ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-1— 2007

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ, ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Часть 1

Общие требования

IEC 61508-1:1998
Functional safety of electrical/electronic/programmable electronic safety-related systems —
Part 1: General requirements
(IDT)

Издание официальное

БЗ 3—2006/36

Москва
Стандартинформ
2008

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» и Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков» на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Управлением развития, информационного обеспечения и аккредитации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 582-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61508-1:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования» (IEC 61508-1:1998 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements», IDT).

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 С

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2008

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

Содержание

1 Область применения 1
2 Нормативные ссылки 4
3 Термины и определения 4
4 Соответствие настоящему стандарту 4
5 Документация 5
6 Управление функциональной безопасностью 6
7 Требования к полному жизненному циклу безопасности 7
8 Оценка функциональной безопасности 34
Приложение А (справочное) Пример структуры документации 37
Приложение В (справочное) Компетентность лиц 42
Приложение С (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 43
Библиография 44

Введение

Системы, состоящие из электрических и/или электронных компонентов, в течение многих лет используются для выполнения функций безопасности в большинстве областей применения. Компьютерные системы [обычно называемые программируемыми электронными системами (PES)], использующиеся во всех областях применения для выполнения задач, не связанных с безопасностью, во все более увеличивающихся объемах используются для решения задач обеспечения безопасности. Для эффективной и безопасной эксплуатации технологий, основанных на использовании компьютерных систем, чрезвычайно важно, чтобы лица, ответственные за принятие решений, имели в своем распоряжении руководства по вопросам безопасности, которые они могли бы использовать в своей работе.

Настоящий стандарт устанавливает общий подход к вопросам обеспечения безопасности для всего жизненного цикла систем, состоящих из электрических и/или электронных и/или программируемых электронных компонентов [электрических/ электронных/программируемых электронных систем (E/E/PES)], которые используются для выполнения функций безопасности. Этот унифицированный подход был принят для того, чтобы разработать рациональную и последовательную техническую концепцию для всех электрических систем, связанных с безопасностью. Основной целью при этом является содействие разработке стандартов.

В большинстве ситуаций безопасность достигается за счет использования нескольких систем защиты, в которых используются различные технологии (например, механические, гидравлические, пневматические, электрические, электронные, программируемые электронные). Любая стратегия безопасности должна, следовательно, учитывать не только все элементы, входящие в состав отдельных систем (например, датчики, управляющие устройства и исполнительные механизмы), но также и все подсистемы, связанные с безопасностью, входящие в состав комбинированной системы, связанной с безопасностью. Таким образом, хотя данный стандарт посвящен в основном электрическим/электронным/программируемым электронным (E/E/PE) системам, связанным с безопасностью, он может также предоставлять общую структуру, в рамках которой рассматриваются системы, связанные с безопасностью, основанные на других технологиях.

Признанным фактом является существование огромного разнообразия использования E/E/PES в различных областях применения, отличающихся различной степенью сложности, опасностями и возможными рисками. В каждом конкретном применении необходимые меры безопасности будут зависеть от многочисленных факторов, которые являются специфичными для этого применения. Настоящий стандарт, являясь базовым стандартом, позволит формулировать такие меры в будущих международных стандартах для областей применения

Настоящий стандарт:

- рассматривает все соответствующие этапы жизненного цикла систем безопасности в целом, а также подсистем E/E/PES и программного обеспечения (например, начиная с исходной концепции, включая проектирование, разработку, эксплуатацию, сопровождение и вывод из эксплуатации), в ходе которых E/E/PES используются для выполнения функций безопасности;

- был задуман с учетом быстрого развития технологий; его структура является достаточно устойчивой и полной для того, чтобы удовлетворять потребностям разработок, которые могут появиться в будущем;

- делает возможной разработку стандартов областей применения, где используются системы E/E/PES; разработка стандартов для областей применения в рамках общей структуры, вводимой настоящим стандартом, должна приводить к более высокому уровню согласованности (например, основных принципов, терминологии и т.п.) как для отдельных областей применения, так и для их совокупности; это приносит преимущества как в плане безопасности, так и в плане экономики;

- предоставляет метод разработки спецификаций для требований к безопасности, необходимых для достижения требуемой функциональной безопасности E/E/PE систем, связанных с безопасностью;

- использует уровни полноты безопасности для задания планируемого уровня полноты безопасности для функций, которые должны быть реализованы E/E/PE системами, связанными с безопасностью;

- использует для определения уровней полноты безопасности подход, основанный на оценке рисков;

- устанавливает количественные величины отказов E/E/PE систем, связанных с безопасностью, которые связаны с уровнями полноты безопасности;

- устанавливает нижний предел для планируемой величины отказов в режиме опасных отказов, который может быть задан для отдельной E/E/PE системы, связанной с безопасностью; для E/E/PE систем, связанных с безопасностью, работающих в:

режиме с низкой интенсивностью запросов нижний предел для выполнения планируемой функции по запросу устанавливается на средней вероятности отказов 10^{-5};

режиме с высокой интенсивностью запросов нижний предел устанавливается на вероятности опасных отказов 10^{-9} в час.

Примечание — Отдельная E/E/PE система, связанная с безопасностью, необязательно предполагает одноканальную архитектуру.

- применяет широкий набор принципов, методов и мер для достижения функциональной безопасности E/E/PE систем, связанных с безопасностью, но не использует концепцию безаварийности, которая может иметь важное значение, когда виды отказов хорошо определены, а уровень сложности является относительно невысоким. Концепция безаварийности признана неподходящей из-за широкого диапазона сложности E/E/PE систем, связанных с безопасностью, которые находятся в области применения настоящего стандарта.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ, ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Часть 1

Общие требования

Functional safety of electrical, electronic, programmable electronic safety-related systems.
Part 1. General requirements

Дата введения — 2008—06—01

1 Область применения

1.1 Настоящий стандарт охватывает вопросы, которые должны учитываться при использовании электрических, электронных, программируемых электронных систем для выполнения функций безопасности. Главная цель настоящего стандарта — облегчить техническим комитетам разработку стандартов. Это позволит полностью учесть существенные факторы, связанные с решаемыми задачами, и, таким образом, удовлетворить конкретные потребности области применения. Другая цель настоящего стандарта заключается в том, чтобы сделать возможной разработку электрических, электронных, программируемых электронных (E/E/PE) систем, связанных с безопасностью, в условиях возможного отсутствия стандартов для областей применения.

1.2 В частности, настоящий стандарт:

a) применяется к системам, связанным с безопасностью, когда одна или несколько таких систем включают в себя электрические, электронные, программируемые электронные устройства.

Примечания

1 Для E/E/PE систем, связанных с безопасностью и имеющих низкую сложность, некоторые требования, определенные в настоящем стандарте, могут оказаться необязательными, и становится возможным освобождение от соответствия таким требованиям (см. 4.2, а также определение E/E/PE систем, связанных с безопасностью и имеющих низкую сложность, в МЭК 61508-4, пункт 3.4.4).

2 Хотя человек может быть частью системы, связанной с безопасностью (МЭК 61508-4, пункт 3.4.1), требования к человеческому фактору, относящиеся к проектированию E/E/PE систем, связанных с безопасностью, не рассматриваются подробно в настоящем стандарте

b) является основополагающим и применяется ко всем E/E/PE системам, связанным с безопасностью, независимо от их применения.

Примечание — См. МЭК 61508-4, пункты 3.1.1 и 7.3.1.2.

c) охватывает возможные опасности, вызванные отказами функций безопасности, которые должны выполняться E/E/PE системами, связанными с безопасностью, в отличие от опасностей, связанных с самим E/E/PE оборудованием (например, поражения электрическим током и т.п.);

d) не охватывает E/E/PE систем, в которых:

- необходимое снижение риска может быть достигнуто с помощью единичной E/E/PE системы и
- требуемая полнота безопасности E/E/PE систем меньше той, которая соответствует уровню полноты безопасности, равному 1 (самый низкий уровень полноты безопасности в настоящем стандарте);

e) относится, главным образом, к E/E/PE системам, связанным с безопасностью, отказы которых могут оказывать влияние на безопасность людей и/или на окружающую среду; однако признано, что последствия отказа могут также вызывать серьезные экономические последствия, и в таких случаях настоя-

Издание официальное

щий стандарт может быть использован для точного определения любой E/E/PE системы, используемой для защиты оборудования или продукции;

f) рассматривает E/E/PE системы, связанные с безопасностью, системы, связанные с безопасностью, основанные на других технологиях, и внешние средства уменьшения риска для того, чтобы спецификации требований безопасности E/E/PE систем, связанных с безопасностью, могли быть определены на основе систематического анализа рисков;

g) использует модель полного жизненного цикла безопасности как техническую основу для систематических действий, необходимых для обеспечения функциональной безопасности E/E/PE систем, связанных с безопасностью.

Примечания

1 Ранние этапы полного жизненного цикла безопасности включают, по необходимости, учет других технологий (наряду с E/E/PE системами, связанными с безопасностью) и внешних средств снижения риска для того, чтобы спецификации требований к E/E/PE системам, связанным с безопасностью, могли быть разработаны систематическим образом на основании анализа рисков.

2 Хотя полный жизненный цикл безопасности относится в первую очередь к E/E/PE системам, связанным с безопасностью, он может также предоставлять техническую основу для анализа любой системы, связанной с безопасностью, независимо от технологии, на которой она основана (например, механической, гидравлической или пневматической).

h) не определяет уровней полноты безопасности для областей применения (которые должны основываться на подробной информации и знаниях, относящихся к области применения). Технические комитеты, отвечающие за конкретные области применения, должны определять, где это необходимо, уровни полноты безопасности в стандартах области применения;

i) устанавливает общие требования к E/E/PE системам, связанным с безопасностью, где отсутствуют стандарты области применения;

j) не охватывает меры предосторожности, которые необходимы для того, чтобы предотвратить повреждения или иное неблагоприятное воздействие на функциональную безопасность E/E/PE систем, связанных с безопасностью, со стороны лиц, не имеющих полномочий.

1.3 Настоящий стандарт устанавливает общие требования, которые применимы ко всем частям стандарта. В других частях рассматриваются более конкретные вопросы:

- в МЭК 61508-2 и МЭК 61508-3 предоставлены дополнительные и специфические требования к E/E/PE системам, связанным с безопасностью (требования к аппаратным средствам и программному обеспечению);
- МЭК 61508-4 содержит определения терминов и сокращения, которые используются в настоящем стандарте;
- МЭК 61508-5 содержит руководство по применению МЭК 61508-1 для определения уровней полноты безопасности, основанное на использовании примеров;
- МЭК 61508-6 содержит руководство по применению МЭК 61508-2 и МЭК 61508-3;
- МЭК 61508-7 содержит обзор методов и средств.

1.4. МЭК 61508-1 — МЭК 61508-4 представляют собой основополагающие стандарты по безопасности, хотя этот статус не применяется в контексте E/E/PE систем, связанных безопасностью, имеющих небольшую сложность (МЭК 61508-4, пункт 3.4.4). Как основополагающие стандарты по безопасности они предназначены для использования техническими комитетами при подготовке стандартов в соответствии с МЭК Руководство 104 и ИСО/МЭК Руководство 51. МЭК 61508-1 — МЭК 61508-4 предназначены, кроме того, для использования в качестве самостоятельных стандартов.

В круг обязанностей технического комитета входит использование, где это возможно, основополагающих стандартов по безопасности при подготовке собственных стандартов. В этом случае требования, методы проверки или условия проверки настоящего основополагающего стандарта по безопасности не будут применяться, если это не указано специально, или они будут включаться в стандарты, подготовленные этими техническими комитетами.

Примечание — В США и Канаде до тех пор, пока там не будет опубликована в качестве международного стандарта предлагаемая реализация МЭК 61508 для обрабатывающих отраслей (т.е. МЭК 61511), вместо МЭК 61508 в обрабатывающих отраслях допускается использовать национальный стандарт, базирующийся на МЭК 61508 (т.е. ANSI/ISA S 84.01-1996).

1.5 На рисунке 1 показана общая структура МЭК 61508-1 — МЭК 61508-7 и указана роль, которую играет МЭК 61508-1 в достижении функциональной безопасности E/E/PE систем, связанных с безопасностью.

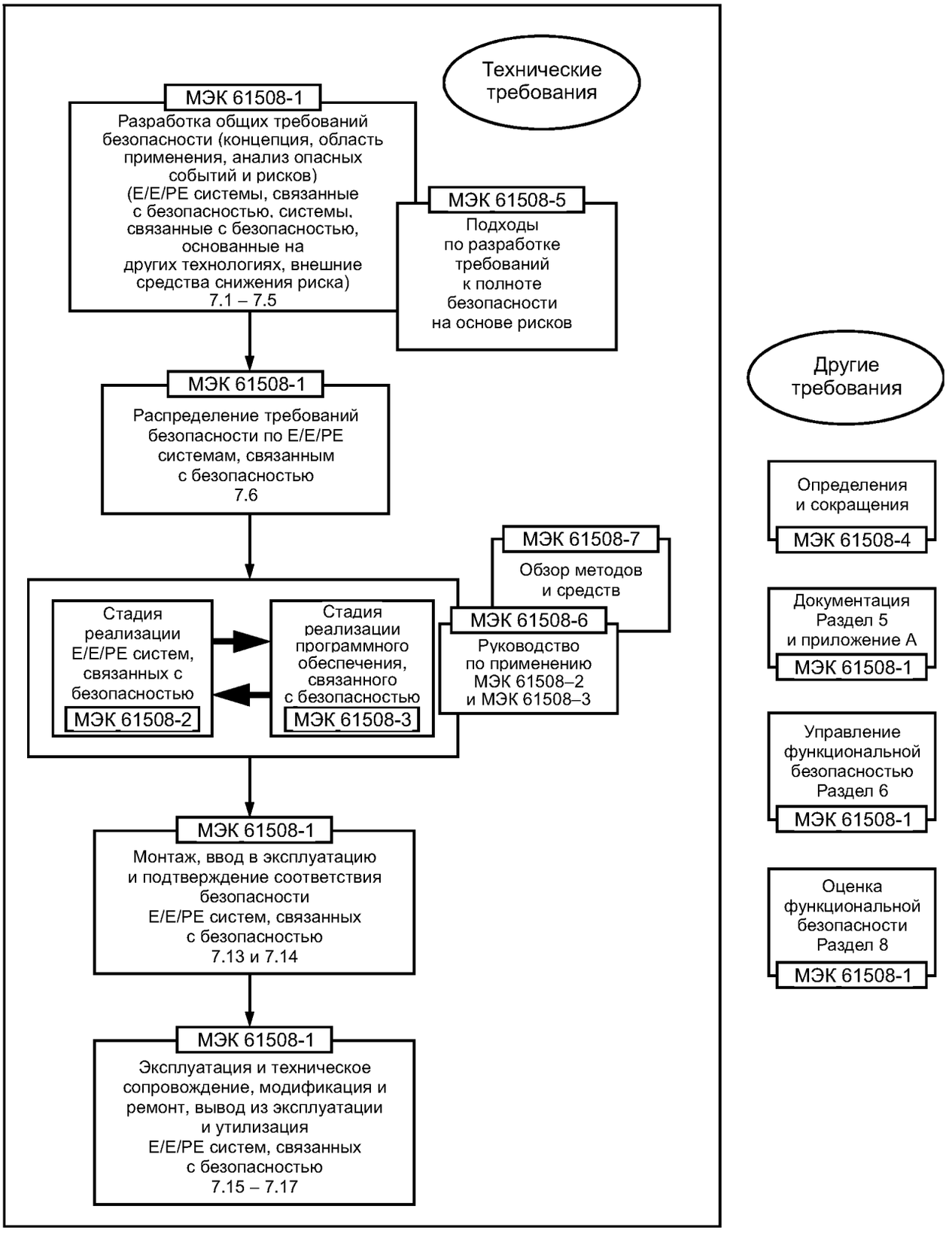


Рисунок 1 — Общая структура настоящего стандарта

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК Руководство 51:1999 Руководящие указания по включению в стандарты аспектов, связанных с безопасностью

МЭК Руководство 104:1997 Подготовка публикаций по безопасности и использование основополагающих групповых публикаций по безопасности

МЭК 61508-2:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к электрическим, электронным, программируемым электронным системам, связанным с безопасностью

МЭК 61508-3:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

МЭК 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения

МЭК 61508-5:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней безопасности

МЭК 61508-6:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2:2000 и МЭК 61508-3:1998

МЭК 61508-7:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Анализ методов и средств

3 Термины и определения

В настоящем стандарте применимы термины по МЭК 61508-4.

4 Соответствие настоящему стандарту

4.1 Для достижения соответствия настоящему стандарту необходимо выполнять требования по отношению к заданным указанным критериям (например, уровню полноты безопасности) и, следовательно, выполнять все требования каждого раздела и подраздела.

Примечание — В общем случае невозможно вычленить один какой-то фактор, определяющий, в какой мере должно выполняться то или иное требование (степень строгости). Решение должно зависеть от нескольких факторов, набор которых, в свою очередь, может зависеть от стадии и процесса полного жизненного цикла безопасности, жизненного цикла безопасности E/E/PES или жизненного цикла безопасности программного обеспечения. В число этих факторов входят:

- характер опасностей;
- уменьшение риска и последствий;
- уровень полноты безопасности;
- тип технологии реализации;
- размер системы;
- число участвующих коллективов;
- физическое распределение;
- новизна проекта.

4.2 Настоящий стандарт определяет требования к E/E/PE системам, связанным с безопасностью. Он был разработан для обеспечения охвата всего диапазона сложности, присущей таким системам. Однако для E/E/PE систем, связанных с безопасностью, имеющих низкую сложность (МЭК 61508-4, пункт 3.4.4), там, где существует надежный практический опыт, дающий необходимую уверенность в том, что будет достигнута необходимая полнота безопасности, возможны следующие варианты:

- в стандартах областей применения, реализующих требования МЭК 61508-1 — МЭК 61508-7, некоторые требования могут быть необязательными и допускается освобождение от соответствия таким требованиям;

- если настоящий стандарт используется в условиях отсутствия стандарта для области применения, то некоторые требования, определенные в настоящем стандарте, могут считаться необязательными, и соответствие этим требованиям может не учитываться при условии, что это решение будет обосновано.

4.3 Стандарты областей применения для E/E/PE систем, связанных с безопасностью, разработанные на основе настоящего стандарта, должны учитывать требования ИСО/МЭК Руководства 51 и МЭК Руководства 104.

5 Документация

5.1 Цели

5.1.1 Первая цель требований настоящего раздела состоит в указании информации, которая должна быть документирована для того, чтобы эффективно выполнять все стадии полного жизненного цикла, жизненного цикла системы E/E/PES и программного обеспечения.

5.1.2 Второй целью требований настоящего раздела является указать информацию, которая должна быть документирована, для того, чтобы можно было эффективно выполнять действия по управлению функциональной безопасностью (см. раздел 6), верификации (см. 7.18) и оценке функциональной безопасности (см. раздел 8).

