ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-1— 2012

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

Часть 1

Общие требования

IEC 61508-1:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 октября 2012 г. № 586-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61508-1:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования» (IEC 61508-1:2010 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements»).

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

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

5 ВЗАМЕН ГОСТ Р МЭК 61508-1—2007

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

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 4
6 Управление функциональной безопасностью 6
7 Требования к жизненному циклу всей системы безопасности 8
8 Оценка функциональной безопасности 41
Приложение А (справочное) Пример структуры документации 45
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 50
Библиография 51

Введение

Системы, состоящие из электрических и/или электронных элементов, в течение многих лет используются для выполнения функций безопасности в большинстве областей применения. Компьютерные системы (обычно называемые программируемыми электронными системами), применяемые во всех прикладных отраслях для выполнения функций, не связанных с безопасностью, во все более увеличивающихся объемах используются для выполнения функций 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 всех стадий жизненного цикла систем, состоящих из электрических и/или электронных, и/или программируемых электронных (Э/Э/ПЭ) элементов, которые используются для выполнения функций обеспечения безопасности. Этот унифицированный подход был принят для того, чтобы разработать рациональную и последовательную техническую политику для всех электрических систем обеспечения безопасности. Основной целью при этом является содействие разработке стандартов для продукции и областей применения на основе стандартов серии МЭК 61508.

Примечание — Примерами стандартов для продукции и областей применения, разработанных на основе стандартов серии МЭК 61508, являются [1]—[3].

В большинстве ситуаций безопасность достигается за счет использования нескольких систем, 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 безопасности, входящие в состав общей системы обеспечения безопасности. Таким образом, хотя настоящий стандарт посвящен в основном Э/Э/ПЭ системам, связанным с безопасностью, он может также предоставлять общий подход, в рамках которого рассматриваются системы, связанные с безопасностью, базирующиеся на других технологиях.

Признанным фактом является существование огромного разнообразия использования Э/Э/ПЭ систем в различных областях применений, отличающихся различной степенью сложности, возможными опасностями и 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 продукции и областей применения, а также в последующих редакциях уже существующих стандартов.

Настоящий стандарт:

- рассматривает все соответствующие стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (от первоначальной концепции, проектирования, реализации, эксплуатации, технического обслуживания и до снятия с эксплуатации), в ходе которых Э/Э/ПЭ системы используются для выполнения функций безопасности;
- был задуман с учетом быстрого развития технологий; его основа является в значительной мере устойчивой и полной для применения во время будущих разработок;
- делает возможной разработку стандартов для продукции и областей применения, где используются Э/Э/ПЭ системы, связанные с безопасностью; разработка стандартов для продукции и областей применения в рамках общей структуры, вводимой настоящим стандартом, должна привести к более высокому уровню согласованности (например, основных принципов, терминологии и т. д.) как для отдельных областей применения, так и для их совокупностей, что даст преимущества в плане безопасности и экономики;
- предоставляет метод разработки спецификации требований к системе безопасности, необходимых для достижения заданной функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью;
- использует для определения требований к уровням полноты безопасности подход, основанный на оценке рисков;
- вводит уровни полноты безопасности при задании целевого уровня полноты безопасности для функций безопасности, которые должны быть реализованы Э/Э/ПЭ системами, связанными с безопасностью.

Примечание — Настоящий стандарт не устанавливает требования к уровню полноты безопасности для любой функции безопасности и не определяет, как устанавливается уровень полноты безопасности. Однако настоящий стандарт формирует основанный на риске концептуальный подход и предлагает примеры методов;

- устанавливает целевые меры отказов для функций безопасности, реализуемых Э/Э/ПЭ системами, связанными с безопасностью, и связывает эти меры с уровнями полноты безопасности;
- устанавливает нижнюю границу для целевых мер отказов для функции безопасности, реализуемой одиночной Э/Э/ПЭ системой, связанной с безопасностью. Для Э/Э/ПЭ систем, связанных с безопасностью в режиме:
- низкой интенсивности запросов на обслуживание: нижняя граница для выполнения функции, для которой система предназначена, устанавливается в соответствии со средней вероятностью опасного отказа по запросу, равной 10^{-5},
- высокой интенсивности запросов на обслуживание или в непрерывном режиме: нижняя граница устанавливается в соответствии со средней частотой опасных отказов 10^{-9} в час.

Примечания

1 Одиночная Э/Э/ПЭ система, связанная с безопасностью, не обязательно предполагает одноканальную архитектуру.

2 В проектах систем, связанных с безопасностью и имеющих низкий уровень сложности, можно достигнуть более низких значений целевой полноты безопасности, но предполагается, что в настоящее время указанные предельные значения целевой полноты безопасности могут быть достигнуты для относительно сложных систем (например, программируемые электронные системы, связанные с безопасностью);

- устанавливает требования по предотвращению и управлению систематическими отказами, основанные на опыте и заключениях из практического опыта. Учитывая, что вероятность возникновения систематических отказов в общем случае не может быть определена количественно, настоящий стандарт позволяет утверждать для специфицируемой функции безопасности, что целевая мера отказов, связанных с этой функцией, может считаться достигнутой, если все требования стандарта были выполнены;
- вводит понятие стойкости к систематическим отказам, применяемую к элементу, характеризующее уверенность в том, что полнота безопасности, касающаяся систематических отказов элемента, удовлетворяет требованиям заданного уровня полноты безопасности;
- применяет широкий диапазон принципов, методов и средств для достижения функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью, но не использует явно понятие «безопасного отказа». В то же время понятия «безопасный отказ» и «безопасный в своей основе» могут быть использованы, но для этого необходимо обеспечить подходящие требования в соответствующих разделах стандарта, которым эти понятия должны удовлетворять.

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 — 2013—08—01

1 Область применения

1.1 Настоящий стандарт охватывает вопросы, которые должны учитываться при использовании электрических, электронных, программируемых электронных (Э/Э/ПЭ) систем для выполнения функций безопасности. Главной целью настоящего стандарта является облегчить разработку стандартов для продукции и областей применения техническими комитетами, ответственными за эту продукцию и область применения. Это позволит полностью учесть существенные факторы, связанные с изделием или областью применения, и, таким образом, удовлетворить конкретные потребности области применения и потребителей изделия. Другая цель настоящего стандарта заключается в том, чтобы сделать возможной разработку Э/Э/ПЭ систем, связанных с безопасностью, в условиях возможного отсутствия стандартов для изделий и 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 элементы.

