безопасности (ФБПСБ)	Функция безопасности по МЭК 61508, выполняемая Э/Э/ПЭ системой, связанной с безопасностью и применяющей иные технологии, или внешними средствами снижения риска. По МЭК 61511 функция безопасности выполняется только приборной системой безопасности

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60654-1:1993	—	*
МЭК 60654-3:1998	—	*
МЭК 61326-1:2005	—	*
МЭК 61508-2:2000	IDT	ГОСТ Р МЭК 61508-2—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
МЭК 61508-3:1998	IDT	ГОСТ Р МЭК 61508-3—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
МЭК 61508-4:1998	IDT	ГОСТ Р МЭК 61508-4—2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
МЭК 61511-2:2003	IDT	ГОСТ Р МЭК 61511-2—2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1»

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

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

- IDT — идентичные стандарты.

Библиография

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

[2] ISO/IEC 2382 (all parts), Information technology — Vocabulary

[3] ИСО/МЭК Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards

[4] IEC 61131-3:1993, Programmable controllers — Part 3: Programming language

[5] IEC 60617-12:1997, Graphical symbols for diagrams — Part 12: Binary logic elements

[6] IEC 61511-3: 2003, Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidance for the determination of the required safety integrity levels

[7] ISO 9000: 2000, Quality management systems — Fundamentals and vocabulary

[8] ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms

[9] ISO 9000-3:1997, Quality management and quality assurance standards — Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software

[10] IEC 60050(351):1998, International Electrotechnical Vocabulary — Part 351: Automatic control

[11] IEC 61508-6:2000, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

[12] IEC 61508-1:1998, Functional safety of electrical/electronic/programmable electronic safety related systems — Part 1: General requirements

[13] IEC 61506:1997, Industrial-process measurement and control — Documentation of application software

УДК 62-783:614.8:331.454:006.354 ОКС 13.110 25.040.01 Т51

Ключевые слова: функциональная безопасность, жизненный цикл систем, промышленные процессы, приборные системы безопасности, планирование функциональной безопасности, жизненный цикл безопасности, уровень полноты безопасности

Редактор *А. Д. Чайка*
Технический редактор *В. Н. Прусакова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *В. Н. Романовой*

Сдано в набор 07.11.2012. Подписано в печать 24.01.2013. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 8,37. Уч.-изд. л. 7,60. Тираж 98 экз. Зак. 1740.

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

gost.e-ecolog.ru