Примечания

1 Требования к документации в настоящем стандарте относятся, по сути, скорее к информации, чем к физическим документам. Не требуется включать информацию в физические документы, если это не указано явным образом в соответствующем подразделе.

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

3 Возможную структуру документации см. в приложении А.

4 См. [4].

5.2 Требования

5.2.1 Для каждой завершенной стадии полного жизненного цикла безопасности, жизненного цикла безопасности E/E/PES и программного обеспечения документация должна содержать информацию, которая является достаточной для эффективной реализации последующих стадий и для процессов верификации.

Примечание — Понятие достаточной информации зависит от ряда факторов, включая сложность и размер E/E/PE системы, связанной с безопасностью, и требований, относящихся к конкретному применению.

5.2.2 Документация должна содержать информацию, достаточную для управления функциональной безопасностью (раздел 6).

Примечание — См. примечания к 5.1.2.

5.2.3 Документация должна содержать достаточную информацию, необходимую для реализации оценки функциональной безопасности, а также данные и результаты, полученные при оценке функциональной безопасности.

Примечание — См. примечания к 5.1.2.

5.2.4 Если только иное не было обосновано при планировании функциональной безопасности или определено в стандарте области применения, документируемая информация должна соответствовать положениям, приведенным в разделах настоящего стандарта.

5.2.5 Доступность информации должна быть достаточной для выполнения служебных обязанностей в соответствии с положениями настоящего стандарта.

Примечание — Участвующим сторонам следует предоставлять только информацию, необходимую для выполнения конкретных действий, требуемых настоящим стандартом.

5.2.6 Документация должна быть:

- точной и краткой;
- понятной для тех, кто должен ее использовать;
- пригодной для тех целей, для которых она предназначена;
- доступной и поддерживаемой.

5.2.7 Документация или набор информации должны иметь заголовки или названия, указывающие на область применения содержания, а также указатель того или иного рода, облегчающий доступ к информации, требуемой настоящим стандартом.

5.2.8 Документация может учитывать процедуры, используемые компаниями, а также рабочую практику, сложившуюся в конкретных прикладных областях.

5.2.9 Документы или набор информации должны иметь номер изменения (номер версии), позволяющий идентифицировать различные версии документа.

5.2.10 Документ или набор информации должен быть структурирован таким образом, чтобы облегчить поиск необходимой информации. Должна быть возможность установления последнего изменения (версии) документа или набора информации.

Примечание — Физическая структура документации может меняться в зависимости от ряда факторов, таких как размер системы, ее сложность и организационные требования.

5.2.11 Все документы должны подвергаться изменению, исправлениям, проверке, утверждению и контролю с помощью соответствующей схемы контроля.

Примечание — При использовании для разработки документации автоматических и полуавтоматических средств могут потребоваться специальные процедуры, гарантирующие принятие эффективных мер для управления версиями и обеспечивающие контроль других аспектов, относящихся к документации.

6 Управление функциональной безопасностью

6.1 Цели

6.1.1 Первой целью требований настоящего подраздела является определение действий по управлению и технических действий на стадиях полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения, которые необходимы для достижения требуемой функциональной безопасности E/E/PE систем, связанных с безопасностью.

6.1.2 Второй целью требований настоящего подраздела является определение ответственности отдельных лиц, подразделений и организаций для каждой стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения, а также для действий в течение каждой стадии.

Примечание — Организационные мероприятия, относящиеся к данному разделу, обеспечивают эффективную реализацию технических требований и предназначены для достижения и поддержания функциональной безопасности E/E/PE систем, связанных с безопасностью. Технические требования, необходимые для поддержания функциональной безопасности, обычно определяются как часть информации, предоставляемой поставщиком E/E/PE систем, связанных с безопасностью.

6.2 Требования

6.2.1 Те организации или отдельные лица, которые несут полную ответственность за одну или несколько стадий полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения, должны определять управленческие и технические действия для каждой из стадий, за которую они несут полную ответственность, гарантирующие достижение и поддержание необходимой функциональной безопасности E/E/PE систем, связанных с безопасностью. В частности, должны быть рассмотрены такие вопросы, как:

a) политика и стратегия достижения функциональной безопасности, а также средства для оценки ее достижения и средства коммуникации внутри организации для обеспечения культуры безопасной работы;

b) идентификация отдельных лиц, подразделений и организаций, несущих ответственность за выполнение и контроль над соответствующими стадиями полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения (включая, где это необходимо, государственные органы лицензирования и органы регулирования в области безопасности);

c) применяемые этапы полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES систем или программного обеспечения;

d) способ структурирования и объем информации, подлежащий документированию (см. раздел 5);

e) меры и методы, используемые для выполнения требований конкретных разделов и подразделов (МЭК 61508-2, МЭК 61508-3 и МЭК 61508-6);

f) действия по оценке функциональной безопасности (см. раздел 8);

g) процедуры, предназначенные для обеспечения быстрого исполнения решений и учета рекомендаций, относящихся к E/E/PE системам, связанным с безопасностью, являющихся результатом:

- анализа опасностей и рисков (см. 7.4);
- оценки функциональной безопасности (см. раздел 8);
- действий по верификации (см. 7.18);
- действий по подтверждению соответствия (см. 7.8 и 7.14)*);
- управления конфигурацией (см. 6.2.1, перечисление o), 7.16, а также МЭК 61508-2 и МЭК 61508-3);

*) Оценка соответствия — в соответствии с Федеральным Законом «О техническом регулировании».

h) процедуры, гарантирующие, что стороны, участвующие во всех процессах, связанных с полным жизненным циклом систем безопасности, жизненными циклами безопасности E/E/PES или программного обеспечения, компетентны в выполнении тех процессов, в которых они участвуют; в частности, должны быть определены:

- подготовка персонала в части диагностики и устранения отказов, а также тестирования системы;
- подготовка эксплуатационного персонала;
- переподготовка персонала через определенные периоды времени.

Примечание — В приложении В приведены руководящие указания, касающиеся требований к компетенции персонала, участвующего в полном жизненном цикле систем безопасности, жизненных циклах безопасности E/E/PES или программного обеспечения.

i) процедуры, которые гарантируют, что опасные инциденты (или инциденты, которые могут привести к опасным последствиям) будут проанализированы и что будут выработаны рекомендации по минимизации возможности их повторения;

j) процедуры для анализа работ по эксплуатации и обслуживанию, в частности, процедуры для:

- выявления систематических отказов, которые могут нарушить функциональную безопасность, включая процедуры, которые используются во время обычного обслуживания при обнаружении повторяющихся отказов;
- оценки того, находятся ли интенсивность запросов и частота отказов при работе в соответствии с предположениями, сделанными на этапе проектирования системы;

k) требования к периодическому аудиту функциональной безопасности в соответствии с настоящим подразделом, включая:

- частоту проведения аудита функциональной безопасности;
- анализ уровня независимости стороны, отвечающей за аудит;
- документацию и программу выполнения аудита;

l) процедуры по инициированию модификаций систем, связанных с безопасностью (см. 7.16.2.2);

m) необходимые процедуры согласования и утверждение для осуществления модификаций;

n) процедуры, связанные с предоставлением точной информации, касающейся возможных опасностей и систем, связанных с безопасностью;

o) процедуры управления конфигурацией E/E/PE систем, связанных с безопасностью, в течение стадий полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения; в частности, должны быть указаны:

- стадии, на которых должен проводиться формальный контроль конфигурации;
- процедуры, которые должны быть использованы для уникальной идентификации всех составных частей компонентов (аппаратных средств и программного обеспечения);
- процедуры для предотвращения использования неутвержденных компонентов.

Примечание — Более подробное описание управления конфигурацией приводится в [6] и [7].

p) обеспечение, при необходимости, подготовки и информации для аварийных служб.

6.2.2 Действия, указанные в 6.2.1, должны быть реализованы, их выполнение должно контролироваться.

6.2.3 Требования 6.2.1 должны быть отрецензированы заинтересованными организациями, и должно быть достигнуто согласие по этим вопросам.

6.2.4 Все несущие ответственность за действия по управлению функциональной безопасностью должны быть проинформированы о том, за что несут ответственность.

6.2.5 Поставщики, предоставляющие продукцию или услуги организациям, несущим общую ответственность за одну или несколько стадий полного жизненного цикла безопасности, жизненных циклов E/E/PES систем или программного обеспечения (см. 6.2.1), должны поставлять свою продукцию в соответствии со спецификациями этих организаций и иметь соответствующую систему управления качеством.

7 Требования к полному жизненному циклу безопасности

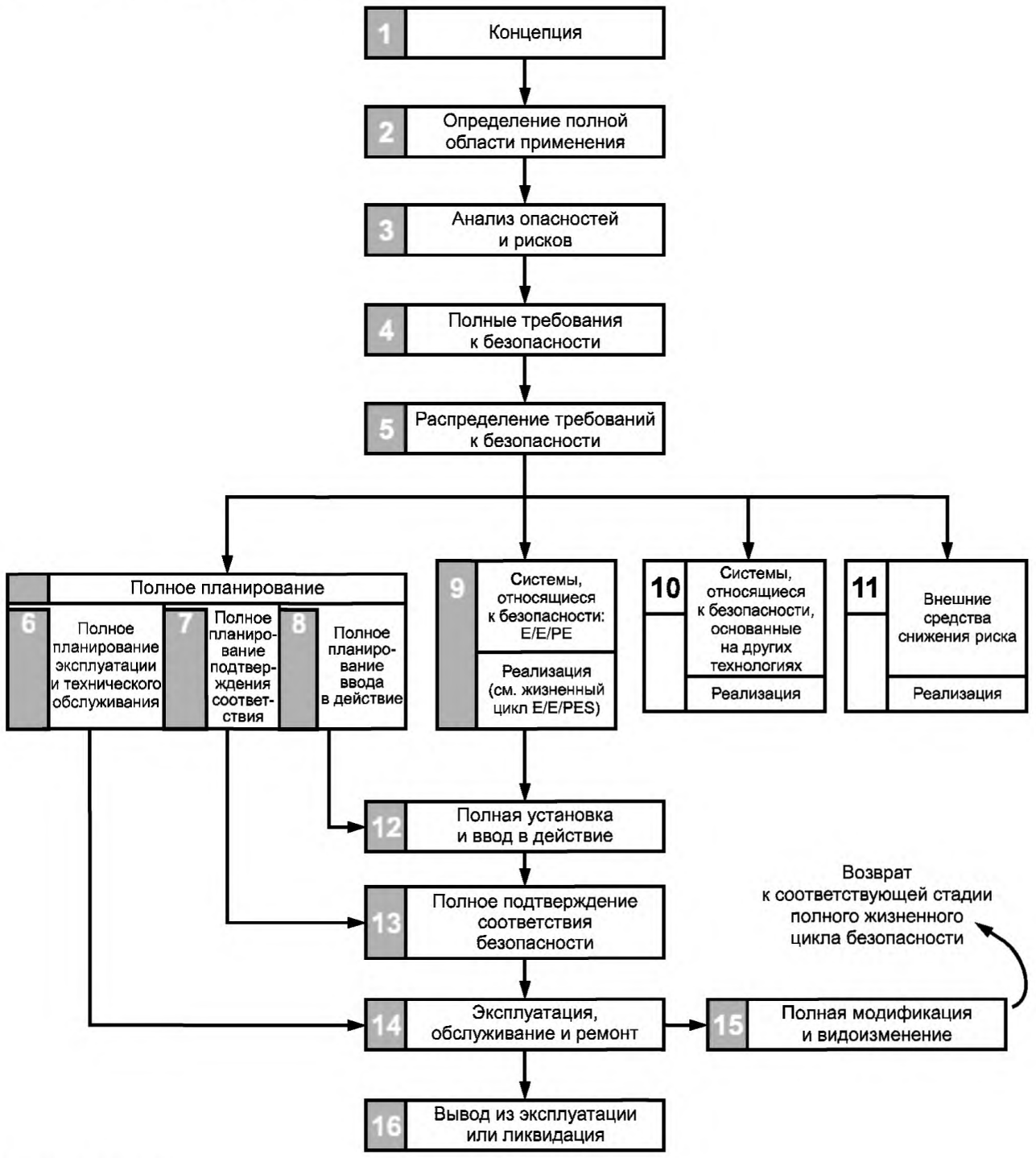
7.1 Общие положения

7.1.1 Введение

7.1.1.1 Для того, чтобы на систематической основе выполнить все действия, необходимые для достижения требуемого уровня полноты безопасности E/E/PE систем, связанных с безопасностью, в настоящем

стандарте в качестве технической основы принята модель полного жизненного цикла безопасности (см. рисунок 2).

Примечание — Полный жизненный цикл безопасности должен использоваться как основа при декларировании соответствия настоящему стандарту, однако при этом может использоваться жизненный цикл безопасности, отличный от того, который показан на рисунке 2, при условии, что все цели и требования каждого раздела настоящего стандарта выполняются.



Примечания

1 Действия, относящиеся к верификации, управлению функциональной безопасностью и оценке функциональной безопасности, не показаны из соображений ясности рисунков, однако они относятся ко всем стадиям полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения.

2 Стадии, представленные на рисунке прямоугольниками 10 и 11, находятся вне области применения настоящего стандарта.

3 МЭК 61508-2 и МЭК 61508-3 относятся к прямоугольнику 9 (реализация), но они также относятся, при необходимости, к аспектам прямоугольников 13, 14 и 15 программируемой электроники (аппаратным средствам и программному обеспечению).

Рисунок 2 — Полный жизненный цикл безопасности

7.1.1.2 Модель полного жизненного цикла безопасности включает следующие меры по снижению риска:

- E/E/PE системы, связанные с безопасностью;
- системы, связанные с безопасностью, основанные на других технологиях;
- внешние средства уменьшения риска.

7.1.1.3 Часть полного жизненного цикла безопасности, которая имеет дело с E/E/PE системами, связанными с безопасностью, показана на рисунке. 3. Она носит название жизненного цикла E/E/PES и составляет техническую основу МЭК 61508-2. Жизненный цикл безопасности программного обеспечения показан на рисунке 4, он образует техническую основу для МЭК 61508-3. Соотношения между полным жизненным циклом безопасности и жизненными циклами E/E/PES и программного обеспечения показаны на рисунке 5.

7.1.1.4 Рисунки 2 — 4, на которых показаны полный жизненный цикл безопасности, жизненные циклы безопасности E/E/PES и программного обеспечения, представляют собой упрощенное отображение действительности; они не показывают итеративных процессов внутри стадий или между стадиями. В то же время итерации представляют собой существенную и жизненно важную часть разработки полного жизненного цикла безопасности и жизненных циклов безопасности E/E/PES и программного обеспечения.

7.1.1.5 На рисунках 2 — 4, изображающих полный жизненный цикл безопасности, жизненные циклы безопасности E/E/PES и программного обеспечения, не показаны действия, относящиеся к управлению функциональной безопасностью (см. раздел 6), верификации (см. 7.18) и оценке функциональной безопасности (см. раздел 8). Это было сделано для упрощения рисунков. Эти действия, при необходимости, должны применяться на соответствующих стадиях полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения.

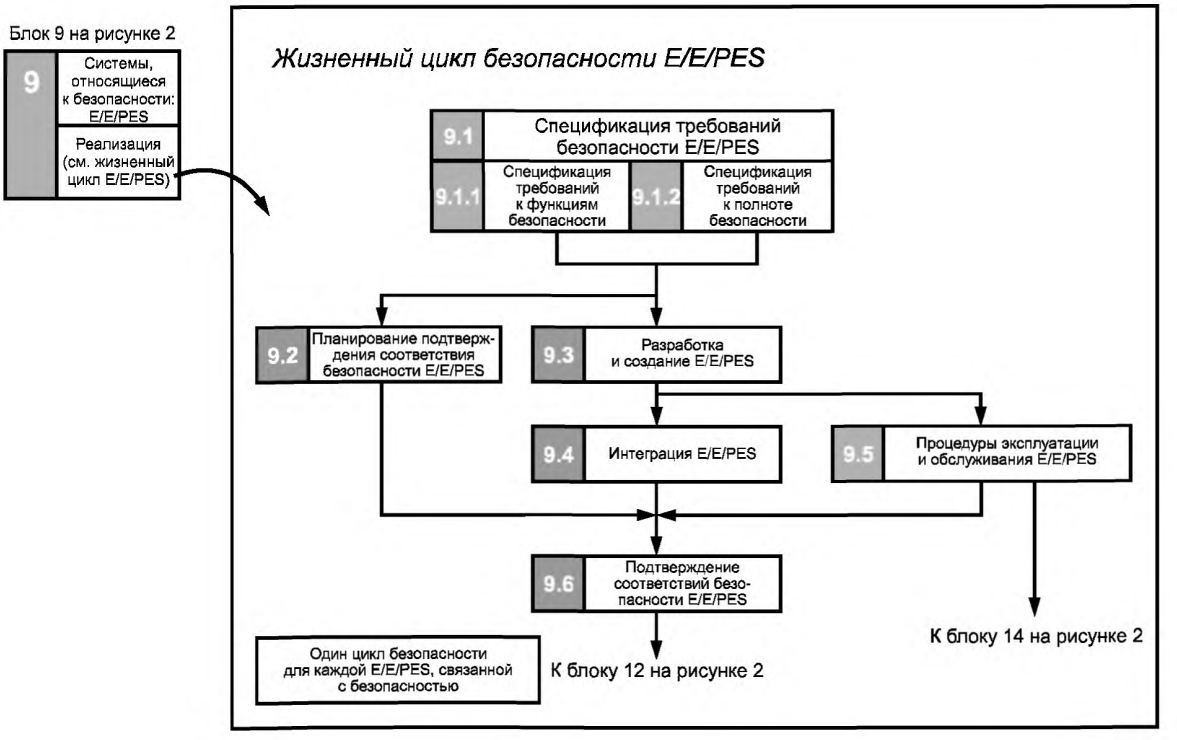


Рисунок 3 — Жизненный цикл безопасности E/E/PES (на этапе реализации)