Примечания

1 Для Э/Э/ПЭ 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 Э/Э/ПЭ 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 Э/Э/ПЭ систем, связанных с безопасностью, не рассматриваются подробно в настоящем стандарте;

b) является основополагающим и применяется ко всем Э/Э/ПЭ системам, связанным с безопасностью, независимо от их применения;

c) охватывает достижение допустимого риска при помощи применения Э/Э/ПЭ систем, связанных с безопасностью, но не распространяется на опасности, источником которых является само Э/Э/ПЭ оборудование (например, поражение электрическим током);

d) применяется ко всем типам Э/Э/ПЭ систем, связанных с безопасностью, включая системы защиты и системы контроля;

e) не охватывает Э/Э/ПЭ системы, в которых:

- одной Э/Э/ПЭ системы достаточно для достижения допустимого риска, и
- требуемая полнота безопасности функций безопасности одной Э/Э/ПЭ системы меньше задаваемой для уровня полноты безопасности, равного 1 (самый низкий уровень полноты безопасности в настоящем стандарте);

f) относится, главным образом, к Э/Э/ПЭ 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 случа-

Издание официальное

ях настоящий стандарт может быть использован для определения любой Э/Э/ПЭ системы, используемой для защиты оборудования или продукции.

Примечание — См. МЭК 61508-4, пункт 3.1.1;

g) рассматривает Э/Э/ПЭ системы, связанные с безопасностью, и другие меры снижения риска для того, чтобы спецификации требований безопасности Э/Э/ПЭ систем, связанных с безопасностью, могли быть определены на основе систематического анализа рисков;

h) использует модель жизненного цикла всей системы безопасности как техническую основу для систематических действий, необходимых для обеспечения функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью.

Примечание — Хотя жизненный цикл всей системы безопасности относится в первую очередь к Э/Э/ПЭ системам, связанным с безопасностью, он может также лежать в основе анализа любой системы, связанной с безопасностью, независимо от технологии, на которой она основана (например, механической, гидравлической или пневматической);

i) 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;

j) устанавливает общие требования к Э/Э/ПЭ системам, связанным с безопасностью, где отсутствуют стандарты на продукцию или области применения;

k) требует рассмотрения злонамеренных и непредусмотренных действий во время анализа отказов и рисков. Сфера анализа включает в себя все стадии жизненного цикла системы безопасности.

Примечание — Другие стандарты МЭК/ИСО более глубоко рассматривают данный вопрос, см. ИСО/МЭК/TR 19791 [4] и серию МЭК 62443 [5];

l) не охватывает меры предосторожности, которые необходимы для того, чтобы предотвратить повреждения или иное неблагоприятное воздействие на функциональную безопасность Э/Э/ПЭ систем, связанных с безопасностью, со стороны лиц, не имеющих полномочий (см. перечисление k));

m) не определяет требования к разработке, внедрению, обслуживанию и/или эксплуатации политик безопасности или служб безопасности, необходимых для выполнения политики безопасности, которые могут потребоваться для Э/Э/ПЭ систем, связанных с безопасностью;

n) не применяется к медицинскому оборудованию, удовлетворяющему требованиям серии МЭК 60601 [6].

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 конкретные требования к Э/Э/ПЭ системам, связанным с безопасностью (требования к аппаратным средствам и программному обеспечению);
- МЭК 61508-4 содержит определения терминов и сокращения, которые используются в настоящем стандарте;
- [7] содержит руководство по применению МЭК 61508-1 для определения уровней полноты безопасности на основе использования различных методов;
- [8] содержит руководство по применению МЭК 61508-2 и МЭК 61508-3;
- [9] содержит обзор методов и средств.

1.4 МЭК 61508-1—МЭК 61508-4 являются базовыми стандартами по безопасности, хотя этот статус не применим в контексте Э/Э/ПЭ систем, связанных с безопасностью, имеющих низкую сложность (МЭК 61508-4, пункт 3.4.3). В качестве базовых стандартов по безопасности они предназначены для использования техническими комитетами при подготовке стандартов в соответствии с принципами, изложенными в руководстве МЭК 104 и руководстве ИСО/МЭК 51. МЭК 61508-1, МЭК 61508-2, МЭК 61508-3 и МЭК 61508-4 предназначены для использования в качестве самостоятельных стандартов. Функция безопасности настоящего стандарта не применима к медицинскому оборудованию, соответствующему требованиям серии горизонтальных стандартов МЭК 60601 [6].

Примечание — 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 на них нет конкретной ссылки или они не включены в стандарты, подготовленные этими техническими комитетами.

1.5 На рисунке 1 изображена общая структура стандартов серии МЭК 61508 и показана роль, которую играет настоящий стандарт в достижении функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью.

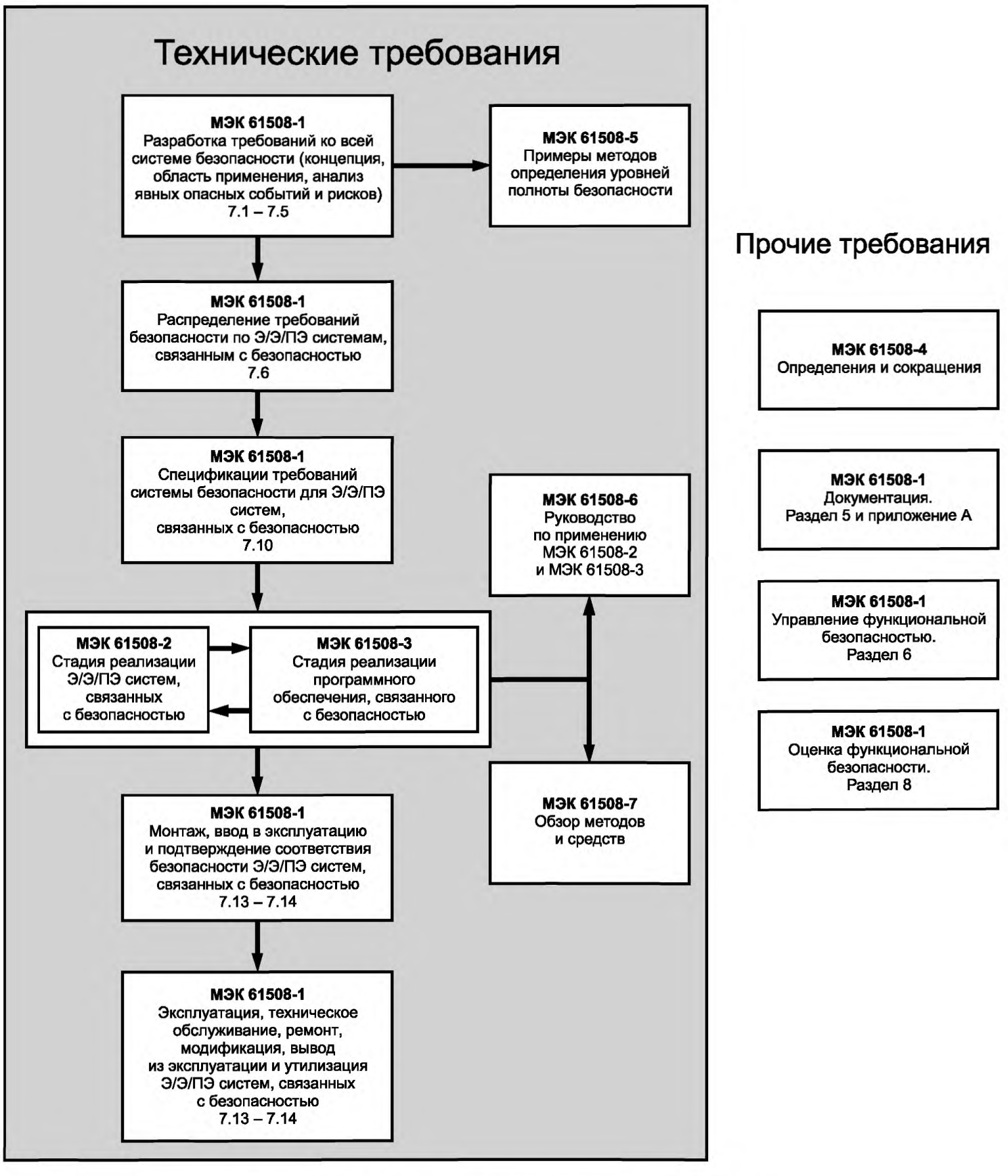


Рисунок 1 — Общая структура стандартов серии МЭК 61508

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

МЭК Руководство 104:1997 Подготовка стандартов по безопасности и использование базовых стандартов по безопасности и стандартов по безопасности групп (IEC Guide 104:1997, The preparation of safety publications and the use of basic safety publications and group safety publications)

ИСО/МЭК Руководство 51:1990 Аспекты безопасности. Руководящие указания по включению в стандарты (ISO/IEC Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards)

МЭК 61508-2:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к электрическим, электронным, программируемым электронным системам, связанным с безопасностью (IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2. Requirements for electrical/electronic/programmable electronic safety-related systems)

МЭК 61508-3:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению (IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements)

МЭК 61508-4:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения (ISO/IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4. Definitions and abbreviations)

3 Термины и определения

В настоящем стандарте применены термины и определения по МЭК 61508-4.

4 Соответствие настоящему стандарту

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

4.2 Настоящий стандарт определяет требования к Э/Э/ПЭ системам, связанным с безопасностью. Он был разработан для обеспечения охвата всего диапазона сложности, присущей таким системам. Однако для Э/Э/ПЭ систем, связанных с безопасностью, имеющих низкую сложность (МЭК 61508-4, пункт 3.4.3), там, где существует надежный практический опыт, дающий необходимую уверенность в том, что будет достигнута необходимая полнота безопасности, возможны следующие варианты:

- в международных стандартах для продукции и областей применения, реализующих требования серии стандартов МЭК 61508, некоторые требования могут быть необязательными и допускается освобождение от соответствия таким требованиям;
- если настоящий стандарт используется в условиях отсутствия стандарта для продукции или 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 для продукции и областей применения для Э/Э/ПЭ систем, связанных с безопасностью, разработанные на основе настоящего стандарта, должны учитывать требования ИСО/МЭК Руководство 51 и МЭК Руководство 104.

5 Документация

5.1 Цели

5.1.1 Первая цель требований настоящего раздела состоит в указании информации, которая должна быть документально оформлена для того, чтобы эффективно выполнять все стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

5.1.2 Второй целью требований настоящего раздела является указание информации, которая должна быть документально оформлена 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. [10].

5.2 Требования

5.2.1 Для каждой стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности 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 Э/Э/ПЭ 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 или определено в стандарте для продукции или 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 должна 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 изменяться, исправляться, проверяться и утверждаться под управлением соответствующей схемы контроля.

Примечание — При использовании для разработки документации автоматических и автоматизированных 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 раздела является определение обязанностей в управлении функциональной безопасностью для тех, кто несет ответственность за Э/Э/ПЭ систему, связанную с безопасностью, или за одну или более стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

6.1.2 Второй целью требований настоящего раздела является определение действий, выполняемых ответственными за управление функциональной безопасностью.

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

6.2 Требования

6.2.1 Организация, ответственная за Э/Э/ПЭ систему, связанную с безопасностью, или за одну или несколько стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, должна выделить одного или более сотрудников, несущих полную ответственность за:

- систему и стадии ее жизненного цикла;
- координацию действий, связанных с безопасностью, выполняемых на этих стадиях;
- взаимодействие между этими стадиями и другими стадиями, выполняемыми другими организациями;
- выполнение требований пунктов с 6.2.2 по 6.2.11 и 6.2.13;
- координацию оценки функциональной безопасности (см. 6.2.12, перечисление b) и раздел 8), особенно на тех стадиях, где выполнение оценки функциональной безопасности различается, включая взаимодействие, планирование, а также обобщение документации, обоснований и рекомендаций;
- удостоверение того, что функциональная безопасность достигнута и продемонстрировано соответствие с целями и требованиями настоящего стандарта.

Примечание — Ответственность за действия, связанные с безопасностью, или за стадии жизненного цикла безопасности, могут быть делегированы другим сотрудникам, в частности, выполняющим экспертизу. При этом разные сотрудники могут быть ответственными за разные действия и требования. Однако ответственность за координацию и функциональную безопасность всей системы должна принадлежать одному или небольшой группе сотрудников с достаточным уровнем административного ресурса.

6.2.2 Должна быть определена политика и стратегия достижения функциональной безопасности, а также средства для оценки ее достижения и средства взаимодействия внутри организации.

6.2.3 Должны быть определены все лица, подразделения и организации, ответственные за выполнение действий на соответствующих стадиях жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (включая отдельных лиц, ответственных за проверку и оценку функциональной безопасности, и, где это необходимо, органы лицензирования и органы регулирования в области безопасности), и их ответственность должна быть полностью и ясно доведена до их сведения.

6.2.4 Должны быть разработаны процедуры для определения, какая информация будет передаваться между соответствующими сторонами и как эта передача будет осуществляться.