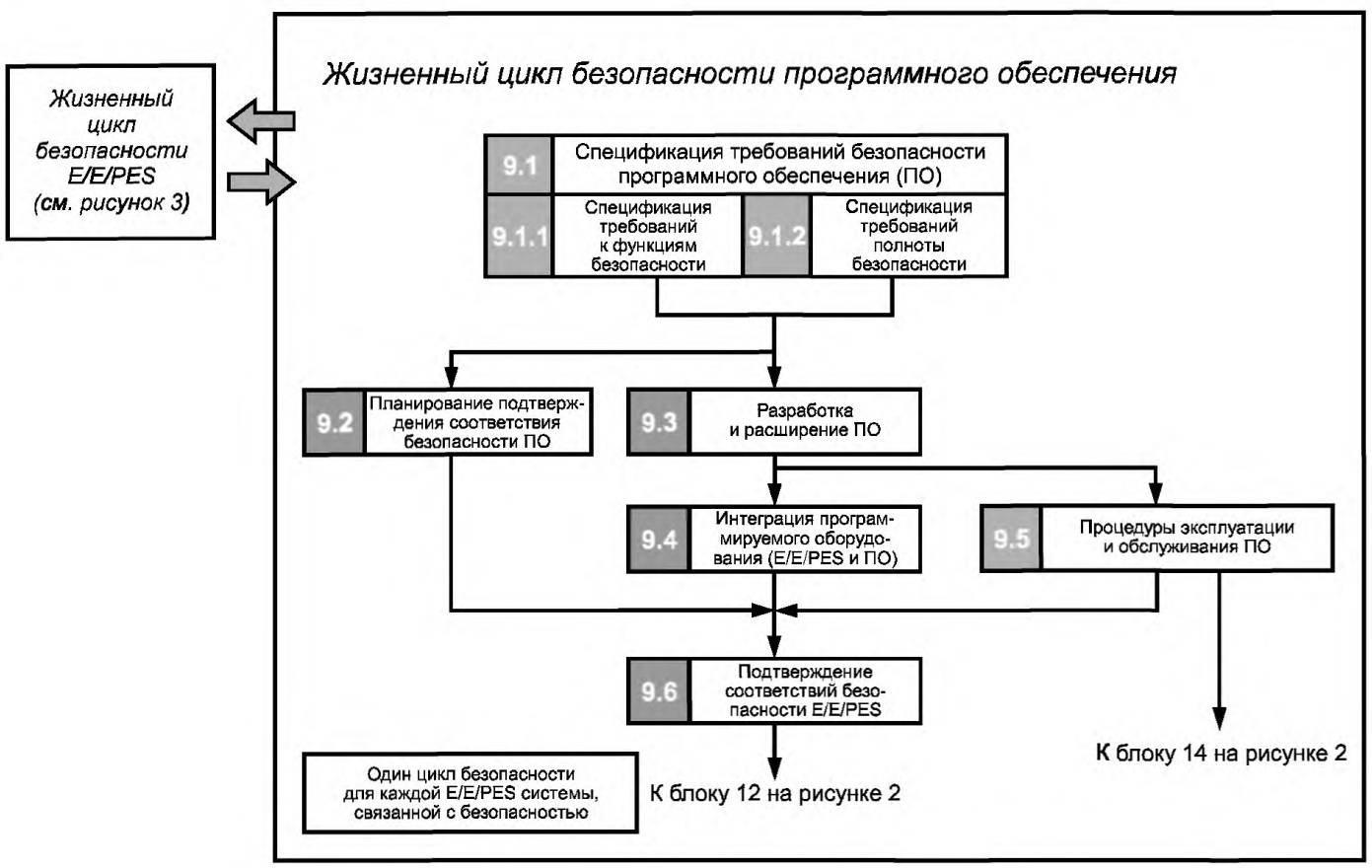


Рисунок 4 — Жизненный цикл безопасности программного обеспечения (на этапе реализации)

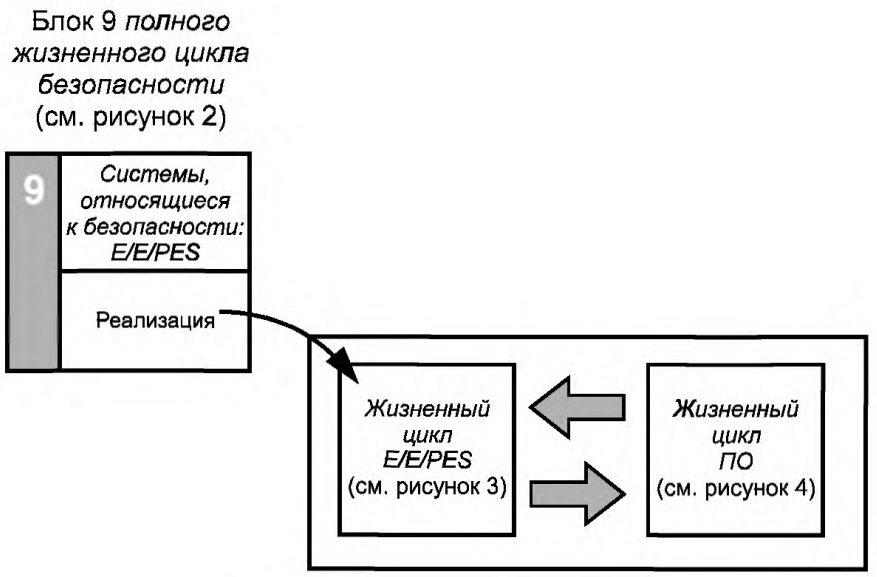


Рисунок 5 — Соотношение между полным жизненным циклом безопасности и жизненными циклами безопасности E/E/PES и программного обеспечения

7.1.2 Цели и требования: общие положения

7.1.2.1 Цели и требования для стадий полного жизненного цикла безопасности содержатся в 7.2 — 7.17. Цели и требования для стадий жизненного цикла E/E/PES и программного обеспечения содержатся в МЭК 61508-2 и МЭК 61508-3 соответственно.

Примечание — Подразделы 7.2 — 7.17 связаны с прямоугольниками (стадиями) на рисунке 2. Конкретный прямоугольник указан в примечаниях к соответствующему подразделу.

7.1.2.2 Для всех стадий полного жизненного цикла безопасности в таблице 1 указаны:
- цели, которые должны быть достигнуты;
- область применения стадий;
- ссылки на подразделы, содержащие требования;
- требования к входным материалам для стадии;
- выходные материалы, необходимые для обеспечения соответствия с требованиями.

Таблица 1 — Полный жизненный цикл безопасности: обзор

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
1 Концепция	7.2.1 Повышение уровня понимания EUC и его среды (физической, законодательной и др.), достаточного для удовлетворительного выполнения других действий в жизненном цикле безопасности	EUC и его среда (физическая, законодательная и др.)	7.2.2	Вся существенная информация, необходимая для удовлетворения требований подраздела	Информация, полученная в 7.2.2.1 – 7.2.2.6
2 Полное определение области распространения	7.3.1 Определение границ EUC и систем управления EUC. Определение границ анализа опасностей и рисков (например, техногенного, природного характера и др.)	EUC и его среда	7.2.3	Информация изложена в 7.2.2.1 – 7.2.2.6	Информация, полученная в 7.2.2.1 – 7.2.2.6
3 Анализ опасностей и рисков	7.4.1 Определение опасностей и опасных событий EUC и систем управления EUC (во всех режимах эксплуатации) для всех достаточно предсказуемых обстоятельств, включая условия ошибок и неправильного использования. Определение последовательностей событий, приводящих к определенным опасным событиям. Определение рисков EUC, связанных с определенными опасными событиями	Область распространения зависит от стадии, которая достигнута в полном жизненном цикле безопасности, циклах безопасности E/E/PES и программного обеспечения (поскольку может потребоваться осуществление более чем одного анализа опасностей и рисков). Для предварительного анализа опасностей и рисков в область распространения должны быть включены EUC, системы управления EUC и человеческий фактор	7.4.2	Информация изложена в 7.2.2.1 – 7.2.2.5	Описание и информация, относящаяся к анализу опасностей и рисков

Продолжение таблицы 1

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
4 Полные требования безопасности	7.5.1 Разработка спецификации полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности для E/E/PE систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, и внешних средств уменьшения риска для достижения требуемой функциональной безопасности	EUC, системы управления EUC и человеческий фактор	7.5.2	Описание и информация, относящаяся к анализу опасностей и рисков	Спецификация для полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности
5 Распределение требований безопасности	7.6.1 Распределение функций безопасности, содержащихся в спецификации полных требований безопасности (как требований к функциям безопасности, так и требований к полноте безопасности)	EUC, системы управления EUC и человеческий фактор	7.6.2	Спецификация для полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности	Информация и результаты распределения требований безопасности
6 Планирование эксплуатации и обслуживания	7.7.1 Разработка плана эксплуатации и технического обслуживания E/E/PE систем, связанных с безопасностью, для гарантирования выполнения требований функциональной безопасности в период эксплуатации и технического обслуживания	EUC, системы управления EUC и человеческий фактор. E/E/PE системы, связанные с безопасностью	7.7.2	Спецификация полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности	План для эксплуатации и технического обслуживания E/E/PE систем, связанных с безопасностью
7 Планирование полного подтверждения соответствия безопасности	7.8.1 Разработка плана содействия полному подтверждению соответствия безопасности E/E/PE систем, связанных с безопасностью	EUC, системы управления EUC и человеческий фактор. E/E/PE системы, связанные с безопасностью	7.8.2	Спецификация полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности	План содействия подтверждению соответствия безопасности E/E/PE систем, связанных с безопасностью

Продолжение таблицы 1

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
8 Полное планирование установки и пуска в действие	7.9.1 Разработка плана установки E/E/PE систем, связанных с безопасностью, в контролируемой форме для гарантирования выполнения требований функциональной безопасности. Разработка плана пуска в действие E/E/PE систем, связанных с безопасностью, в контролируемой форме для гарантирования выполнения требований функциональной безопасности	EUC и системы управления EUC. E/E/PE системы, связанные с безопасностью	7.9.2	Спецификация полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности	План установки E/E/PE систем, связанных с безопасностью. План пуска в действие E/E/PE систем, связанных с безопасностью
9 Реализация E/E/PE систем, связанных с безопасностью	7.10.1 Создание E/E/PE систем, связанных с безопасностью, в соответствии со спецификацией требований безопасности к E/E/PES (включая спецификацию требований к функциям безопасности E/E/PES и спецификацию требований к полноте безопасности E/E/PES)	E/E/PE системы, связанные с безопасностью	7.10.2 МЭК 61508-2 МЭК 61508-3	Спецификация требований к E/E/PES	Подтверждение, что каждая E/E/PE система, связанная с безопасностью, отвечает спецификации требований безопасности E/E/PES
10 Реализация систем, связанных с безопасностью, основанных на других технологиях	7.11.1 Создание систем, относящихся к безопасности, основанных на других технологиях, отвечающих требованиям к функциям безопасности и требованиям к полноте безопасности, определенных для таких систем (выходит за рамки области определения настоящего стандарта)	Системы, связанные с безопасностью, основанные на других технологиях	7.11.2	Спецификация требований безопасности систем, основанных на других технологиях (выходит за пределы области определения настоящего стандарта и в дальнейшем не рассматривается в настоящем стандарте)	Подтверждение того, что системы, связанные с безопасностью, основанные на других технологиях, отвечают требованиям безопасности для этих систем

Продолжение таблицы 1

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
11 Реализация внешних средств уменьшения риска	7.12.1 Создание внешних средств сокращения риска для удовлетворения требований к функциям безопасности и требований к полноте безопасности, определенных для таких средств (выходит за область определения настоящего стандарта)	Внешние средства уменьшения риска	7.12.2	Спецификация требований безопасности к внешним средствам сокращения риска (выходит за пределы области определения настоящего стандарта, и в дальнейшем не рассматривается в настоящем стандарте)	Подтверждение, что внешние средства сокращения риска отвечают требованиям безопасности для таких средств
12 Полная установка и пуск в действие	7.13.1 Установка E/E/PE систем, связанных с безопасностью. Пуск в действие E/E/PE систем, связанных с безопасностью	EUC и системы управления EUC. E/E/PE системы, связанные с безопасностью	7.13.2	План по установке E/E/PE систем, связанных с безопасностью. План по пуску в действие систем, связанных с безопасностью	Полностью установленные E/E/PE системы, связанные с безопасностью. Полностью пущенные в действие E/E/PE системы, связанные с безопасностью
13 Полное подтверждение соотвествия безопасности	7.14.1 Подтверждение того, что E/E/PE системы, связанные с безопасностью, отвечают спецификации полных требований безопасности в терминах полных требований к функциям безопасности и полных требований к полноте безопасности с учетом распределения требований безопасности для E/E/PE систем, связанных с безопасностью, в соответствии с 7.6	EUC и системы управления EUC. E/E/PE системы, связанные с безопасностью	7.14.2	Полный план подтверждения соответствия для E/E/PE систем, связанных с безопасностью. Спецификация полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности. Распределение требований безопасности	Подтверждение того, что E/E/PE системы, связанные с безопасностью, отвечают спецификации полных требований безопасности в терминах требований к функциям безопасности и требований к полноте безопасности с учетом распределения требований безопасности для E/E/PE систем, связанных с безопасностью

Окончание таблицы 1

Стадия жизненного цикла безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
14 Эксплуатация, обслуживание и ремонт	7.15.1 Реализация эксплуатации, обслуживания и ремонта (восстановления) E/E/PE систем, связанных с безопасностью таким образом, чтобы выполнялись определенные (заданные) требования функциональной безопасности	EUC и системы управления EUC. E/E/PE системы, связанные с безопасностью	7.15.2	План эксплуатации, технического обслуживания и восстановления. E/E/PE систем, связанных с безопасностью.	Долговременная реализация требуемой функциональной безопасности для E/E/PE систем, связанных с безопасностью. Хронологическая документация по эксплуатации, обслуживанию и восстановлению E/E/PE систем, связанных с безопасностью
15 Внесение изменений и модификация	7.16.1 Функциональная безопасность E/E/PE систем, связанных с безопасностью, должна соответствовать необходимым требованиям как во время, так и после стадии внесения изменений и модификации, если она имела место	EUC и системы управления EUC. E/E/PE системы, связанные с безопасностью	7.16.2	Запрос на внесение изменений или модификацию в соответствии с процедурами по управлению функциональной безопасностью	Обеспечение требуемой функциональной безопасности для E/E/PE систем, связанных с безопасностью как во время, так и после стадии внесения изменений и модификации, если она имела место. Хронологическая документация по эксплуатации, обслуживанию и восстановлению E/E/PE систем, связанных с безопасностью
16 Вывод из эксплуатации или утилизация	7.17.1 Функциональная безопасность E/E/PE систем, связанных с безопасностью, должна находиться в соответствии с обстоятельствами как во время, так и после осуществления действий по выводу из эксплуатации или утилизации EUC	EUC и системы управления EUC. E/E/PE системы, связанные с безопасностью	7.17.2	Запрос на вывод из эксплуатации или утилизацию в соответствии с процедурами по управлению функциональной безопасностью	Обеспечение требуемой функциональной безопасности для E/E/PE систем, связанных с безопасностью как во время, так и после осуществления действий по выводу из эксплуатации или утилизации. Хронологическая документация по действиям по выводу из эксплуатации и утилизации

7.1.3 Цели

7.1.3.1 Первой целью требований настоящего подраздела является структурирование на систематической основе стадий полного жизненного цикла безопасности, которые должны рассматриваться для достижения требуемой функциональной безопасности E/E/PE систем, связанных с безопасностью.

7.1.3.2 Вторая цель требований настоящего подраздела состоит в документировании ключевой информации, имеющей отношение к функциональной безопасности E/E/PE систем, связанных с безопасностью на протяжении полного жизненного цикла безопасности.

Примечание — Структуру документации см. в разделе 5 и приложении А. Структура документации может учитывать процедуры, используемые в компаниях, и рабочую практику, сложившуюся в конкретных прикладных областях.

7.1.4 Требования

7.1.4.1 Полный жизненный цикл безопасности, который должен использоваться как основа для декларирования соответствия настоящему стандарту, показан на рисунке 2. Если используется иная модель полного жизненного цикла безопасности, она должна быть определена во время планирования функциональной безопасности, при этом должны быть реализованы все задачи и требования каждого раздела и подраздела настоящего стандарта.

Примечание — Жизненный цикл безопасности E/E/PES и жизненный цикл безопасности программного обеспечения (образующие стадию реализации полного жизненного цикла систем безопасности), которые должны использоваться при декларировании соответствия, определены соответственно в МЭК 61508-2 и МЭК 61508-3.

7.1.4.2 Требования к управлению функциональной безопасностью (см. раздел 6) должны выполняться параллельно стадиям полного жизненного цикла безопасности.

7.1.4.3 Если иное не обосновано специально, должна применяться каждая стадия полного жизненного цикла безопасности, и требования должны выполняться.

7.1.4.4 Каждая стадия полного жизненного цикла безопасности должна быть разделена на элементарные действия, для которых должны быть указаны область применения, входные и выходные материалы.

7.1.4.5 Область применения и входные материалы для каждой стадии полного жизненного цикла безопасности должны соответствовать тем, которые указаны в таблице 1.

7.1.4.6 Если иное не обосновано при планировании функциональной безопасности или не определено в стандарте для области применения, выходные материалы для каждой стадии полного жизненного цикла безопасности должны соответствовать материалам, которые указаны в таблице 1.

7.1.4.7 Выходные материалы каждой стадии полного жизненного цикла безопасности должны удовлетворять целям и требованиям, специфицированным для каждой стадии (см. 7.2 — 7.17).

7.1.4.8 Требования к верификации, которые должны быть выполнены для каждой стадии полного жизненного цикла безопасности, определены в 7.18.

7.2 Концепция

Примечание — Эта стадия представлена прямоугольником 1 на рисунке 2.

7.2.1 Цель

Цель требований настоящего подраздела состоит в расширении уровня понимания EUC и окружающей среды (физической, законодательной и т.п.), достаточного для того, чтобы могли быть удовлетворительно выполнены другие действия на жизненном цикле безопасности.

7.2.2 Требования

7.2.2.1 Необходимо собрать подробную информацию о EUC, требуемых функциях управления и окружающей среде.

7.2.2.2 Необходимо определить потенциальные источники опасностей.

7.2.2.3 Необходимо получить информацию об установленных опасностях (токсичности, взрывоопасности, коррозионной активности, реакционной способности, возгораемости и т.д.).

7.2.2.4 Необходимо получить информацию о текущем состоянии регулирования в области безопасности (на национальном и международном уровнях).

7.2.2.5 Должны быть рассмотрены опасности, вызванные взаимодействием с другими EUC (установленными или которые будут установлены), вблизи рассматриваемого EUC.

7.2.2.6 Требования 7.2.2.1 — 7.2.2.5 и результаты их выполнения должны быть документированы.

7.3 Определение полной области применения

Примечание — Эта стадия представлена на рисунке 2 прямоугольником 2.

7.3.1 Цели

7.3.1.1 Первая цель требований настоящего подраздела состоит в определении границ между EUC и системой управления EUC.

7.3.1.2 Второй целью требований настоящего подраздела является определение области применения анализа опасностей и рисков (например, опасностей, связанных с процессами, опасностей, связанных с окружающей средой, и т.п.).

7.3.2 Требования

7.3.2.1 Должно быть определено физическое оборудование, включая EUC и системы управления EUC, которое входит в область применения анализа опасностей и рисков.

Примечание — См. [1] и [2].

7.3.2.2 Должны быть определены внешние события, которые должны быть учтены при анализе опасностей и рисков.

7.3.2.3 Должны быть определены подсистемы, связанные с опасностями и рисками.