Примечание — Требования к документации см. в разделе 5.

6.2.5 Должны быть разработаны процедуры, предназначенные для обеспечения быстрого исполнения решений и учета рекомендаций, относящихся к Э/Э/ПЭ системам, связанным с безопасностью, сформированных по результатам:

a) анализа опасностей и рисков (см. 7.4);

b) оценки функциональной безопасности (см. раздел 8);

c) действий по верификации (см. 7.18);

d) действий по подтверждению соответствия[1)] (см. 7.8 и 7.14);

e) управления конфигурацией (см. 6.2.10, 7.16, а также МЭК 61508-2 и МЭК 61508-3);

f) отчетов и анализа инцидентов (см. 6.2.6).

6.2.6 Должны быть разработаны процедуры, которые гарантируют, что все обнаруженные опасные события будут проанализированы и что будут выработаны рекомендации по минимизации возможности их повторения.

6.2.7 Должны быть определены требования к периодическому аудиту функциональной безопасности, включая:

a) частоту проведения аудита функциональной безопасности;

b) уровень независимости стороны, отвечающей за аудит;

c) требуемую документацию и программу выполнения аудита.

6.2.8 Должны быть разработаны процедуры для:

a) инициирования изменений в Э/Э/ПЭ системах, связанных с безопасностью (см. 7.16.2.2);

b) получения полномочий и разрешения для внесения изменений.

6.2.9 Должны быть разработаны процедуры для поддержания точной информации об опасностях и опасных событиях, функциях безопасности и Э/Э/ПЭ системах, связанных с безопасностью.

6.2.10 Должны быть разработаны процедуры для управления конфигурацией Э/Э/ПЭ систем, связанных с безопасностью, в течение всех стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, включая, в частности:

a) указатель на определенные стадии, на которых должен быть реализован формальный контроль конфигурации;

b) процедуры, которые должны быть использованы для уникальной идентификации всех составных частей компонентов (аппаратных средств и программного обеспечения);

c) процедуры для предотвращения использования неутвержденных компонентов.

6.2.11 Для аварийно-спасательных служб должно быть обеспечено соответствующее обучение и предоставлена соответствующая информация.

6.2.12 Те лица, которые несут ответственность за одну или более стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, должны для тех стадий, за которые они несут ответственность, и в соответствии с процедурами, определенными в 6.2.1—6.2.11, определить все управленческие и технические действия, необходимые для обеспечения достижения, демонстрации и поддержания функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью, включая:

a) определение мер и методов, используемых для удовлетворения требованиям конкретного раздела или подраздела (см. МЭК 61508-2, МЭК 61508-3 и МЭК 61508-6);

b) действия по оценке функциональной безопасности, а также способ, с помощью которого будет продемонстрировано достижение функциональной безопасности для тех, кто осуществляет ее оценку (см. раздел 8).

Примечание — При оценке функциональной безопасности должны быть использованы соответствующие процедуры для:

- определения соответствующей организации, лица или лиц с надлежащим уровнем независимости;
- составления и внесения изменений при оценке функциональной безопасности;
- замены тех, кто осуществляет оценку функциональной безопасности на каждом этапе жизненного цикла системы;
- разрешения споров с участием лиц, осуществляющих оценку функциональной безопасности.

c) процедуры для анализа и поддержки выполнения, в частности, для:

[1)] Оценка соответствия — в соответствии с Федеральным законом «О техническом регулировании».

- распознавания систематических отказов, которые могут поставить под угрозу функциональную безопасность, включая процедуры, используемые во время регламентных работ по обнаружению повторяющихся отказов;

- сравнения оцениваемых интенсивностей запросов и интенсивностей отказов во время эксплуатации и технического обслуживания с соответствующими предположениями, сделанными в ходе разработки системы.

6.2.13 Должны быть разработаны процедуры, гарантирующие, что все лица, ответственность которых определена в соответствии с 6.2.1 и 6.2.3 (т. е. все лица, участвующие в любом из жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, включая их действия по проверке, управлению функциональной безопасностью и оценке функциональной безопасности), должны иметь соответствующую компетентность (т. е. пройти обучение, обладать техническими знаниями, опытом и квалификацией), относящуюся к конкретным обязанностям, которые они должны выполнять. Такие процедуры должны включать требования к актуализации, обновлению и продолжению оценки компетентности.

6.2.14 Соответствие компетентности должно рассматриваться для конкретной области применения с учетом всех факторов, включая:

a) ответственность конкретного лица;

b) уровень необходимого надзора;

c) возможные последствия в случае отказа Э/Э/ПЭ систем, связанных с безопасностью, — чем серьезнее последствия, тем более строгой должна быть спецификация компетентности;

d) уровни полноты безопасности Э/Э/ПЭ систем, связанных с безопасностью, — чем выше уровень полноты безопасности, тем более строгой должна быть спецификация компетентности;

e) новизна проекта, проектных процедур или области применения — чем более новыми или менее проверенными они являются, тем более строгой должна быть спецификация компетентности;

f) предыдущий опыт и его актуальность для конкретных выполняемых обязанностей и используемых технологий — чем больше требуемая компетентность, тем выше должно быть соответствие между компетентностью, полученной из предыдущего опыта, и компетентностью, необходимой для конкретных видов деятельности, которые должны быть выполнены;

g) тип компетентности, соответствующей обстоятельствам (например, квалификация, опыт, соответствующая подготовка и последующая практика, способности к лидерству и принятию решений);

h) инженерные знания, соответствующие области применения и технологии;

i) инженерные знания в области безопасности, соответствующие применяемой технологии;

j) знание законодательной базы и нормативно-правовой базы в области безопасности;

k) соответствие квалификации конкретным выполняемым действиям.

Примечание — В [11] содержится пример метода управления компетентностью для Э/Э/ПЭ систем, связанных с безопасностью.

6.2.15 Компетентность всех лиц и их ответственности, определенные в соответствии с 6.2.1 и 6.2.3, должны быть документально оформлены.

6.2.16 Действия, указанные в 6.2.2 и 6.2.15, должны быть реализованы и их выполнение должно контролироваться.

6.2.17 Поставщики, предоставляющие продукцию или услуги организациям, несущим полную ответственность за одну или несколько стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (см. 6.2.1), должны поставлять свою продукцию и услуги в соответствии со спецификациями этих организаций и должны иметь соответствующую систему управления качеством.

6.2.18 Действия, относящиеся к управлению функциональной безопасностью, должны быть применены на соответствующих стадиях жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (см. 7.1.1.5).