7.3.2.4 Должны быть определены типы событий, приводящие к аварии или несчастному случаю, которые необходимо учитывать (например, отказы компонентов, отказы процедур, человеческие ошибки, зависимые механизмы отказов, которые могут привести к последовательности аварий).

7.3.2.5 Требования 7.3.2.1 — 7.3.2.4 и результаты их выполнения должны быть документированы.

7.4 Анализ опасностей и рисков

Примечание — Данная стадия представлена на рисунке 2 прямоугольником 3.

7.4.1 Цели

7.4.1.1 Первая цель требований настоящего подраздела состоит в определении опасностей и опасных событий EUC и системы управления EUC (во всех режимах работы) для всех обоснованных предсказуемых случаев, включая условия появления отказов и предсказуемое неправильное применение аппаратных средств и программного обеспечения.

7.4.1.2 Вторая цель требований настоящего подраздела заключается в определении последовательностей событий, приводящих к опасным событиям, определенным в 7.4.1.1.

7.4.1.3 Третьей целью требований настоящего подраздела является определение рисков EUC, связанных с опасными событиями, определенными в 7.4.1.1.

Примечания

1 Настоящий подраздел необходим потому, что требования безопасности для E/E/PE систем, связанных с безопасностью, базируются на подходе, основанном на систематическом анализе рисков. Такой подход не может быть реализован без учета EUC и системы управления EUC.

2 В тех областях применения, в которых могут быть сделаны достоверные предположения о рисках, вероятных опасностях, опасных событиях и их последствиях, анализ, необходимый для данного подраздела (и подраздела 7.5), может быть выполнен разработчиками версий настоящего стандарта, предназначенных для областей применения; анализ может быть встроен в упрощенные графические требования. Примеры таких методов приведены в МЭК 61508-5 (приложения D и E).

7.4.2 Требования

7.4.2.1 Должен быть проведен анализ опасностей и рисков, который учитывает информацию, полученную в ходе стадии определения полной области применения (см. 7.3). Если на более поздних стадиях полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения принимаются решения, которые могут изменить базис, на котором основывались более ранние решения, должен быть проведен дальнейший анализ опасностей и рисков.

Примечания

1 Руководящие указания см. в [1] и [2].

2 Может возникнуть необходимость в выполнении анализа опасностей и рисков несколько раз.

3 В качестве примера необходимости проводить углубленный анализ опасностей и рисков в ходе полного жизненного цикла безопасности рассмотрим анализ EUC, который включает в себя клапан, связанный с безопасностью. Анализ опасностей и рисков может определить две последовательности событий, одну для случая отказа при закрывании клапана, другую — для случая отказа при его открывании, которые могут приводить к опасным событиям. Однако при детальном анализе системы управления EUC, управляющей работой клапана,

может быть обнаружен новый режим отказов, связанный с колебаниями клапана, который добавляет новую последовательность событий, приводящую к опасному событию.

7.4.2.2 Должно быть рассмотрено исключение опасностей.

Примечание — Хотя это и не относится к области применения настоящего стандарта, первостепенную важность имеет изначальное исключение выявленных опасностей, связанных с EUC, например путем применения безопасных в своей основе принципов и хороших инженерных решений.

7.4.2.3 Опасности и опасные события, связанные с EUC и системой управления EUC, должны быть определены для всех разумно предсказуемых условий (включая условия возникновения отказов и разумно предсказуемое неправильное использование). В этот круг входят все случаи, связанные с человеческим фактором. Особое внимание должно быть уделено аномальным и редким режимам работы EUC.

Примечание — Разумно предсказуемое неправильное использование см. в МЭК 61508-4 (пункт 3.1.11).

7.4.2.4 Должны быть определены последовательности событий, ведущие к опасным событиям, определенным в 7.4.2.3.

Примечание — Обычно имеет смысл рассмотреть возможность исключения какой-либо последовательности событий путем модификации процесса проектирования или используемого оборудования.

7.4.2.5 Должна быть оценена вероятность опасных событий для условий, указанных в 7.4.2.3.

Примечание — Вероятность конкретного события может быть выражена количественно или качественно (МЭК 61508-5).

7.4.2.6 Должны быть определены возможные последствия, связанные с опасными событиями, определенными в 7.4.2.3.

7.4.2.7 Для каждого опасного события должен быть рассчитан или оценен риск, связанный с EUC.

7.4.2.8 Требования 7.4.2.1 — 7.4.2.7 могут быть удовлетворены путем применения качественного или количественного анализа рисков и опасностей (МЭК 61508-5).

7.4.2.9 Пригодность метода и область его применения зависят от ряда факторов, в число которых входят:

- конкретные опасности и их последствия;
- прикладная область и принятая в нем практика, считающаяся «хорошей»;
- требования норм правового и технического регулирования в области безопасности;
- риски EUC;
- доступность точных данных, на которых должен основываться анализ опасностей и рисков.

7.4.2.10 При анализе опасностей и рисков должно быть учтено следующее:

- каждое установленное опасное событие и все компоненты, оказывающие влияние на него;
- последствия и вероятность последовательности событий, с которой связано каждое опасное событие;
- необходимое уменьшение риска для каждого опасного события;
- меры, предпринимаемые для уменьшения или исключения опасностей и рисков;
- допущения, сделанные при анализе рисков, включая оцененные интенсивности запросов и интенсивности отказов оборудования; должна быть детализирована степень доверия к ограничениям в работе и вмешательству человека;
- ссылки на ключевую информацию (см. раздел 5 и приложение А), относящуюся к системам, связанным с безопасностью, на каждой стадии жизненного цикла E/E/PES (например, на действия по верификации и подтверждению соответствия).

7.4.2.11 Информация и результаты, которые составляют анализ опасностей и рисков, должны быть документированы.

7.4.2.12 Информация и результаты анализа опасностей и рисков для EUC и системы управления EUC должны поддерживаться на протяжении всего жизненного цикла безопасности, начиная со стадии анализа опасностей и рисков и до вывода из эксплуатации или ликвидации.

Примечание — Поддержка информации и результатов анализа опасностей и рисков, начиная со стадии анализа опасностей и рисков, является главным средством для установления прогресса в разрешении проблем, связанных с результатом анализа опасностей и рисков.

7.5 Полные требования к безопасности

Примечание — Эта стадия представлена на рисунке 2 прямоугольником 4.

7.5.1 Целью требований настоящего подраздела является разработка полных требований к безопасности, выраженных в требованиях к функциям безопасности и требованиях к полноте безопасности, относящихся к E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и к внешним средствам снижения риска и предназначенных для достижения необходимой функциональной безопасности.

Примечание — В тех областях применения, в которых могут быть сделаны достоверные предположения о рисках, вероятных опасностях, опасных событиях и их последствиях, анализ, необходимый для данного подраздела (и подраздела 7.5), может быть выполнен разработчиками версий настоящего стандарта, предназначенных для областей применения; анализ может быть встроен в упрощенные графические требования. Примеры таких методов приведены в МЭК 61508-5 (приложения D и E).

7.5.2 Требования

7.5.2.1 Для каждой установленной опасности должны быть определены функции безопасности, необходимые для обеспечения требуемой функциональной безопасности. Они должны формировать общую спецификацию требований к функциям безопасности.

Примечание — На этой стадии функции безопасности, которые должны выполняться, не описываются на технологическом уровне, поскольку используемые методы и технология реализации станут известны позже. При определении требований к безопасности (см. 7.6) может потребоваться изменить описание функций безопасности в соответствии с конкретными методами реализации.

7.5.2.2 Для каждого установленного опасного события должно быть определено требуемое уменьшение риска. Требуемое уменьшение риска может быть определено количественным или качественным методом.

Примечание — Требуемое уменьшение риска необходимо для того, чтобы определить требования к полноте безопасности для E/E/PE систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, и внешних средств уменьшения риска. В МЭК 61508-5 (приложение C) описан один из методов, который может применяться для определения требуемого уменьшения риска при использовании количественного подхода. В МЭК 61508-5 (приложения D и E) описаны качественные методы, однако в приводимых примерах требуемое уменьшение риска включается неявно, то есть не формулируется явным образом.

7.5.2.3 В тех случаях, когда существуют международные стандарты для прикладных областей, которые включают методы для прямого определения требуемого уменьшения риска, эти стандарты могут быть использованы для выполнения требований настоящего подраздела.

7.5.2.4 Когда отказы системы управления EUC относятся к одной или нескольким системам, связанным с безопасностью, основанным на E/E/PE или других технологиях, и/или к внешним средствам уменьшения риска и когда система управления EUC не позиционируется как система, связанная с безопасностью, то должны применяться следующие требования:

a) интенсивность опасных отказов для системы управления EUC должна быть подтверждена:

- данными по фактической работе системы управления EUC в схожем применении, или
- анализом надежности, выполненным с использованием признанной процедуры, или
- данными по надежности из промышленной базы данных по оборудованию;

b) интенсивность опасных отказов, объявленная для системы управления EUC, должна быть не ниже чем 10^{-5} отказов в час.

Примечание — Обоснование этого требования состоит в том, что если система управления EUC не позиционируется как система, связанная с безопасностью, то интенсивность отказов, которая может быть объявлена для системы управления EUC, не должна быть ниже, чем верхнее целевое (планируемое) значение отказов для уровня полноты безопасности 1 (которая составляет 10^{-5} опасных отказов в час; см. таблицу 3);

c) должны быть определены и учтены при разработке спецификации общих требований к безопасности все разумно предсказуемые режимы опасных отказов системы управления EUC;

d) система управления EUC должна быть отдельной и независимой от E/E/PE систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, и внешних средств уменьшения риска.

Примечание — Если системы, связанные с безопасностью, проектировались для обеспечения адекватной полноты безопасности с учетом обычной интенсивности запросов от системы управления EUC, то не требуется позиционировать систему управления EUC как систему, связанную с безопасностью, (и, следовательно, ее функции не будут позиционироваться как функции безопасности в контексте настоящего стандарта).

В некоторых применениях, в частности, где требуется очень высокая степень полноты безопасности, может оказаться приемлемым уменьшение интенсивности запросов путем проектирования для системы управления EUC меньшей, чем обычно, интенсивности отказов. В таких случаях, если интенсивность отказов меньше, чем верхняя граница целевой полноты безопасности для уровня полноты безопасности, равного 1 (см. таблицу 3), система управления становится системой, связанной с безопасностью, и к ней применяются требования настоящего стандарта.

7.5.2.5 Если требования 7.5.2.4 [перечисления a) — d)] не могут быть соблюдены, то система управления EUC должна рассматриваться как система, связанная с безопасностью. Уровень полноты безопасности, отнесенный к системе управления EUC, должен основываться на интенсивности отказов, объявленной для системы управления EUC в соответствии с целевыми значениями отказов, приведенными в таблицах 2 и 3. В таких случаях требования настоящего стандарта, относящиеся к назначаемому уровню полноты безопасности, должны применятся к системе управления EUC.

Примечания

1 Например, если для системы управления EUC объявлена интенсивность отказов 10^{-6} — 10^{-5} отказов в час, то должны быть выполнены требования, соответствующие уровню полноты безопасности, равному 1.

2 См. также 7.6.2.10.

7.5.2.6 Для каждой функции безопасности должны быть указаны требования к полноте безопасности, выраженные в требуемом уменьшении риска. Они должны составлять спецификацию полных требований к полноте безопасности.

Примечание — Спецификация требований к полноте безопасности представляет собой промежуточную стадию на пути к определению уровней полноты безопасности для функций безопасности, которые должны быть реализованы E/E/PE системами, связанными с безопасностью. Некоторые из качественных методов, используемых для определения уровней полноты безопасности [МЭК 61508-5 (приложения D и E)] содержат переход непосредственно от параметров риска к уровням полноты безопасности. В таких случаях требуемое уменьшение риска является неявным, то есть не формулируется явным образом, поскольку оно интегрировано в сам метод.

7.5.2.7 Спецификации функций безопасности (см. 7.5.2.1) и требований к полноте безопасности (см. 7.5.2.6) должны совместно формировать спецификацию полных требований безопасности.

7.6 Распределение требований безопасности

Примечание — Эта стадия представлена на рисунке 2 прямоугольником 5.

7.6.1 Цели

7.6.1.1 Первой целью требований настоящего подраздела является распределение функций безопасности, содержащихся в спецификации полных требований безопасности (включающей требования к функциям безопасности и требования к полноте безопасности), по назначенным E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам уменьшения риска.

Примечание — Системы безопасности, основанные на других технологиях, и внешние средства уменьшения риска рассматриваются, при необходимости, когда распределение по E/E/PE системам, связанным с безопасностью, не может быть выполнено без учета других мер по снижению риска.

7.6.1.2 Второй целью требований настоящего подраздела является распределение уровня полноты безопасности для каждой функции безопасности.

Примечание — Уровни полноты безопасности, как указано в 7.5, выражаются через снижение риска.

7.6.2 Требования

7.6.2.1 Должны быть определены назначенные системы, связанные с безопасностью, которые будут использоваться для достижения требуемой функциональной безопасности. Требуемое уменьшение риска может быть достигнуто за счет:

- внешних средств уменьшения риска;
- E/E/PE систем, связанных с безопасностью;
- систем, связанных с безопасностью, основанных на других технологиях.

Примечание — Настоящий подраздел применим только при условии, что одна из систем, связанных с безопасностью, представляет собой E/E/PES.

7.6.2.2 При распределении функций безопасности по назначенным E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам уменьшения риска, должны быть учтены возможности и ресурсы всех стадий полного жизненного цикла безопасности.

Примечания

1 Все последствия использования систем, связанных с безопасностью, основанных на сложных технологиях, часто недооцениваются. В частности, реализация сложной технологии требует более высокого уровня компетентности на всех уровнях от разработки спецификаций до эксплуатации и сопровождения. Использование других, более простых технологических решений, может быть равным по эффективности и в тоже время обладать рядом преимуществ из-за уменьшившейся сложности E/E/PES.

2 Доступность возможностей и ресурсов при эксплуатации и сопровождении, а также условия работы могут иметь критическое значение для достижения требуемой функциональной безопасности в условиях реальной эксплуатации.

7.6.2.3 Каждая функция безопасности вместе с относящимся к ней требованием к полноте безопасности, разработанным в соответствии с 7.5, должна быть распределена по назначенным E/E/PE системам, связанным с безопасностью, с учетом снижения риска, достигаемого за счет систем, связанных с безопасностью, основанных на других технологиях, и внешних средств уменьшения риска для достижения требуемого снижения уровня риска для этой функции безопасности. Это распределение имеет итерационный характер. Если будет установлено, что требуемое уменьшение риска не может быть достигнуто, то архитектура должна быть изменена и распределение должно быть выполнено повторно.

Примечания

1 Каждая функция безопасности вместе с относящимся к ней требованием к полноте безопасности, выраженным через требуемое снижение риска (см. 7.5), распределяется по одной или нескольким E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях и внешним средствам уменьшения риска. Решение о распределении конкретной функции безопасности по одной или нескольким системам, связанным с безопасностью, зависит от ряда факторов, но в особенности от степени уменьшения риска, которое должно быть достигнуто с помощью функции безопасности. Чем большее снижение риска необходимо, тем больше вероятность того, что функция будет распределена между несколькими системами, связанными с безопасностью.

2 На рисунке 6 показан принятый в настоящем подразделе подход к распределению требований к безопасности.

7.6.2.4 Распределение, указанное в 7.6.2.3, должно быть выполнено таким образом, чтобы все функции безопасности были распределены и чтобы требования в отношении полноты безопасности для каждой функции безопасности были выполнены (в том числе важнейшие требования, определенные в 7.6.2.10).

7.6.2.5 Требования к полноте безопасности для каждой функции безопасности должны быть пригодны для указания того, что каждый планируемый параметр полноты безопасности является либо

- средней вероятностью отказов от выполнения ее предназначенной функции по запросу (для режима работы с низкой частотой обращений (запросов)) или
- вероятностью опасного отказа в час (для режима работы с высокой частотой запросов или режима с непрерывными запросами).

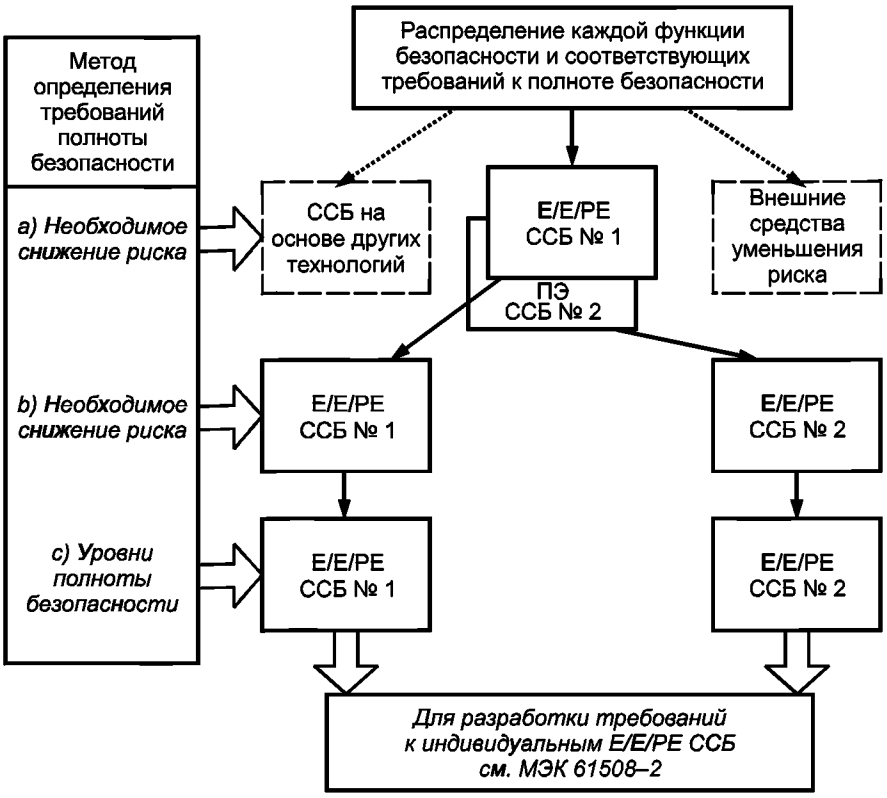
7.6.2.6 Распределение требований к полноте безопасности должно проводиться с использованием соответствующих методов для определения вероятности совместных событий.

Примечание — Распределение требований к полноте безопасности может быть выполнено с помощью качественных и/или количественных методов.

7.6.2.7 Распределение следует проводить с учетом вероятности отказов, имеющих общую причину. Если E/E/PE системы, связанные с безопасностью, системы, связанные с безопасностью, основанные на других технологиях, и внешние средства уменьшения риска должны рассматриваться при распределении как независимые, они:

- должны быть функционально различными (т.е. использовать совершенно различные подходы для достижения одних и тех же результатов);
- должны основываться на различных технологиях (т.е. в них должно использоваться оборудование различных видов для достижения одних и тех же результатов).

Примечание — Следует понимать, что сколь бы разнообразна ни была технология, в случае систем с высокой полнотой безопасности и с особо тяжелыми последствиями в случае отказа, должны быть приняты особые меры предосторожности по отношению к маловероятным событиям с общей причиной, например авиационным катастрофам или землетрясениям.



Примечания

1 Требования к полноте безопасности связываются с каждой функцией безопасности до распределения (см. 7.5.2.6).

2 Функция безопасности может быть распределена по нескольким системам, связанным с безопасностью.

3 ССБ — система(ы), связанная(ые) с безопасностью.

Рисунок 6 — Распределение требований безопасности по E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам снижения риска

- не должны иметь общих частей, систем сервиса или поддержки (например, источников питания), отказ которых может привести к отказу всех систем в опасном режиме;
- не должны иметь общих процедур эксплуатации, обслуживания или тестирования;
- должны быть физически разделенными так, чтобы предсказуемые отказы не влияли на избыточные системы, связанные с безопасностью, и внешние средства уменьшения риска.

Примечание — Настоящий стандарт касается именно распределения требований к полноте безопасности E/E/PE систем, связанных с безопасностью, и требования в нем определены так, как они должны быть заданы для этих систем. Распределение требований к полноте безопасности для систем, связанных с безопасностью, основанных на других технологиях, и для внешних средств уменьшения риска в данном стандарте подробно не рассматриваются.

7.6.2.8 Если не все требования 7.6.2.7 могут быть выполнены, то E/E/PE системы, связанные с безопасностью, системы, связанные с безопасностью, основанные на других технологиях, и внешние средства уменьшения риска не должны считаться независимыми при распределении уровней полноты безопасности, если только проведенный анализ не покажет, что они являются в достаточной степени независимыми (с точки зрения полноты безопасности).

Примечания

1 Более подробную информацию по вопросу анализа зависимых отказов см. в [9] и [10].

2 Достаточная независимость устанавливается путем демонстрации того, что вероятность зависимого отказа является достаточно низкой по сравнению с требованиями к полноте безопасности для E/E/PE систем, связанных с безопасностью.

7.6.2.9 При завершении проработки распределения требований к полноте безопасности для каждой функции безопасности, распределенных по E/E/PE системе(ам), связанной(ым) с безопасностью, должны быть выражены в терминах полноты безопасности в соответствии с таблицами 2 и 3 и должны быть пригодны для того, чтобы показать одно из двух: является ли планируемый параметр полноты безопасности

- средней вероятностью отказов по запросу от выполнения ее назначенной функции (для режима работы с низкой частотой запросов) или

- вероятностью опасных отказов в час (для режима работы с высокой частотой запросов или с непрерывными запросами).

Примечания

1 До этой стадии требования к полноте безопасности были определены в терминах уменьшения риска (см. 7.5).

2 Таблицы 2 и 3 содержат планируемые величины отказов для уровней полноты безопасности. Допускается, что может оказаться невозможным предсказать количественно полноту безопасности для всех аспектов E/E/PE систем, связанных с безопасностью. В этом случае по отношению к мерам предосторожности, необходимым для достижения запланированных характеристик отказов, должны быть применены качественные методы, меры и заключения. Это особенно относится к случаю полноты безопасности по отношению к систематическим отказам [МЭК 61508-4 (пункт 3.5.4)].

Таблица 2 — Уровни полноты безопасности: планируемые величины отказов для функции безопасности, работающей в режиме низкой интенсивности запросов

Уровень полноты безопасности	Режим работы с низкой интенсивностью запросов (средняя вероятность отказа выполнения функции по запросу)
4	$> 10^{-5} — < 10^{-4}$
3	$> 10^{-4} — < 10^{-3}$
2	$> 10^{-3} — < 10^{-2}$
1	$> 10^{-2} — < 10^{-1}$
Примечание — Подробности интерпретации данной таблицы см. в примечаниях 3 — 9 ниже.	

Таблица 3 — Уровни полноты безопасности: планируемые величины отказов для функции безопасности, работающей в режиме высокой интенсивности запросов или в режиме непрерывных запросов

Уровень полноты безопасности	Режим работы с высокой интенсивностью запросов или режим непрерывных запросов (вероятность опасных отказов в час)
4	$> 10^{-9} — < 10^{-8}$
3	$> 10^{-8} — < 10^{-7}$
2	$> 10^{-7} — < 10^{-6}$
1	$> 10^{-6} — < 10^{-5}$
Примечание — Подробности интерпретации данной таблицы см. в примечаниях 3 — 9 ниже.	

3 Определения терминов режим работы с низкой интенсивностью запросов и режим работы с высокой интенсивностью запросов или режим с непрерывными запросами см. в МЭК 61508-4, пункт 3.5.12.

4 Вероятность опасных отказов в час — параметр, используемый в таблице 3 для режима работы с высокой интенсивностью отказов или для работы в режиме с непрерывными запросами, иногда фигурирует под названием частоты опасных отказов или интенсивности опасных отказов с единицей измерения — опасные отказы в час.

5 Для E/E/PE систем, связанных с безопасностью, действующих в режиме высокой интенсивности запросов или в режиме непрерывных запросов, когда работа длится определенный промежуток времени, в течение которого ремонт не может быть выполнен, требуемый уровень полноты безопасности для функции безопасности может быть получен следующим образом. Определяется требуемая вероятность отказа функции безопасности в расчете на период работы. Полученное значение делится на продолжительность периода, в результате получается требуемая вероятность отказов в расчете на час. Далее с использованием данных таблицы 3 определятся необходимый уровень полноты безопасности.

6 Настоящий стандарт устанавливает нижнюю границу планируемых величин отказов в режиме опасных отказов, которые могут объявляться для случая опасных отказов. Они определяются как нижний предел уровня полноты безопасности 4 (т. е. средняя вероятность отказов, равная 10^{-5} при выполнении назначенной функции по запросу, или как вероятность опасного отказа, равная 10^{-9} в час). Может оказаться возможным разработать системы, связанные с безопасностью, с более низкими значениями планируемых величин отказов для несложных систем, однако считается, что цифры, приведенные в таблице, представляют предел, который может быть достигнут в настоящее время для относительно сложных систем (например, для программируемых электронных систем, связанных с безопасностью).

7 Планируемые величины отказов, которые могут быть заявлены в случае использования двух и более E/E/PE систем, связанных с безопасностью, могут оказаться лучше тех, которые приведены в таблицах 2 и 3, при условии, что достигнуты адекватные уровни независимости.

8 Важно отметить, что величины отказов для уровней полноты безопасности 1, 2, 3 и 4 являются планируемыми величинами. Принято считать, что только по отношению к полноте безопасности аппаратных средств [МЭК 61508-4 (пункт 3.5.5)] возможно дать количественную оценку и использовать надежные методы предсказания при оценке того, будут ли достигнуты планируемые величины отказов. При определении того, будут ли достаточны меры предосторожности для достижения планируемых величин отказов по отношению к полноте безопасности, связанной с систематическими отказами [МЭК 61508-4 (пункт 3.5.4)], должны быть использованы качественные методы и заключения.

9 Требования к полноте безопасности для каждой функции безопасности должны указывать, что представляют собой параметры, характеризующие планируемые величины отказов:

- среднюю вероятность не выполнения назначенной функции по запросу (при работе в режиме низкой интенсивности запросов) или
- вероятность возникновения опасных отказов в час (для режима с высокой интенсивностью запросов или режима с непрерывными запросами).

7.6.2.10 Для E/E/PE системы, связанной с безопасностью, которая реализуют функции безопасности с различными уровнями полноты безопасности, те компоненты аппаратных средств и программного обеспечения, связанного с безопасностью, для которых не установлена достаточная степень независимости, должны считаться принадлежащими к функциям безопасности с наивысшим уровнем полноты безопасности, если только не будет установлена достаточная независимость реализации этих конкретных функций. Следовательно, ко всем этим компонентам должны применяться требования, относящиеся к соответствующему наивысшему уровню полноты безопасности.

Примечание — См. также МЭК 61508-2 (пункт 7.4.2.4) и МЭК 61508-3 (пункт 7.4.2.8).

7.6.2.11 Архитектура, представленная единственной E/E/PE системой, связанной с безопасностью, имеющей уровень полноты безопасности 4, допустима только при условии выполнения требований перечисления a) либо одновременного выполнения требований перечислений b) и c):

a) была явно продемонстрирована с использованием комбинации соответствующих аналитических методов и тестирования величина отказов планируемой полноты безопасности;

b) был получен обширный опыт эксплуатации компонентов, используемых как часть E/E/PE системы, связанной с безопасностью; этот опыт должен быть получен в схожей окружающей среде и относиться к системам, имеющим, как минимум, сопоставимый уровень сложности;

c) имеется достаточный объем данных по отказам аппаратных средств, полученный для элементов, используемых в качестве компонентов E/E/PE системы, связанной с безопасностью, дающий достаточную уверенность в величине планируемых отказов для заявляемого уровня полноты безопасности аппаратуры. Данные должны соответствовать предполагаемым окружающей среде, применению и уровню сложности.

7.6.2.12 Ни одна одиночная E/E/PE система, связанная с безопасностью, не должна быть размещена по величине отказов полноты безопасности ниже, чем указано в таблицах 2 и 3. То есть, для систем, связанных с безопасностью, работающих:

- в режиме низкой интенсивности запросов в качестве нижней границы принимается средняя вероятность отказа, равная 10^{-5}, для выполнения назначенной функции по запросу;
- в режиме высокой интенсивности запросов или в режиме непрерывных запросов в качестве нижней границы принимается вероятность опасных отказов, равная 10^{-9} в час.

7.6.2.13 Информация и результаты распределения требований к безопасности, полученные в подразделах 7.6.2.1 — 7.6.2.12, вместе с любыми сделанными допущениями и обоснованиями должны быть документированы.

Примечание — Для каждой E/E/PE системы, связанной с безопасностью, должен быть достаточный объем информации по функциям безопасности и связанными с ними уровнями полноты безопасности. Эта информация образует основу требований к безопасности для E/E/PE систем, связанных с безопасностью, определяемых в МЭК 61508-2.

7.7 Полное планирование эксплуатации и сопровождения

Примечания

1 Данная стадия представлена прямоугольником 6 на рисунке 2.

2 Пример модели действий при эксплуатации и сопровождении показан на рисунке 7.

3 Пример модели управления эксплуатацией и сопровождением показан на рисунке 8.

7.7.1 Цель

Целью требований настоящего подраздела является разработка плана эксплуатации и сопровождения E/E/PE систем, связанных с безопасностью, гарантирующего, что требуемая функциональная безопасность будет поддерживаться в процессе эксплуатации и сопровождения.

7.7.2 Требования

7.7.2.1 Должен быть подготовлен план, в котором необходимо указать следующее:

a) типовые действия, необходимые для поддержания требуемой функциональной безопасности E/E/PE систем, связанных с безопасностью;

b) действия и ограничения, которые необходимы (например, при запуске, нормальной работе, стандартном тестировании, предсказуемых нарушениях, отказах и выключении) для предотвращения перехода в неустойчивое состояние, уменьшения потребности в E/E/PE системе, связанной с безопасностью, либо ослабления последствий опасных событий;

Примечание — К E/E/PE системам, связанным с безопасностью, относятся следующие ограничения:

- ограничения на работу EUC при сбое или отказе E/E/PE систем, связанных с безопасностью;
- ограничения на работу EUC в период обслуживания E/E/PE систем, связанных с безопасностью;
- когда могут быть отменены ограничения на работу EUC;
- процедуры возврата к нормальной работе;
- процедуры подтверждения того, что достигнут нормальный режим работы;
- обстоятельства, при которых функции E/E/PE систем, связанных с безопасностью, могут быть пропущены при пуске, во время выполнения специальных операций или при тестировании;
- процедуры, которым необходимо следовать до, во время и после отключения E/E/PE систем, связанных с безопасностью, включая разрешение на рабочие процедуры и уровни полномочий.

c) документацию, которую необходимо вести, и в которой отображаются результаты аудита функциональной безопасности и тестирования;

d) документацию, которая необходима для сохранения информации об опасных происшествиях и всех происшествиях, которые потенциально приводят к опасному событию;

e) совокупность действий по обслуживанию (в отличие от действий по модификации);

f) действия, которые должны быть предприняты в случае возникновения опасных событий;

g) содержание документации, в которой в хронологическом порядке регистрируются действия в период эксплуатации и обслуживания (см. 7.15).

Примечания

1 Большинство E/E/PE систем, связанных с безопасностью, имеет некоторые виды отказов, которые могут быть обнаружены только при тестировании во время стандартного обслуживания. Если тестирование не будет проводиться с достаточной частотой, требуемый уровень полноты безопасности E/E/PE систем, связанных с безопасностью, не будет достигнут. Когда тестирование выполняется в рабочем режиме, может потребоваться временное отключение E/E/PE системы, связанной с безопасностью. Это должно быть обосновано только в случае, если вероятность запросов, случающихся в это время, мала. Если в этом нет уверенности, может оказаться необходимым установить дополнительные сенсоры и исполнительные устройства для сохранения требуемой функциональной безопасности во время тестирования.

2 Данный подраздел применяется к поставщику программного обеспечения, который должен сопроводить программный продукт информацией и процедурами, которые дают возможность пользователю обеспечить необходимую функциональную безопасность во время эксплуатации и обслуживания системы, связанной с безопасностью. Подраздел включает подготовительные процедуры для любой модификации программного обеспечения, которые могут быть результатом потребностей, возникших в период эксплуатации или обслуживания [см. также МЭК 61508-3 (пункт 7.6)]. Реализация этих процедур — по МЭК 61508-3 (пункты 7.8 и 7.15). Процедуры подготовки к будущим изменениям программного обеспечения, которые являются результатом потребностей в изменении систем, связанных с безопасностью, рассматриваются в МЭК 61508-3 (пункты 7.6 и 7.16). Реализация этих процедур — по МЭК 61508-2 (пункты 7.8 и 7.16).

3 Следует учитывать процедуры по эксплуатации и обслуживанию, разработанные для того, чтобы выполнить требования МЭК 61508-2 и МЭК 61508-3.

7.7.2.2 Стандартные действия по обслуживанию, которые выполняются для обнаружения невыявленных неисправностей, должны быть выполнены на основе систематического анализа.

Примечание — Если невыявленные неисправности не обнаружены, они могут:

- в случае применения E/E/PE систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, или внешних средств уменьшения риска привести к отказам при работе по запросу;

- в случае применения систем, не связанных с безопасностью, привести к появлению (ложных) запросов к E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, или внешним средствам уменьшения риска.

7.7.2.3 План обслуживания E/E/PE систем, связанных с безопасностью, должен быть согласован с теми, кто несет ответственность за будущую эксплуатацию и обслуживание E/E/PE систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, внешних средств уменьшения риска, а также систем, не связанных с безопасностью, которые могут приводить к появлению запросов к системам, связанным с безопасностью.

7.8 Планирование полного подтверждения соответствия безопасности

Примечание — Эта стадия представлена на рисунке 2 прямоугольником 7.

7.8.1 Цель

Целью требований настоящего подраздела является разработка плана, облегчающего полное подтверждение соответствия безопасности E/E/PE систем, связанных с безопасностью.

7.8.2 Требования

7.8.2.1 Должен быть разработан план, включающий в себя следующее:

a) подробное описание того, когда должно происходить подтверждение соответствия;

b) подробности о лицах, которые должны осуществлять подтверждение соответствия;

c) спецификацию существенных режимов работы EUC с указанием их отношения к E/E/PE системе, связанной с безопасностью, включая, где это необходимо:

- подготовку к использованию, включая установку и регулировку;
- запуск;
- обучение;
- автоматический режим;
- ручной режим;
- полуавтоматический режим;
- установившийся режим работы;
- переустановку;
- выключение;
- обслуживание;
- разумно предсказуемые ненормальные условия;

d) спецификацию E/E/PE систем, связанных с безопасностью, которые требуют подтверждения соответствия для каждого режима работы EUC до начала ввода в эксплуатацию;

e) техническую стратегию для подтверждения соответствия (например, аналитические методы, статистические тесты и т.п.);

f) меры, методы и процедуры, которые должны использоваться для подтверждения того, что распределение функций безопасности было выполнено корректно; они включают подтверждение того, что каждая функция безопасности соответствует:

- спецификации полных требований к функциям безопасности и
- спецификации полных требований к полноте безопасности;

g) конкретную ссылку на каждый элемент, содержащийся в выходных материалах 7.5 и 7.6;

h) требования к окружающим условиям, при которых должны проходить действия по подтверждению соответствия (для тестирования они, например, могут включать калиброванные средства и оборудование);

i) критерии прохождения и непрохождения подтверждения соответствия;

j) политику и процедуры оценки результатов подтверждения соответствия, в частности, непрохождения подтверждения соответствия.

Примечание — При планировании полного подтверждения соответствия безопасности следует учесть работы, планируемые для подтверждения соответствия безопасности E/E/PES и подтверждения соответствия безопасности программного обеспечения согласно требованиям МЭК 61508-2 и МЭК 61508-3. Важно обеспечить, чтобы было учтено взаимодействие между всеми мерами по уменьшению риска и чтобы были реализованы все функции безопасности (определенные в выходных материалах 7.5).

7.8.2.2 Информация 7.8.2.1 должна быть документирована, и должен быть установлен план для полного подтверждения соответствия безопасности E/E/PE систем, связанных с безопасностью.

7.9 Планирование полной установки и ввода в эксплуатацию

Примечание — Эта стадия представлена на рисунке 2 прямоугольником 8.

7.9.1 Цели

7.9.1.1 Первой целью требований настоящего подраздела является разработка плана в контролируемой форме по установке E/E/PE систем, связанных с безопасностью, гарантирующего, что будет достигнута требуемая функциональная безопасность.

7.9.1.2 Вторая цель требований настоящего подраздела состоит в разработке плана в контролируемой форме по вводу в эксплуатацию E/E/PE систем, связанных с безопасностью, гарантирующего, что будет достигнута требуемая функциональная безопасность.

7.9.2 Требования

7.9.2.1 Должен быть разработан план установки E/E/PE систем, связанных с безопасностью, определяющий:

- график установки;
- лиц, ответственных за различные части установки;
- процедуры по установке;
- последовательность, в которой интегрируются различные компоненты;
- критерии для декларирования готовности к установке всех компонент E/E/PE систем, связанных с безопасностью, а также критерии для декларирования завершения установки;
- процедуры по устранению отказов и несовместимости.

7.9.2.2 Должен быть разработан план по вводу в действие E/E/PE систем, связанных с безопасностью, определяющий:

- график ввода в эксплуатацию;
- лиц, ответственных за различные этапы ввода в действие;
- процедуры по вводу в действие;
- взаимосвязь с этапами установки;
- взаимосвязь с подтверждением соответствия.