7 Требования к жизненному циклу всей системы 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 требуемой полноты безопасности для функций безопасности, выполняемых Э/Э/ПЭ систе-

мами, связанными с безопасностью, в настоящем стандарте в качестве технического подхода принят жизненный цикл всей системы безопасности (см. рисунок 2).

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

7.1.1.2 Жизненный цикл всей системы безопасности охватывает следующие меры по достижению приемлемого риска:

- Э/Э/ПЭ системы, связанные с безопасностью;
- прочие меры снижения риска.

7.1.1.3 Стадия реализации Э/Э/ПЭ систем, связанных с безопасностью, жизненного цикла всей системы безопасности развернута и показана на рисунке 3. Эта часть жизненного цикла Э/Э/ПЭ системы рассмотрена в МЭК 61508-2. Стадия реализации жизненного цикла программного обеспечения системы безопасности показана на рисунке 4 и рассмотрена в МЭК 61508-3. Соотношения между жизненным циклом всей системы безопасности и жизненными циклами Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности для систем, связанных с безопасностью, показаны на рисунке 5.

7.1.1.4 Рисунки 2—4, на которых показаны жизненный цикл всей системы безопасности, жизненные циклы Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, 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 стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

7.1.1.5 На рисунках 2—4, изображающих жизненные циклы всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, 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 выполняться на соответствующих стадиях жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

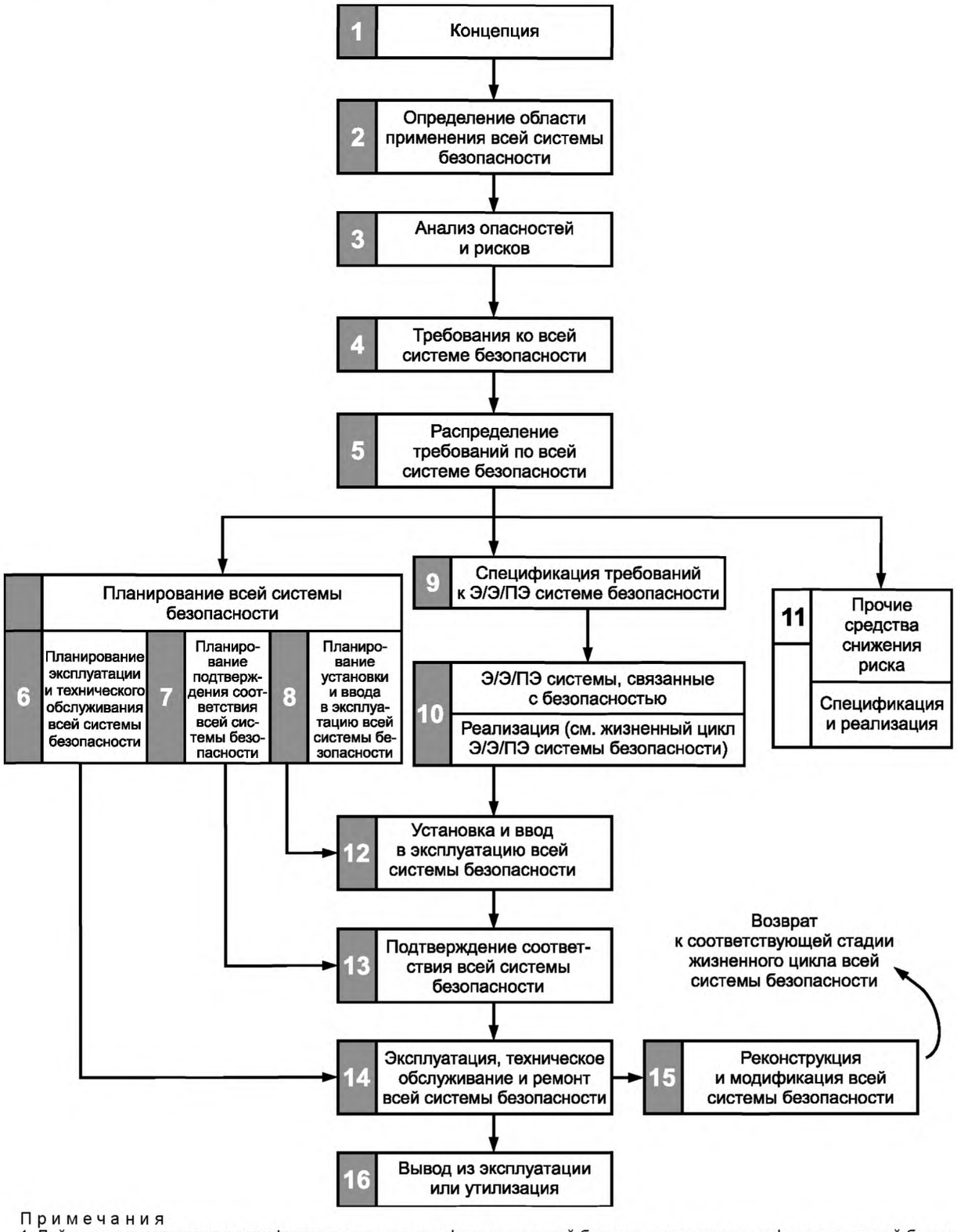
7.1.2 Цели и требования. Общие положения

7.1.2.1 Цели и требования для стадий жизненного цикла всей системы безопасности содержатся в 7.2—7.17. Цели и требования для стадий жизненного цикла Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности 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 жизненного цикла всей системы безопасности в таблице 1 указаны:

- цели, которые должны быть достигнуты;
- область распространения стадий;
- ссылки на подразделы, содержащие требования;
- требования к входным материалам для стадии;
- выходные материалы, необходимые для обеспечения соответствия с требованиями.



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 жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

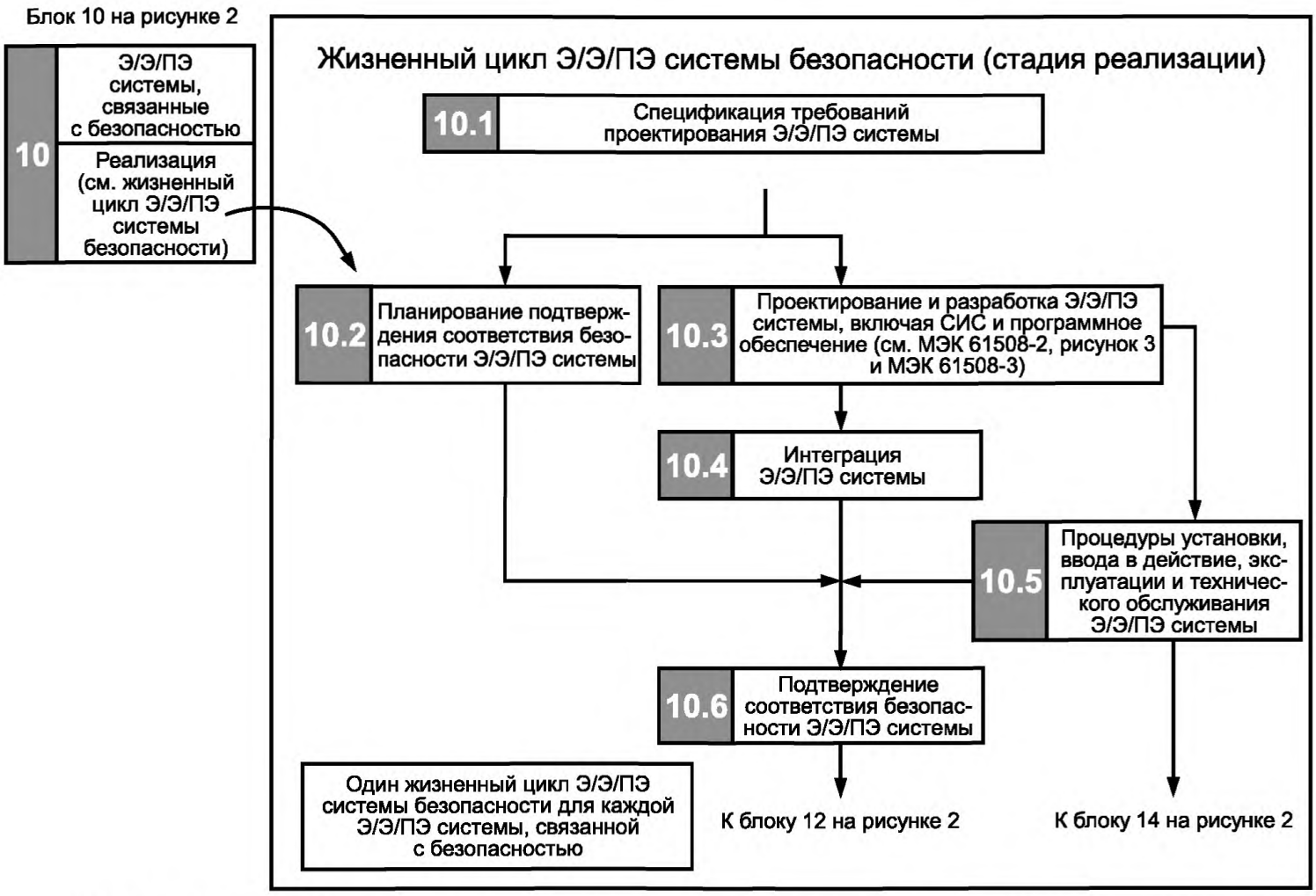
2 Стадии, представленные на рисунке блоком 11, находятся вне области применения настоящего стандарта.

3 МЭК 61508-2 и МЭК 61508-3 относятся к блоку 10 (реализация), но они также относятся при необходимости к аспектам блоков 13, 14 и 15 программируемой электроники (аппаратным средствам и программному обеспечению).

4 В таблице 1 описаны цели и область распространения стадий, представленных каждым блоком.

5. Технические требования, необходимые для эксплуатации, технического обслуживания, ремонта, модификации, модернизации и выводу из эксплуатации или утилизации всей системы безопасности, будут заданы как часть информации, предоставляемой поставщиком Э/Э/ПЭ системы, связанной с безопасностью, и ее элементов и компонентов.

Рисунок 2 — Структура жизненного цикла всей системы безопасности



Примечание — На рисунке представлены только те стадии жизненного цикла Э/Э/ПЭ системы безопасности, которые составляют стадию реализации жизненного цикла всей системы безопасности. Полный жизненный цикл Э/Э/ПЭ системы безопасности также содержит в себе стадии, реализуемые для Э/Э/ПЭ системы, связанной с безопасностью, соответствующие последующим стадиям жизненного цикла всей системы безопасности (блоки с 12 по 16 на рисунке 2).

Рисунок 3 — Структура жизненного цикла Э/Э/ПЭ системы безопасности (стадия реализации)



Примечание — На рисунке представлены только те стадии жизненного цикла программного обеспечения системы безопасности, которые находятся внутри стадии реализации жизненного цикла всей системы безопасности. Полный жизненный цикл программного обеспечения системы безопасности также содержит в себе стадии, реализуемые для программного обеспечения Э/Э/ПЭ системы, связанной с безопасностью, соответствующие последующим стадиям жизненного цикла всей системы безопасности (блоки с 12 по 16 на рисунке 2).

Рисунок 4 — Структура жизненного цикла программного обеспечения системы безопасности (стадия реализации)

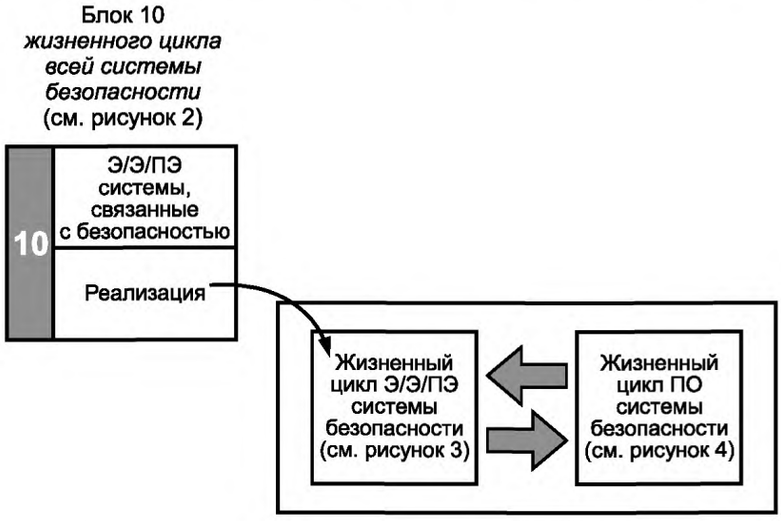


Рисунок 5 — Соотношение между жизненным циклом всей системы безопасности и жизненными циклами Э/Э/ПЭ системы безопасности и программного обеспечения (ПО) системы безопасности