7.9.2.3 Планирование полной установки и ввода в действие должно быть документировано.

7.10 Реализация: E/E/PES

Примечание — Данная стадия представлена на рисунке 2 прямоугольником 9 и на рисунках 3 и 4 — прямоугольниками 9.1 — 9.6.

7.10.1 Цель

Целью требований настоящего подраздела является создание E/E/PE систем, связанных с безопасностью, соответствующих спецификации требований к безопасности E/E/PES (включая спецификацию требований к функциям безопасности E/E/PES и спецификацию требований к полноте безопасности E/E/PES). См. МЭК 61508-2 и МЭК 61508-3.

7.10.2 Требования

Требования — по МЭК 61508-2 и МЭК 61508-3.

7.11 Реализация: другие технологии

Примечание — Эта стадия представлена на рисунке 2 прямоугольником 10.

7.11.1 Цель

Целью требований настоящего подраздела является создание систем, связанных с безопасностью, основанных на других технологиях, удовлетворяющих требованиям к функциям безопасности и полноте безопасности, определенным для таких систем.

7.11.2 Требования

Спецификации подлежащих выполнению требований к функциям безопасности и к полноте безопасности систем, связанных с безопасностью, основанных на других технологиях, не охватываются настоящим стандартом.

Примечание — Системы, связанные с безопасностью, основанные на других технологиях, базируются на технологиях, отличных от электрической/электронной/программируемой электронной (например, на гидравлической, пневматической и т.п.). Системы, связанные с безопасностью, основанные на других технологиях, для полноты картины включены в общий жизненный цикл систем безопасности наряду с внешними средствами уменьшения риска (см. 7.12).

7.12 Реализация: внешние средства уменьшения риска

Примечание — Данная стадия представлена на рисунке 2 прямоугольником 11.

7.12.1 Цель

Целью требований настоящего подраздела является создание внешних средств уменьшения риска, удовлетворяющих требованиям к функциям безопасности и полноте безопасности, определенным для таких средств.

7.12.2 Требования

Спецификации подлежащих выполнению требований к функциям безопасности и полноте безопасности внешних средств уменьшения риска не охватываются настоящим стандартом.

Примечание — Внешние средства уменьшения риска для полноты картины были включены в общий жизненный цикл систем безопасности наряду с системами, связанными с безопасностью, основанными на других технологиях (см. 7.11).

7.13 Полная установка и ввод в действие

Примечание — Данная стадия представлена на рисунке 2 прямоугольником 12.

7.13.1 Цели

7.13.1.1 Первой целью требований настоящего подраздела является установка E/E/PE систем, связанных с безопасностью.

7.13.1.2 Вторая цель требований настоящего подраздела состоит в вводе в действие E/E/PE систем, связанных с безопасностью.

7.13.2 Требования

7.13.2.1 Действия по установке должны выполняться в соответствии с планом по установке E/E/PE систем, связанных с безопасностью.

7.13.2.2 Информация, документируемая во время установки, должна включать в себя:

- документацию по процессам установки;
- информацию об устранении отказов и несовместимости.

7.13.2.3 Ввод в действие следует выполнять в соответствии с планом по вводу в действие E/E/PE систем, связанных с безопасностью.

7.13.2.4 Информация, документируемая во время ввода в действие, должна включать в себя:

- документацию по действиям по вводу в действие;
- ссылки на отчеты об отказах;
- информацию об устранении отказов и несовместимости.

7.14 Полное подтверждение соответствия безопасности

Примечание — Эта фаза представлена на рисунке 2 прямоугольником 13.

7.14.1 Цель

Целью требований настоящего подраздела является подтверждение соответствия того, что E/E/PE система, связанная с безопасностью, удовлетворяет полным требованиям к безопасности, выраженным в виде полных требований к функциям безопасности и полноте безопасности, с учетом требований к распределению требований безопасности по E/E/PE системам, связанным с безопасностью, разработанным в соответствии с 7.6.

7.14.2 Требования

7.14.2.1 Действия по подтверждению соответствия должны выполняться в соответствии с планом полного подтверждения соответствия безопасности E/E/PE систем, связанных с безопасностью.

7.14.2.2 Все оборудование, используемое для количественных измерений, используемое при действиях по подтверждению соответствия, должно быть калибровано в соответствии с требованиями национального стандарта или спецификаций поставщика.

7.14.2.3 Информация, подлежащая документированию в период подтверждения соответствия, должна включать в себя:

- документацию в хронологической форме по действиям в период подтверждения соответствия;
- использовавшуюся версию полных требований к безопасности;
- функции безопасности, подтверждение соответствия которых осуществлялось (с использованием тестирования или анализа);

- используемые инструменты и оборудование, а также данные калибровки;
- результаты действий по подтверждению соответствия;
- конфигурацию проверяемого компонента, применявшиеся процедуры и условия испытаний;
- расхождения между ожидаемыми и фактическими результатами.

7.14.2.4 В случае расхождения между ожидаемыми и фактическими результатами, проводится анализ и принимается решение о продолжении действий по подтверждению соответствия или о направлении запроса на внесение изменений и возврате к более ранней стадии подтверждения соответствия; это решение должно быть документировано.

7.15 Эксплуатация, обслуживание и ремонт

Примечания

1 Эта стадия представлена на рисунке 2 прямоугольником 14.

2 Организационные мероприятия, рассматриваемые в настоящем подразделе, осуществляются для эффективного выполнения технических требований и предназначены исключительно для достижения и поддержания функциональной безопасности E/E/PE систем, связанных с безопасностью. Технические требования, необходимые для поддержания функциональной безопасности, обычно определяются как часть информации, предоставляемой поставщиком E/E/PE систем, связанных с безопасностью.

3 Требования к функциональной безопасности при обслуживании и ремонте могут отличаться от требований, относящихся к эксплуатации.

4 Не следует считать, что процедуры проверки, разработанные для первоначальной установки и ввода в действие, могут быть использованы без проверки их обоснованности и практической целесообразности в процессе эксплуатации EUC.

7.15.1 Цель

Цель требований настоящего подраздела состоит в осуществлении эксплуатации, обслуживания и ремонта E/E/PE систем, связанных с безопасностью, таким образом, чтобы поддерживалась требуемая функциональная безопасность.

7.15.2 Требования

7.15.2.1 Должно быть реализовано следующее:

- план обслуживания E/E/PE систем, связанных с безопасностью;
- процедуры, связанные с эксплуатацией, обслуживанием и ремонтом E/E/PE систем, связанных с безопасностью (МЭК 61508-2);
- процедуры, связанные с эксплуатацией и сопровождением программного обеспечения (МЭК 61508-3).

7.15.2.2 Реализация положений, указанных в 7.15.2.1, должна включать:

- реализацию процедур;
- следование графику обслуживания;
- поддержание документации;
- периодическое проведение аудита функциональной безопасности [см. п. 6.2.1, перечисление k)];
- документирование модификаций E/E/PE систем, связанных с безопасностью.

Примечания

1 Пример модели действий по эксплуатации и обслуживанию показан на рисунке 7.

2 Пример модели управления эксплуатацией и обслуживанием показан на рисунке 8.

7.15.2.3 Необходимо вести документирование в хронологическом порядке действий по эксплуатации, ремонту и обслуживанию E/E/PE систем, связанных с безопасностью; документация должна содержать следующую информацию:

- результаты аудитов и тестирования функциональной безопасности;
- время и причины запросов к E/E/PE системам, связанным с безопасностью (при эксплуатации), а также характеристики E/E/PE систем, связанных с безопасностью, при обработке этих запросов и отказов, обнаруженных при обычном обслуживании;
- документацию по модификации EUC, систем управления EUC и E/E/PE систем, связанных с безопасностью.

7.15.2.4 Точные требования к хронологической документации зависят от конкретной области применения и должны быть, где это важно, более детально описаны в стандартах этой области применения.

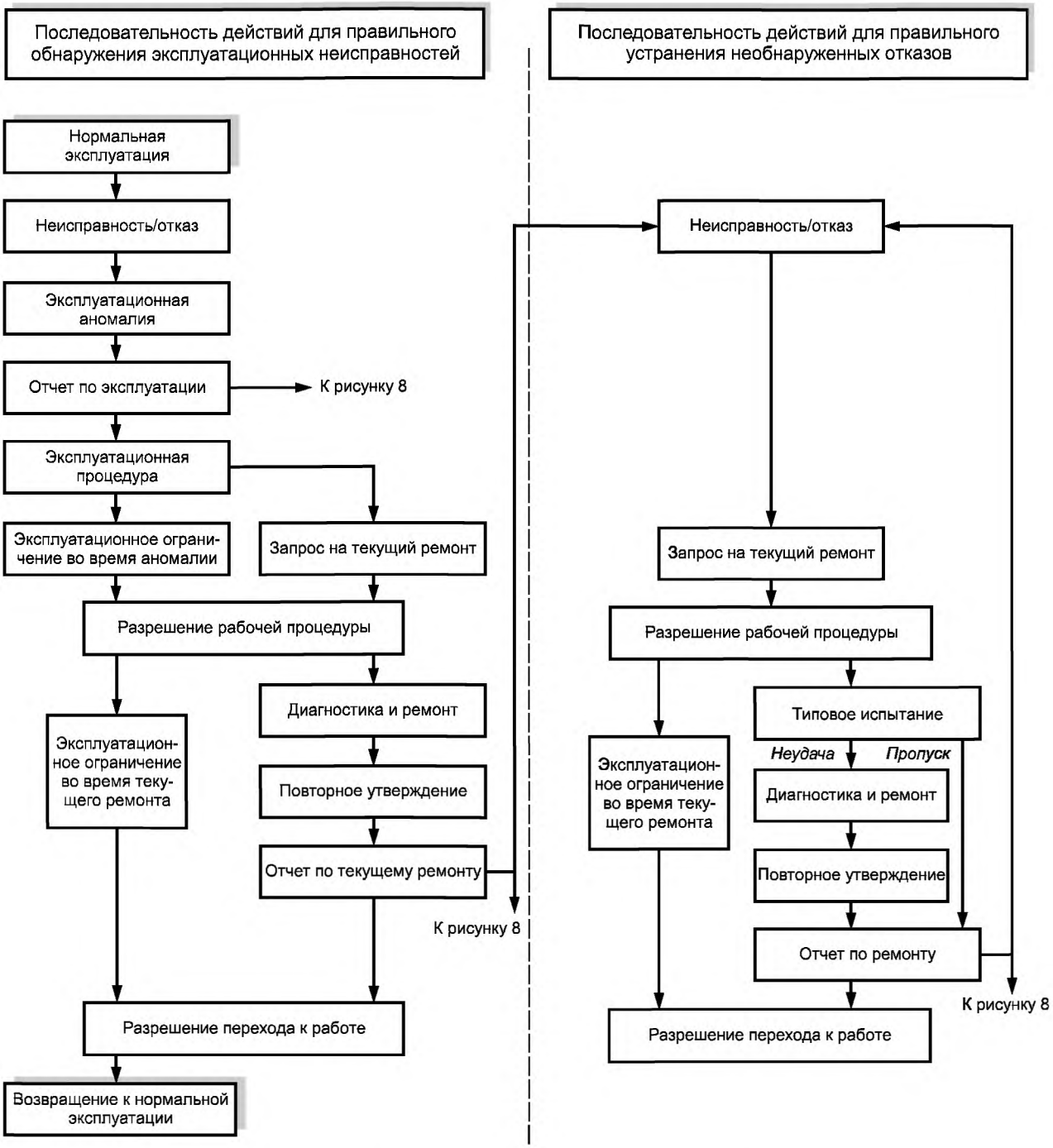


Рисунок 7 — Пример модели действий при эксплуатации и обслуживании

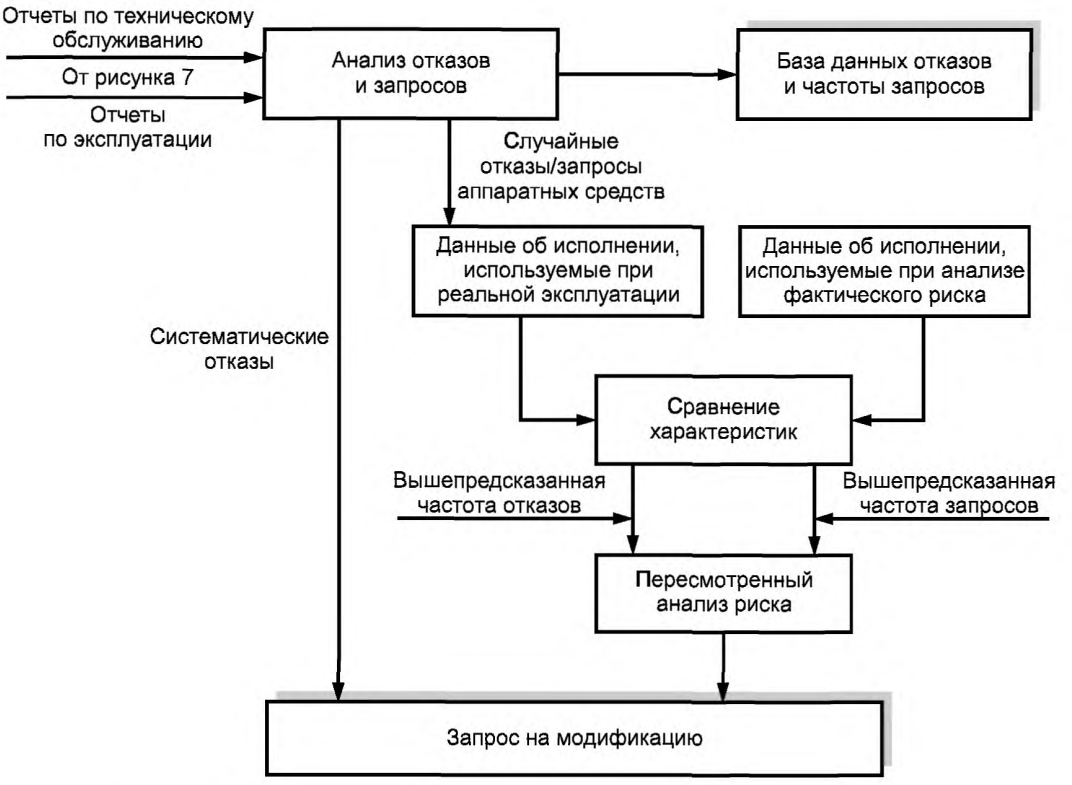


Рисунок 8 — Пример модели управления эксплуатацией и обслуживанием

7.16 Модификация и изменение

Примечания

1 Данная стадия соответствует прямоугольнику 15 на рисунке 2.

2 Организационные мероприятия, рассмотренные в настоящем подразделе, обеспечивают выполнение технических требований и предназначены для достижения и поддержания функциональной безопасности E/E/PE систем, связанных с безопасностью. Технические требования, необходимые для поддержания функциональной безопасности, обычно определяются как часть информации, предоставляемой поставщиком E/E/PE систем, связанных с безопасностью.

7.16.1 Цель

Цель требований настоящего подраздела состоит в том, чтобы гарантировать, что функциональная безопасность E/E/PE систем, связанных с безопасностью, соответствует планируемой безопасности как в период, так и после стадии модификации и изменения.

7.16.2 Требования

7.16.2.1 Перед выполнением любых модификаций или изменений должно быть проведено планирование соответствующих процедур (см. 6.2.1).

Примечание — Пример модели процедуры модификации показан на рисунке 9.

7.16.2.2 Стадия модификации и изменения должна инициироваться только путем внесения утвержденного запроса в рамках процедур управления функциональной безопасностью (см. раздел 6). В запросе должны быть детализированы:

- установленные опасности, которые могут быть вызваны модификацией;
- предложенные изменения (в аппаратных средствах и программном обеспечении);
- причины для внесения изменений.

Примечание — Причинами для появления запроса на модификацию могут быть, например:

- функциональная безопасность, оказавшаяся ниже заданной;
- систематические отказы;

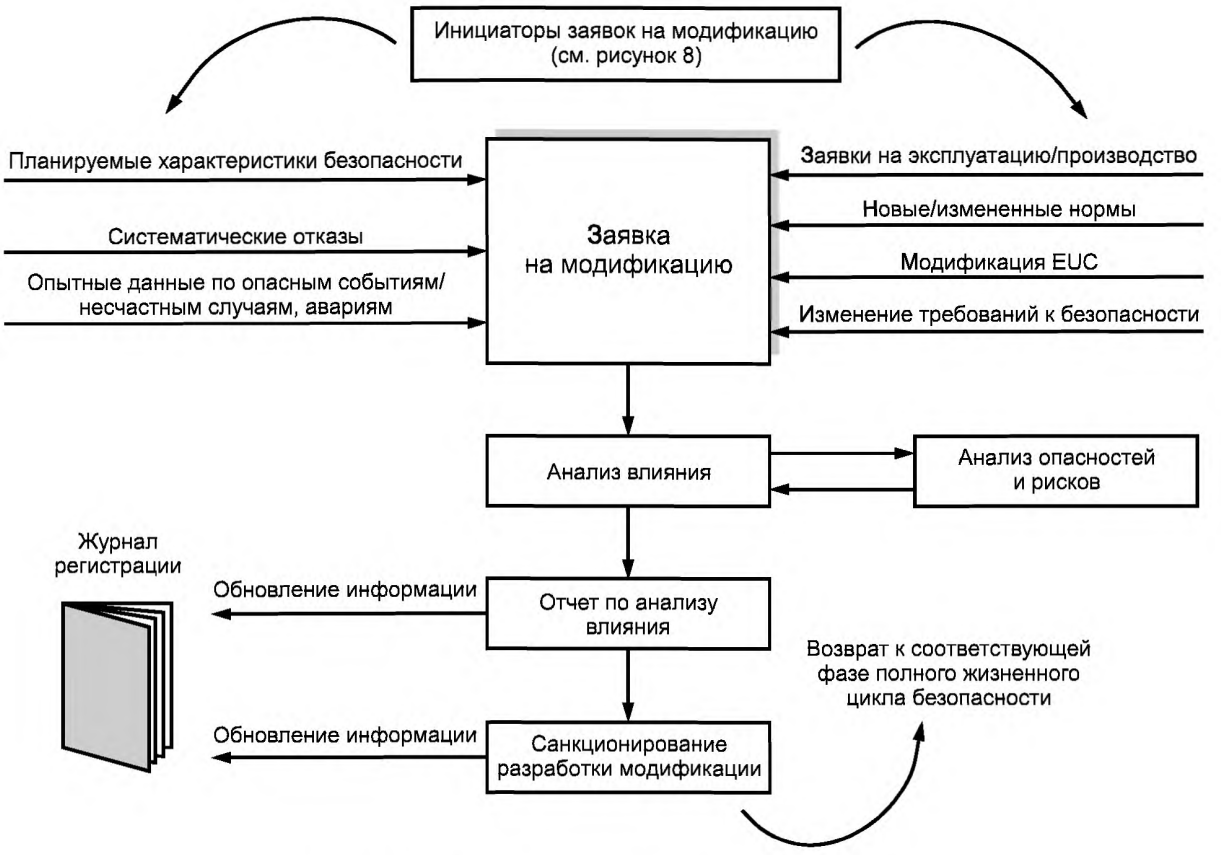


Рисунок 9 — Пример модели процедуры модификации

- новое или измененное законодательство в области безопасности;
- модификации EUC или способа его использования;
- модификации полных требований к безопасности;
- анализ эксплуатационных характеристик работы и характеристик обслуживания, показавший, что эти характеристики оказались ниже запланированных;
- обычный аудит функциональной безопасности.