Таблица 1 — Жизненный цикл всей системы безопасности: обзор

Стадия жизненного цикла системы 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 УО и его среды (физической, законодательной и др.), достаточного для удовлетворительного выполнения других действий в жизненном цикле системы безопасности	УО и его среда (физическая, законодательная и др.)	7.2.2	Вся существенная информация, необходимая для удовлетворения требований подраздела	Информация об УО, его окружении и опасностях
2 Определение области распространения всей системы безопасности	7.3.1 Определение границ УО и систем управления УО. Определение границ анализа опасностей и рисков (например, техногенного, природного характера и др.)	УО и его среда	7.2.3	Информация об УО, его окружении и опасностях	Определена область распространения анализа опасностей и рисков
3 Анализ опасностей и рисков	7.4.1 Определение опасностей, опасных событий и опасных ситуаций, связанных с УО и системой управления УО (во всех режимах эксплуатации) для всех достаточно предсказуемых обстоятельств, включая условия ошибок и неправильного использования (см. МЭК 61508-4, пункт 3.1.14). Определение последовательностей событий, приводящих к определенным опасным событиям. Определение рисков УО, связанных с определенными опасными событиями	Область распространения зависит от стадии в жизненных циклах всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (поскольку может потребоваться осуществление более чем одного анализа опасностей и рисков). Для предварительного анализа опасностей и рисков область распространения будет определена как результат определения области распространения всей системы безопасности	7.4.2	Определена область распространения анализа опасностей и рисков	Описание и информация, относящаяся к анализу опасностей и рисков

Продолжение таблицы 1

Стадия жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
4 Требования ко всей системе безопасности	7.5.1 Разработка спецификации требований ко всей системе безопасности в терминах требований к функциям безопасности и требований к полноте безопасности для Э/Э/ПЭ систем, связанных с безопасностью, других мер снижения риска, для достижения требуемой функциональной безопасности	В соответствии с определением области распространения всей системы безопасности	7.5.2	Описание и информация, относящаяся к анализу опасностей и рисков	Спецификация требований к безопасности для всей системы безопасности в терминах требований к функциям безопасности и требований к полноте безопасности
5 Распределение требований к безопасности по всей системе безопасности	7.6.1 Распределение функций безопасности, содержащихся в спецификации требований к безопасности по всей системе безопасности (требований к функциям безопасности и требований к полноте безопасности), назначая их Э/Э/ПЭ системам, связанным с безопасностью, и другим мерам снижения риска. Распределение уровней полноты безопасности для каждой функции безопасности, выполняемой Э/Э/ПЭ системой, связанной с безопасностью	В соответствии с определением области распространения всей системы безопасности	7.6.2	Спецификация требований к безопасности для всей системы безопасности в терминах требований к функциям безопасности и требований к полноте безопасности	Информация о распределении всех функций безопасности, их мер по целевым отказам и соответствующих уровней полноты безопасности. Предположения, касающиеся других мер по снижению риска, которые должны осуществляться в течение всего времени использования УО (см. 7.6.2.13)

Продолжение таблицы 1

Стадия жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
6 Планирование эксплуатации и технического обслуживания всей системы безопасности	7.7.1 Разработка плана эксплуатации и технического обслуживания Э/Э/ПЭ систем, связанных с безопасностью, гарантирующего выполнение требований функциональной безопасности в период эксплуатации и технического обслуживания	УО, системы управления УО и человеческий фактор. Э/Э/ПЭ системы, связанные с безопасностью	7.7.2	Информация о распределении всех функций безопасности, их мер по целевым отказам и соответствующих уровней полноты безопасности. Предположения, касающиеся других мер по сокращению риска, которые должны осуществляться в течение всего времени использования УО (см. 7.6.2.13)	План эксплуатации и технического обслуживания Э/Э/ПЭ систем, связанных с безопасностью
7 Планирование подтверждения соответствия всей системы безопасности	7.8.1 Разработка плана подтверждения соответствия Э/Э/ПЭ систем, связанных с безопасностью, безопасности всей системы	УО, системы управления УО и человеческий фактор. Э/Э/ПЭ системы, связанные с безопасностью	7.8.2	Информация и результаты распределения требований по всей системе безопасности	План подтверждения соответствия Э/Э/ПЭ систем, связанных с безопасностью, безопасности всей системы
8 Планирование установки и ввода в эксплуатацию всей системы безопасности	7.9.1 Разработка плана установки Э/Э/ПЭ систем, связанных с безопасностью, в контролируемой форме, гарантирующего выполнение требований функциональной безопасности. Разработка плана ввода в эксплуатацию Э/Э/ПЭ систем, связанных с безопасностью, в контролируемой форме, гарантирующего выполнение требований функциональной безопасности	УО и системы управления УО. Э/Э/ПЭ системы, связанные с безопасностью	7.9.2	Информация и результаты распределения требований по всей системе безопасности	План установки Э/Э/ПЭ систем, связанных с безопасностью. План ввода в эксплуатацию Э/Э/ПЭ систем, связанных с безопасностью

Продолжение таблицы 1

Стадия жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
9 Спецификация требований к Э/Э/ПЭ системе безопасности	7.10.1 Определение требований к Э/Э/ПЭ системе безопасности, в терминах требований к функциям безопасности Э/Э/ПЭ системы и требований к полноте безопасности Э/Э/ПЭ системы, для достижения требуемой функциональной безопасности	Э/Э/ПЭ системы, связанные с безопасностью	7.10.2	Информация и результаты распределения требований по всей системе безопасности	Спецификация требований к Э/Э/ПЭ системе безопасности
10 Реализация Э/Э/ПЭ систем, связанных с безопасностью	7.11.1 и части 2 и 3. Создание Э/Э/ПЭ систем, связанных с безопасностью, в соответствии со спецификацией требований к Э/Э/ПЭ системе безопасности (включая спецификацию требований к функциям безопасности Э/Э/ПЭ системы и специификацию требований к полноте безопасности Э/Э/ПЭ системы)	Э/Э/ПЭ системы, связанные с безопасностью	7.11.2, МЭК 61508-2 и МЭК 61508-3	Спецификация требований к Э/Э/ПЭ системе безопасности	Реализация каждой Э/Э/ПЭ системы, связанной с безопасностью, в соответствии со спецификацией требований к Э/Э/ПЭ системе безопасности
11 Прочие меры по снижению риска: спецификация и реализация	7.12.1 Создание прочих мер по снижению риска для достижения требований к функциям безопасности и требований полноты безопасности, определенных для таких систем (выходит за рамки области определения настоящего стандарта)	Прочие меры по снижению риска	7.12.2	Спецификация требований к безопасности прочих мер по снижению риска (выходит за рамки области определения настоящего стандарта и в дальнейшем не рассматривается)	Реализация каждой прочей меры по снижению риска в соответствии с требованиями к данной мере безопасности
12 Установка и ввод в эксплуатацию всей системы безопасности	7.13.1 Установка Э/Э/ПЭ систем, связанных с безопасностью. Ввод в эксплуатацию Э/Э/ПЭ систем, связанных с безопасностью	УО и системы управления УО. Э/Э/ПЭ системы, связанные с безопасностью	7.13.2	План установки Э/Э/ПЭ систем, связанных с безопасностью. План ввода в эксплуатацию Э/Э/ПЭ систем, связанных с безопасностью	Полностью установленные Э/Э/ПЭ системы, связанные с безопасностью. Полностью введенные в эксплуатацию Э/Э/ПЭ системы, связанные с безопасностью