7.16.2.3 Должен быть выполнен анализ влияния, включающий оценку влияния предлагаемых изменений на функциональную безопасность каждой E/E/PE системы, связанной с безопасностью. Оценка должна включать анализ опасностей и рисков, достаточный для того, чтобы определить степень охвата и глубину последующих стадий полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения, которые должны быть выполнены. При оценке необходимо учитывать влияние действий по другим одновременно проводимым модификациям или изменениям и рассматривать состояние функциональной безопасности до и после проведения модификации и внесения изменений.

7.16.2.4 Результаты анализа влияния, описанные в 7.16.2.3, должны быть документированы.

7.16.2.5 Разрешение на проведение требуемой модификации или внесения изменений должно зависеть от результатов анализа влияния.

7.16.2.6 Все модификации, оказывающие влияние на функциональную безопасность любой E/E/PE системы, связанной с безопасностью, должны приводить к возврату к соответствующей стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения. Все последующие стадии должны осуществляться в соответствии с процедурами, определенными для этих стадий согласно требованиям настоящего стандарта.

Примечания

1 Может потребоваться провести полный анализ опасностей и рисков, который может вызвать необходимость установления уровней полноты безопасности, которые отличаются от имеющихся установленных уровней полноты безопасности для E/E/PE систем, связанных с безопасностью.

2 Не допускается, чтобы процедуры тестирования, разработанные для первоначальной установки и пуска в эксплуатацию, использовались без проверки подтверждения их соответствия и практической целесообразности в контексте нормальной работы EUC.

7.16.2.7 Должна быть создана документация и в дальнейшем поддержана в хронологическом порядке, которая должна содержать подробное описание всех действий по модификации и внесению изменений и включать:

- запросы на проведение модификаций и внесение изменений;
- анализ влияния;
- повторное подтверждение соответствия и повторную верификацию данных и результатов;
- все документы, затрагиваемые процессами модификации и изменения.

7.17 Вывод из эксплуатации или ликвидация

Примечание — Эта стадия представлена прямоугольником 16 на рисунке 2.

7.17.1 Цель

Целью требований настоящего подраздела стандарта является обеспечение того, чтобы функциональная безопасность E/E/PE систем, связанных с безопасностью, соответствовала обстоятельствам в течение и после действий по выводу из эксплуатации или ликвидации EUC.

7.17.2 Требования

7.17.2.1 Перед выводом из эксплуатации или утилизацией необходимо выполнить анализ влияния предлагаемых действий по выводу из эксплуатации или утилизации на функциональную безопасность каждой E/E/PE системы, связанной с безопасностью, имеющей отношение к EUC и к смежным EUC. Оценка должна включать анализы опасностей и рисков, достаточные для определения необходимой широты и глубины охвата последующих стадий полного жизненного цикла безопасности, жизненного цикла безопасности E/E/PES или программного обеспечения.

7.17.2.2 Результаты требований, описанные в 7.17.2.1, должны быть документированы.

7.17.2.3 Стадия вывода из эксплуатации или ликвидации должна инициироваться выпуском авторизованного запроса в рамках процедур по управлению функциональной безопасностью (см. раздел 6).

7.17.2.4 Разрешение на проведение требуемого вывода из эксплуатации или ликвидации должно зависеть от результатов анализа влияния.

7.17.2.5 Перед выводом из эксплуатации или ликвидацией должен быть подготовлен план по:

- прекращению работы E/E/PE систем, связанных с безопасностью;
- демонтажу E/E/PE систем, связанных с безопасностью.

7.17.2.6 Если какие-либо действия по выводу из эксплуатации или ликвидации оказывают влияние на функциональную безопасность любой из E/E/PE систем, связанных с безопасностью, то должен быть инициирован возврат к соответствующей стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения. Все последующие стадии должны быть выполнены в соответствии с процедурами, определенными в настоящем стандарте для заданных уровней полноты безопасности E/E/PE систем, связанных с безопасностью.

Примечания

1 Может возникнуть необходимость в проведении полного анализа опасностей и рисков, результатом которого может явиться необходимость установления другого уровня полноты безопасности для E/E/PE систем, связанных с безопасностью.

2 Требования к функциональной безопасности на стадии вывода из эксплуатации или ликвидации могут отличаться от требований, которые используются на стадии эксплуатации.

7.17.2.7 Должна быть создана документация и в дальнейшем поддержана в хронологическом порядке, которая должна содержать подробное описание всех действий по выводу из эксплуатации или ликвидации и должна включать:

- план, используемый для выполнения действий по выводу из эксплуатации или ликвидации;
- анализ влияния.

7.18 Верификация

7.18.1 Цель

Цель требований настоящего подраздела состоит в демонстрации для каждой стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения (путем проверки, анализа и/или тестирования) того, что выходные материалы отвечают всем соответствующим целям и требованиям, определенным для этой стадии.

7.18.2 Требования

7.18.2.1 Для каждой стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения одновременно с разработкой плана этой стадии должен быть установлен план верификации.

7.18.2.2 В плане верификации должны содержаться критерии, методы и средства, используемые при верификации, или даны ссылки на них.

7.18.2.3 Верификацию следует выполнять согласно плану верификации.

Примечание — Выбор методов и мер для выполнения верификации, а также степень независимости процессов верификации зависят от ряда факторов и могут быть определены в стандартах для областей применения. В число этих факторов могут входить, например:

- размер проекта;
- степень сложности;
- степень новизны проекта;
- степень новизны технологии.

7.18.2.4 Информацию по верификации следует собирать и документировать для того, чтобы засвидетельствовать, что она завершена удовлетворительно во всех отношениях.

8 Оценка функциональной безопасности

8.1 Цель

Целью требований настоящего раздела является изучение и вынесение решения по функциональной безопасности, достигнутой E/E/PE системой, связанной с безопасностью.

8.2 Требования

8.2.1 Для осуществления оценки функциональной безопасности должны быть назначены один или несколько человек, которые должны прийти к заключению относительно функциональной безопасности, достигаемой E/E/PE системами, связанными с безопасностью.

8.2.2 Те, кто выполняет оценку функциональной безопасности, должны иметь доступ ко всем лицам, вовлеченным в любые действия в полном жизненном цикле безопасности, жизненных циклах безопасности E/E/PES или программного обеспечения, а также ко всей информации и оборудованию (включая аппаратные средства и программное обеспечение).

8.2.3 Оценку функциональной безопасности следует применять ко всем этапам на протяжении всего полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения. Те лица, которые осуществляют оценку функциональной безопасности, должны рассмотреть все действия, а также все выходные материалы, полученные в течение каждой стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения, и дать заключение о том, в какой степени выполнены цели и требования настоящего стандарта.

8.2.4 Оценка функциональной безопасности должна выполняться до возникновения выявленных опасностей на протяжении полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения. Ее можно проводить после каждой стадии жизненного цикла безопасности или после нескольких стадий.

8.2.5 Если какие-либо средства используются в качестве составной части при разработке или оценке полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES или программного обеспечения, то они сами должны быть объектом оценки функциональной безопасности.

Примечания

1 Примером средств являются планируемые для работы системы CAD/CAM, компиляторы и компьютеры.

2 Степень использования таких средств должна быть оценена в зависимости от их влияния на функциональную безопасность E/E/PE систем, связанных с безопасностью.

8.2.6 При оценке функциональной безопасности необходимо учитывать следующее:

- работы, выполненные со времени предыдущей оценки функциональной безопасности (которая обычно охватывает предыдущие стадии жизненных циклов безопасности);
- планы или стратегия реализации последующих оценок функциональной безопасности для полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения;
- рекомендации предыдущих оценок функциональной безопасности и объем внесенных изменений.

8.2.7 Действия по оценке функциональной безопасности для различных стадий полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения должны быть согласованными и запланированными.

8.2.8 План оценки функциональной безопасности должен определять:

- лиц, осуществляющих оценку функциональной безопасности;
- выходные материалы при каждой оценке функциональной безопасности;
- границы оценки функциональной безопасности.

Примечание — При установлении границ оценки функциональной безопасности необходимо определить документы, используемые в качестве входных материалов для каждого действия, связанного с оценкой функциональной безопасности, и статус этих документов.

- привлекаемые органы по безопасности;
- требуемые ресурсы;
- уровень независимости выполняющих оценку функциональной безопасности;
- компетентность выполняющих оценку функциональной безопасности в соответствующей области применения.

8.2.9 Перед выполнением оценки функциональной безопасности ее план должен быть утвержден теми, кто будет выполнять эту оценку, и теми, кто несет ответственность за управление функциональной безопасностью на оцениваемой стадии жизненного цикла систем безопасности.

8.2.10 В заключении об оценке функциональной безопасности должны быть выработаны рекомендации по ее принятию, условному принятию или отклонению.

8.2.11 Лица, которые осуществляют оценку функциональной безопасности, должны быть компетентными в выполняемых действиях, а также должны быть учтены факторы, определяющие компетентность (см. приложении В).

8.2.12 Если иное не установлено в стандартах для областей применения, то минимальный уровень независимости выполняющих оценку функциональной безопасности должен соответствовать тому уровню, который указан в таблицах 4 и 5.

В таблицах 4 и 5 приведены следующие рекомендации:

- HR: уровень независимости, определенный как настоятельно рекомендуемый в качестве минимального для указанных последствий (см. таблицу 4) или уровня полноты безопасности (см. таблицу 5). Если принят более низкий уровень независимости, то должно быть приведено подробное обоснование, почему не был использован уровень HR;
- NR: уровень независимости, определенный как недостаточный и явно не рекомендованный для указанных последствий (см. таблицу 4) или уровня полноты безопасности (см. таблицу 5). Если принимается данный уровень независимости, то должно быть приведено подробное обоснование причин его использования;
- -: уровень независимости, определенный как уровень, для которого отсутствуют рекомендации за или против его использования.

Примечания

1 Перед применением данных таблицы 4 необходимо определить категории последствий с учетом практики, сложившейся в области применения. К числу последствий относятся те последствия, которые возникают в результате отказа, требующего вмешательства E/E/PE систем, связанных с безопасностью.

2 В зависимости от организационной структуры компании и опыта внутри компании требования по независимости лиц и подразделений могут быть выполнены путем использования услуг сторонней организации. В свою очередь компании, которые имеют внутренние структуры с опытом в оценке рисков и применении систем, связанных с безопасностью, и которые независимы и отделены (путем управления и использованием других ресурсов) от тех, которые несут ответственность за основную разработку, могут оказаться способными использовать свои собственные ресурсы для выполнения требований по независимости организации.

3 Определения понятий независимого лица, независимого подразделения и независимой организации см. в МЭК 61508-4, пункты 3.8.10, 3.8.11 и 3.8.12 соответственно.

8.2.13 В контексте таблиц 4 и 5 используется уровень независимости либо HR^1, либо HR^2 (но не оба вместе) в зависимости от числа факторов, которое характерно для области применения. Если применяется уровень независимости HR^1, то уровень HR^2 должен читаться как не требующийся; если используется уровень HR^2, то уровень HR^1 должен читаться как NR (нерекомендуемый). В отсутствие стандарта в области применения должно быть приведено подробное обоснование выбора уровня HR^1 или HR^2. К числу

факторов, которые способствуют тому, чтобы сделать уровень HR^2 более подходящим, чем уровень HR^1, относятся следующие факторы:

- недостаток опыта в работе со схожими проектами;
- более высокая степень сложности;
- высокая степень новизны разработки;
- более высокая степень новизны технологии;
- недостаточная степень стандартизации особенностей проекта.

8.2.14 Минимальный уровень независимости (см. таблицу 5) должен основываться на функции безопасности, выполняемой E/E/PE системой, связанной с безопасностью, имеющей наивысший уровень полноты безопасности.

Таблица 4 — Минимальные уровни независимости для выполняющих оценку функциональной безопасности (стадии полного жизненного цикла безопасности 1 — 8 и 12 — 16 включительно (см. рисунок 2))

Минимальный уровень независимости	Последствие (см. примечание 2)			
	A	B	C	D
Независимое лицо	HR	HR^1	NR	NR
Независимое подразделение	- -	HR^2	HR^1	NR
Независимая организация	- -	- -	HR^2	HR

Примечания

1 Подробное описание интерпретации настоящей таблицы см. в 8.2.12 (включая примечания) и в 8.2.13.

2 К числу типичных последствий относятся: последствие A — небольшая травма (например, временное нарушение функции); последствие B — серьезная постоянная травма у одного или нескольких человек, смерть одного человека; последствие C — смерть нескольких человек; последствие D — смерть очень многих людей.

Таблица 5 — Минимальные уровни независимости для выполняющих оценку функциональной безопасности (стадия 9 полного жизненного цикла безопасности, включая все стадии жизненных циклов безопасности E/E/PES и программного обеспечения (см. рисунки 2 — 4))

Минимальный уровень независимости	Уровень полноты безопасности			
	A	B	C	D
Независимое лицо	HR	HR^1	NR	NR
Независимое подразделение	- -	HR^2	HR^1	NR
Независимая организация	- -	- -	HR^2	HR

Примечание — Подробное описание настоящей таблицы см. в 8.2.12 (включая примечания), 8.2.13 и 8.2.14.

Приложение А
(справочное)

Пример структуры документации

А.1 Общие положения

В настоящем приложении приведен пример структуры документации и метод формирования документов, необходимых для структурирования информации в соответствии с требованиями раздела 5. Документация должна содержать информацию, достаточную для эффективного выполнения:

- каждой стадии полного жизненного цикла безопасности, жизненных циклов безопасности E/E/PES и программного обеспечения;
- управления функциональной безопасностью (раздел 6);
- оценки функциональной безопасности (раздел 8).

Понятие достаточности информации зависит от ряда факторов, включая сложность и размер E/E/PE систем, связанных с безопасностью, и требования, относящиеся к конкретной области применения. Необходимая документация может быть определена в стандарте для соответствующей области применения.

Объем информации в каждом документе может изменяться от нескольких строк до многих страниц, полный набор информации может быть разделен между несколькими физическими документами либо может быть представлен одним документом. Физическая структура документации зависит от размера и сложности E/E/PE систем, связанных с безопасностью, и должна учитывать практику, сложившуюся в компании и в конкретной области применения.

Пример структуры документации, приведенный в настоящем приложении, предназначен для того, чтобы проиллюстрировать один конкретный способ структурирования документации и один из способов наименования документов. Более подробную информацию см. в [4].

Документ представляет собой структурированный набор информации, предназначенный для восприятия человеком, пригодный для использования в качестве единицы обмена между пользователями и/или системами [5]. Данный термин применим, следовательно, не только к документам в традиционном смысле, но также и к таким понятиям, как файл данных или информация, хранящаяся в базе данных.

В настоящем стандарте термин документ скорее относится к информации, чем к физическим документам, если только иное не оговорено специально или не может быть понято в контексте раздела или подраздела, в котором используется этот термин. Документ может быть доступен для восприятия человеком в разных формах (например, на бумаге, пленке или ином носителе информации, допускающем ее представление на экране дисплея).

Пример структуры документа, приводимый в настоящем приложении, специфицирует документы в двух отношениях:

- тип документа;
- процесс или объект.

Тип документа определен в соответствии с [3]; он характеризует содержание документа, например описание функций или принципиальную схему соединений. Процессы или объекты описывают собственно предметную область, например схему управления насосом.

Основными документами, определяемыми в настоящем приложении, являются:

- спецификация — определяет необходимую функцию, характеристику или процесс (например, спецификация требований);
- описание — определяет планируемую или реальную функцию, устройство, характеристику или процесс (например, описание функции);
- инструкция — содержит подробные указания о том, когда и как следует выполнять определенные действия (например, инструкция для оператора);
- план — содержит план того, когда, как и кем будут выполняться определенные действия (например, план обслуживания);
- диаграмма — определяет функции с помощью диаграмм (символов и линий), представляющих сигналы, циркулирующие между символами;
- список — представляет информацию в виде списка (например, список кодов, список сигналов);
- журнал — представляет информацию о событиях в хронологической форме;
- отчет — описывает результаты процессов, таких, как исследования, оценки, испытания и т.п. (например, отчет об испытаниях);
- запрос — представляет описание запрашиваемых действий, которые должны быть подтверждены и затем специфицированы (например, запрос на обслуживание).

Основной тип документа может иметь аффикс, например спецификация требований или спецификация испытаний, уточняющий содержание.

А.2 Структура документов, относящихся к жизненному циклу безопасности

Таблицы А.1 — А.3 содержат пример структуры документации, предназначенной для структурирования информации с целью выполнения требований, указанных в разделе 5. Таблицы указывают стадии жизненного цикла безопасности, которые преимущественно связаны с документами (обычно это стадии, в течение которых они разрабатывались). Названия документов — в соответствии с А.1.

В дополнение к документам, перечисленным в таблицах А.1 — А.3, могут существовать дополнительные документы, предоставляющие дополнительную детализирующую информацию или информацию, структурированную для специальных целей, например списки запасных частей, списки сигналов, списки кабелей, диаграммы циклов, списки переменных.

Примечание — Примерами таких переменных являются значения для регуляторов, граничные допустимые значения для переменных, приоритеты выполнения заданий на компьютере. Некоторые значения переменных могут быть предоставлены до поставки системы, другие могут быть предоставлены во время ввода в эксплуатацию или во время обслуживания.

Таблица А.1 — Пример структуры информации, относящейся к жизненному циклу систем безопасности в целом

Фаза жизненного цикла систем безопасности в целом	Информация
Концепция	Описание (полная концепция)
Определение общей области применения	Описание (определение полной области применения)
Анализ опасностей и рисков	Описание (анализ опасностей и рисков)
Полные требования к безопасности	Спецификация (полные требования к безопасности, включая: полные требования к функциям безопасности и полные требования к полноте безопасности)
Распределение требований к безопасности	Описание (распределение требований к безопасности)
Полное планирование эксплуатации и обслуживания	План (полная эксплуатация и обслуживание)
Полное планирование подтверждения соответствия безопасности	План (полное подтверждение соответствия безопасности)
Планирование полной установки и ввода в эксплуатацию	План (полная установка) План (полный ввод в эксплуатацию)
Реализация	Реализация E/E/PE систем, связанных с безопасностью (см. МЭК 61508-2 и МЭК 61508-3)
Полная установка и ввод в эксплуатацию	Отчет (полная установка) Отчет (полный ввод в эксплуатацию)
Полное подтверждение соответствия безопасности	Отчет (полное подтверждение соответствия безопасности)
Полная эксплуатация и обслуживание	Журнал (полная эксплуатация и обслуживание)
Полная модификация и изменения	Запрос (полная модификация) Отчет (анализ влияния полной модификации и изменений) Журнал (модификация и изменения)
Вывод из эксплуатации и ликвидация	Отчет (анализ влияния вывода из эксплуатации или ликвидации); план (вывод из эксплуатации или ликвидация); журнал (вывод из эксплуатации или ликвидация)
Относится ко всем стадиям	План (безопасность); план (верификация); отчет (верификация); план (оценка функциональной безопасности); отчет (оценка функциональной безопасности)

Таблица А.2 — Пример структуры документации для информации, относящейся к жизненному циклу безопасности E/E/PES

Стадия жизненного цикла E/E/PES	Информация
Требования к безопасности E/E/PES	Спецификация (требования к безопасности E/E/PES, включая: требования к функциям безопасности E/E/PES и полноте безопасности E/E/PES)
Планирование подтверждения соответствия E/E/PES	План (подтверждение соответствия безопасности E/E/PES)
Проектирование и создание E/E/PES Архитектура E/E/PES Архитектура аппаратных средств Разработка аппаратных модулей Конструирование и/или приобретение компонентов	Описание (проект архитектуры E/E/PES, включая: архитектуру аппаратных средств и архитектуру программного обеспечения); спецификация (комплексные испытания программируемой электроники); спецификация (комплексные испытания программируемых электронных и непрограммируемых электронных устройств); описание (проект архитектуры аппаратных средств); спецификация (тесты интегральной архитектуры аппаратных средств); спецификация (проект аппаратных модулей); спецификации (испытания аппаратных модулей); аппаратные модули; отчет (проверка аппаратных модулей)
Интеграция программируемой электроники	Отчет (комплексные испытания программмируемой электроники и программного обеспечения) (см. таблицу А.3)
Интеграция E/E/PES	Отчет (комплексные испытания программируемой электроники и других аппаратных средств)
Процедуры эксплуатации и обслуживания E/E/PES	Инструкция (пользователя) Инструкция (эксплуатация и обслуживание)
Подтверждение соответствия безопасности E/E/PES	Отчет (подтверждение соответствия безопасности E/E/PES)
Модификация E/E/PES	Инструкция (процедуры модификации E/E/PES); запрос (модификация E/E/PES); отчет (анализ влияния модификации E/E/PES); журнал (модификация E/E/PES)
Относится ко всем фазам	План (безопасность E/E/PES); план (верификация безопасности E/E/PES); отчет (верификация безопасности E/E/PES); план (оценка функциональной безопасности E/E/PES); отчет (оценка функциональной безопасности E/E/PES)

Таблица А.3 — Пример структуры документации, относящейся к жизненному циклу безопасности программного обеспечения

Фаза жизненного цикла программного обеспечения	Информация
Требования к безопасности программного обеспечения	Спецификация (требования к безопасности программного обеспечения, включая требования: к функциям безопасности и полноте безопасности программного обеспечения)
Планирование подтверждения соответствия программного обеспечения	План (подтверждение соответствия безопасности программного обеспечения)
Проектирование и создание программного обеспечения Архитектура программного обеспечения	Описание (проект архитектуры программного обеспечения) (описание проекта архитектуры аппаратных средств см. в таблице А.2); спецификация (комплексные

Окончание таблицы А.3

Фаза жизненного цикла программного обеспечения	Информация
Разработка системы программного обеспечения Разработка программных модулей Кодирование Тестирование программных модулей Интеграция программного обеспечения	испытания программного обеспечения архитектуры); спецификация (комплексные испытания программируемой электроники и программного обеспечения); инструкция (средства разработки и руководство по кодированию); описание (проект системы программного обеспечения); спецификация (комплексные испытания системы программного обеспечения); спецификация (проект программных модулей); спецификация (испытания программных модулей); список (исходный код); отчет (испытания программных модулей); отчет (просмотр кода); отчет (испытания программных модулей); отчет (комплексные испытания программных модулей); отчет (комплексные испытания программного обеспечения системы); отчет (комплексные испытания программного обеспечения архитектуры)
Интеграция программируемой электроники	Отчет (комплексные испытания программируемой электроники и программного обеспечения)
Процедуры эксплуатации и сопровождения программного обеспечения	Инструкция (пользователя) Инструкция (по эксплуатации и обслуживанию)
Подтверждение соответствия безопасности программного обеспечения	Отчет (подтверждение соответствия безопасности программного обеспечения)
Модификация программного обеспечения	Инструкция (процедуры модификации программного обеспечения); отчет (модификация программного обеспечения); отчет (анализ влияния модификации программного обеспечения); журнал (модификация программного обеспечения)
Относится ко всем фазам	План (безопасность программного обеспечения); план (верификация программного обеспечения); отчет (верификация программного обеспечения); план (оценка функциональной безопасности программного обеспечения); отчет (оценка функциональной безопасности программного обеспечения)

А.3 Физическая структура документа

Физическая структура документации представляет собой способ, которым различные документы объединяются в документы, комплекты документов, книги и группы книг. На рисунке А.1 показаны примеры таких групп книг, структурированных в соответствии с группами пользователей. Один и тот же документ может входить в разные комплекты.

Для больших и сложных систем многие физические документы, по-видимому, должны быть объединены в несколько книг. Для небольшой системы, имеющей невысокую сложность и ограниченное число физических документов, вся документация может быть объединена в одну книгу, с закладками для различных комплектов документов (см. рисунок А.2).

Физическая структура представляет средство для выбора документации, необходимой для специфических действий отдельных лиц или групп лиц, выполняющих эти действия.

Следовательно, некоторые из физических документов могут присутствовать в нескольких книгах, комплектах книг или другом носителе (например, на компьютерных дисках).

Примечание — Информация, необходимая для документов, указанных в таблице А.1, может содержаться в нескольких различных комплектах документов, показанных на рисунках А.1 и А.2. Например, в инженерном комплекте могут содержаться такие документы, как описание анализа опасностей и рисков и/или спецификация полных требований к безопасности.

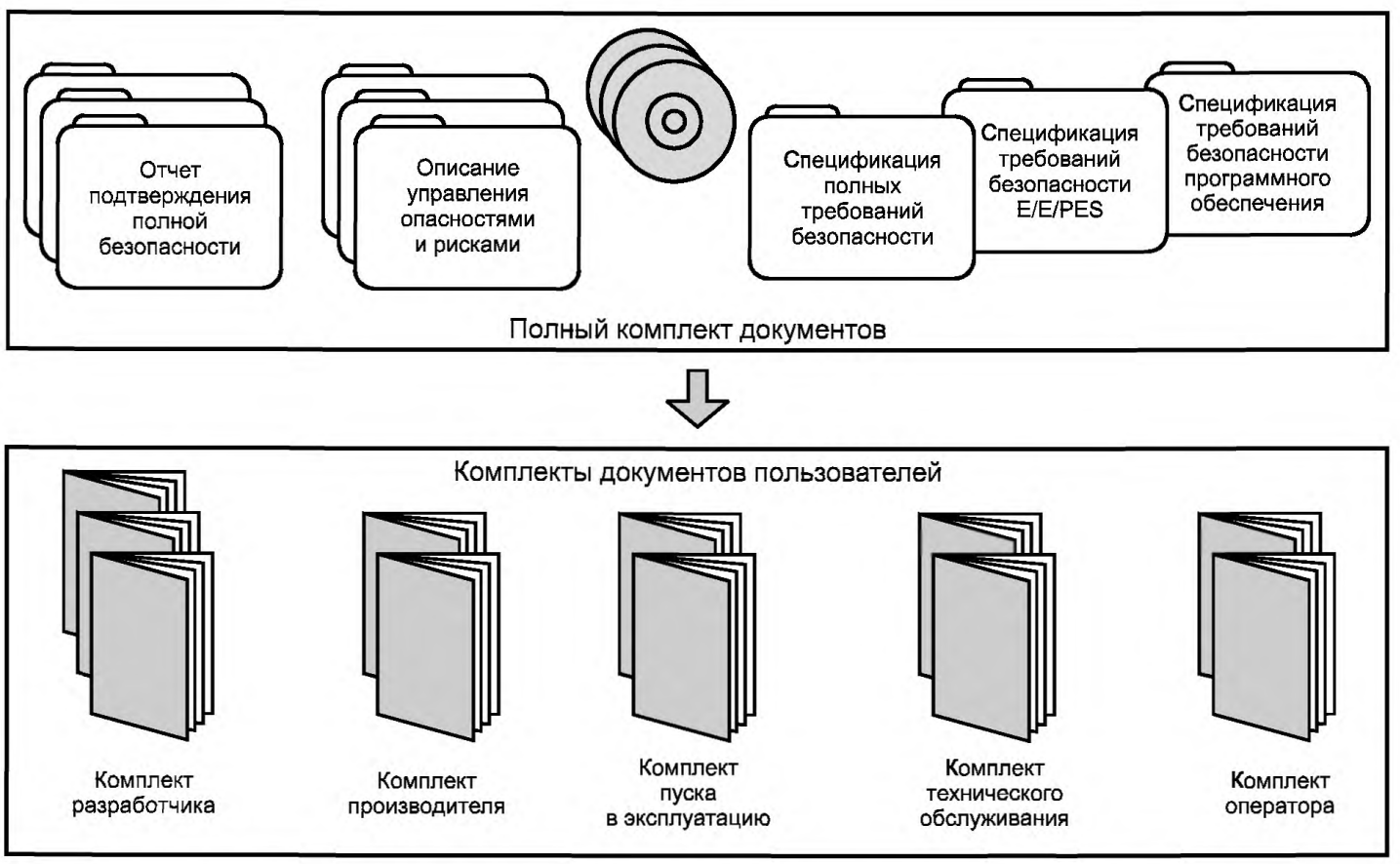


Рисунок А.1 — Структурирование информации в наборы документов для групп пользователей

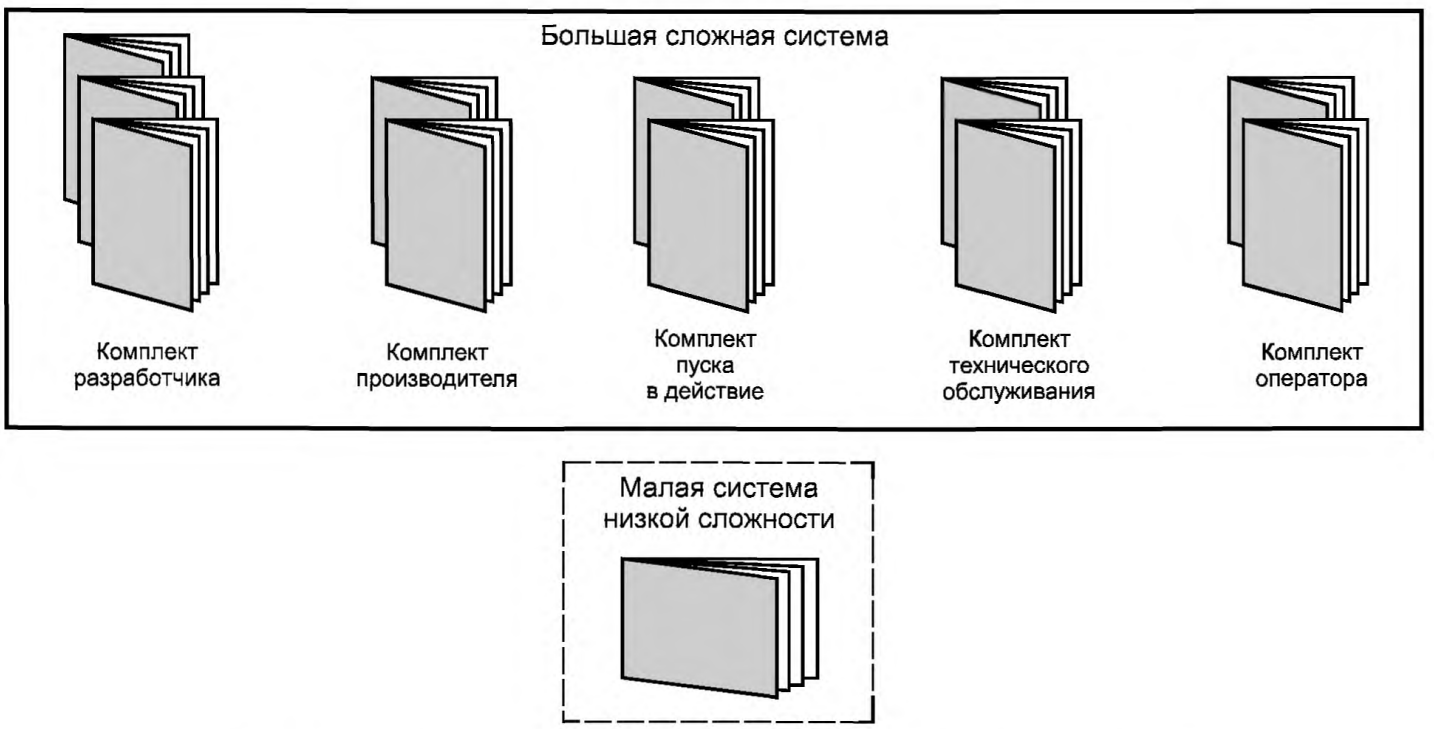


Рисунок А.2 — Структурирование информации для больших сложных систем и для небольших систем малой сложности

А.4 Список документов

Список документов обычно содержит следующую информацию:

- номер чертежа или документа;
- номер изменения;
- код обозначения документа;

- заголовок;
- дату изменения;
- тип носителя информации.

Этот список может быть реализован в различных формах, например, в виде базы данных, в которой имеется возможность сортировки в соответствии с номером документа или чертежа, или в соответствии с кодом документа. Код документа может содержать ссылочное обозначение для функции, местоположения или продукции, описываемой в документе, представляя собой мощный инструмент для поиска информации.

Приложение В
(справочное)

Компетентность лиц

В.1 Цель

В настоящем приложении кратко рассмотрено, как гарантировать, чтобы лица, которые несут ответственность за любые действия, связанные с полным жизненным циклом безопасности, жизненными циклами безопасности E/E/PES или программного обеспечения, являлись компетентными для выполнения этих обязанностей.

В.2 Общие положения

Все лица, вовлеченные в любые действия, связанные с полным жизненным циклом безопасности, жизненным циклом безопасности E/E/PES или программного обеспечения, включая действия по управлению, должны иметь соответствующую подготовку (тренинг), технические знания, опыт и квалификацию, соответствующие служебным обязанностям, которые они должны выполнять.

Подготовка, опыт и квалификация всех лиц, участвующих в каких-либо действиях, связанных с полным жизненным циклом безопасности, жизненным циклом безопасности E/E/PES или программного обеспечения, включая управление действиями по функциональной безопасности, должны быть оценены по отношению к конкретному применению.

При оценке компетентности лиц в выполнении своих обязанностей необходимо принимать во внимание следующее:

a) инженерные знания, соответствующие данной области применения;

b) инженерные знания, соответствующие технологии (например, электрической, электронной, программируемой электроники, разработки программного обеспечения);

c) инженерные знания в области безопасности, соответствующие данной технологии;

d) знание основ правового и технического регулирования в области безопасности;

e) последствия в случае отказов E/E/PE систем, связанных с безопасностью; чем серьезнее последствия, тем более строгими должны быть спецификация и оценка компетентности;

f) уровни полноты безопасности E/E/PE систем, связанных с безопасностью; чем выше уровень полноты безопасности, тем более строгими должны быть спецификация и оценка компетентности;

g) новизна разработки, процедур разработки или применения; чем более новые и непроверенные разработки, процедуры разработки или применения, тем более строгими должны быть спецификация и оценка компетентности;

h) предыдущий опыт и его соответствие конкретным обязанностям, которые предстоит выполнять, а также технологии, которые предстоит использовать; чем выше требуемый уровень компетентности, тем меньше должен быть разрыв между компетентностью, приобретенной в результате предыдущего опыта, и компетентностью, которая требуется для выполнения предстоящих конкретных обязанностей;

i) соответствие квалификации конкретным обязанностям, которые предстоит выполнять.

Подготовка, опыт и квалификация всех лиц, привлеченных к любым действиям, связанным с полным жизненным циклом безопасности, жизненными циклами безопасности E/E/PES или программного обеспечения, должны быть документированы.

Приложение С
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица С.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта Российской Федерации
МЭК 61508-2:2000	*
МЭК 61508-3:1998	ГОСТ Р МЭК 61508-3—2006 (МЭК 61508-3—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
МЭК 61508-4:1998	ГОСТ Р МЭК 61508-4—2006 (МЭК 61508-4—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения
МЭК 61508-5:1998	ГОСТ Р МЭК 61508-5—2006 (МЭК 61508-5—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
МЭК 61508-6:2000	*
МЭК 61508-7:2000	*
ИСО/МЭК Руководство 51:1999	ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты
МЭК Руководство 104:1997	*
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.	

Библиография

[1] МЭК 60300-3-1: 2003. Менеджмент риска. Руководство по применению методов анализа надежности

[2] МЭК 60300-3-9: 1995 Менеджмент риска. Анализ риска технологических систем

[3] МЭК 61355: 1997 Классификация и обозначения документации для установок, систем и оборудования

[4] МЭК 61506: 1997 Измерение и управление в промышленных процессах. Документация к прикладному программному обеспечению

[5] ИСО 8613-1: 1994 Информационные технологии. Открытая структура документа (ODA) и формат обмена. Введение и общие принципы

[6] ИСО 10007: 1995 Контроль качества. Руководство по управлению конфигурацией

[7] ИСО/МЭК TR 15846 Информационные технологии. Процессы жизненного цикла программного обеспечения. Управление конфигурацией программного обеспечения

[8] ANSI/ISA S84:1996 Применение систем, оснащенных средствами безопасности в обрабатывающих отраслях

[9] Процедуры для обработки отказов с общими причинами в исследованиях по безопасности и надежности. Процедурные основы и примеры, NUREG/CR-4780, Volume 1, January, 1988

[10] Процедуры для обработки отказов с общими причинами в исследованиях по безопасности и надежности. Аналитические основы и методы, NUREG/CR-4780, Volume 2, January, 1989

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

Ключевые слова: безопасность функциональная, жизненный цикл систем, электрические компоненты, электронные компоненты, программируемые электронные компоненты и системы, системы, связанные с безопасностью, планирование функциональной безопасности, программное обеспечение, уровень полноты безопасности.

Редактор *О. А. Стояновская*
Технический редактор *В. Н. Прусакова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 16.04.2008. Подписано в печать 07.08.2008. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 5,58. Уч.-изд. л. 5.20. Тираж 278 экз. Зак. 968.

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