Продолжение таблицы 1

Стадия жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
13 Подтверждение соответствия всей системы безопасности	7.14.1 Подтвердить соответствие, что Э/Э/ПЭ системы, связанные с безопасностью, отвечают спецификации требований к безопасности всей системы в терминах требований к функциям безопасности всей системы и требований к полноте безопасности всей системы с учетом распределения требований безопасности по Э/Э/ПЭ системам, связанным с безопасностью, в соответствии с 7.6	УО и системы управления УО. Э/Э/ПЭ системы, связанные с безопасностью	7.14.2	План подтверждения соответствия для Э/Э/ПЭ систем, связанных с безопасностью, безопасности всей системы. Информация и результаты распределения требований по всей системе безопасности	Подтверждение того, что все Э/Э/ПЭ системы, связанные с безопасностью, отвечают спецификации требований к безопасности всей системы с учетом распределения требований к безопасности по Э/Э/ПЭ системам, связанным с безопасностью
14 Эксплуатация, техническое обслуживание и ремонт всей системы безопасности	7.15.1 Гарантировать, что функциональная безопасность Э/Э/ПЭ систем, связанных с безопасностью, поддерживается на заданном уровне. Гарантировать, что технические требования, необходимые для эксплуатации, технического обслуживания и ремонта всей системы безопасности, определены для Э/Э/ПЭ систем, связанных с безопасностью, и предоставлены ответственным за предстоящую эксплуатацию и техническое обслуживание Э/Э/ПЭ систем, связанных с безопасностью	УО и системы управления УО. Э/Э/ПЭ системы, связанные с безопасностью	7.15.2	План эксплуатации и технического обслуживания для Э/Э/ПЭ систем, связанных с безопасностью, на основе плана эксплуатации и технического обслуживания всей системы безопасности	Постоянное обеспечение требуемой функциональной безопасности для Э/Э/ПЭ систем, связанных с безопасностью. Хронологическая документация по эксплуатации, ремонту и обслуживанию Э/Э/ПЭ систем, связанных с безопасностью

Окончание таблицы 1

Стадия жизненного цикла системы безопасности (номер стадии соответствует номеру блока на рисунке 2)	Цель	Область распространения	Номер пункта	Входной материал	Выходной материал
15 Внесение изменений и модификация всей системы безопасности	7.16.1 Определение процедур, необходимых для подтверждения того, что функциональная безопасность Э/Э/ПЭ систем, связанных с безопасностью, является соответствующей как во время, так и после выполнения стадии изменения и модификации	УО и системы управления УО. Э/Э/ПЭ 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 Э/Э/ПЭ систем, связанных с безопасностью как во время, так и после выполнения стадии внесения изменений и модификации. Хронологическая документация по внесению изменений и модификации Э/Э/ПЭ систем, связанных с безопасностью
16 Вывод из эксплуатации или утилизация	7.17.1 Определение процедур, необходимых для подтверждения того, что функциональная безопасность Э/Э/ПЭ систем, связанных с безопасностью, является соответствующей как во время, так и после выполнения действий по выводу из эксплуатации или утилизации УО	УО и системы управления УО. Э/Э/ПЭ 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 Э/Э/ПЭ систем, связанных с безопасностью как во время, так и после выполнения действий по выводу из эксплуатации или утилизации. Хронологическая документация о действиях 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 жизненного цикла всей системы безопасности, которые должны рассматриваться для достижения требуемой функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью.

7.1.3.2 Вторая цель требований настоящего подраздела состоит в документальном оформлении ключевой информации, имеющей отношение к функциональной безопасности Э/Э/ПЭ систем, связанных с безопасностью, на протяжении жизненного цикла всей системы безопасности.

Примечание — Требования к документации см. в разделе 5 и пример структуры документации см. в приложении А. Структура документации может учитывать процедуры, используемые в компаниях, и рабочую практику, сложившуюся в конкретных прикладных областях или для конкретных изделий.

7.1.4 Требования

7.1.4.1 Жизненный цикл всей системы безопасности, который должен использоваться как основа для декларирования соответствия настоящему стандарту, показан на рисунке 2. Если используется иная модель жизненного цикла всей системы безопасности, то она должна быть определена как часть управления действиями по функциональной безопасности (см. раздел 6); при этом должны быть реализованы все цели и требования каждого раздела и подраздела настоящего стандарта.

Примечание — Стадии жизненного цикла Э/Э/ПЭ системы безопасности и жизненного цикла программного обеспечения системы безопасности, образующие стадию реализации жизненного цикла всей системы безопасности, 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 жизненного цикла всей системы безопасности.

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

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

7.1.4.5 Область распространения и входные материалы для каждой стадии жизненного цикла всей системы безопасности должны соответствовать тем, которые указаны в таблице 1, если иное не обосновано специально как часть управления действиями функциональной безопасности (см. раздел 6), или определены в международном стандарте для области применения или конкретной продукции.

7.1.4.6 Выходные материалы каждой стадии жизненного цикла всей системы безопасности должны быть такими, как указано в таблице 1, если иное не обосновано специально как часть управления действиями функциональной безопасности (см. раздел 6), или определены в международном стандарте для области применения или конкретной продукции.

7.1.4.7 Выходные материалы каждой стадии жизненного цикла всей системы 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 жизненного цикла всей системы безопасности, определены в 7.18.

7.2 Концепция

Примечание — Эта стадия представлена на рисунке 2 блоком 1.

7.2.1 Цель

Цель требований данного подраздела состоит в расширении уровня понимания УО и окружающей среды (физической, законодательной и т. п.), достаточного для того, чтобы могли быть удовлетворительно выполнены другие действия в процессе жизненного цикла системы безопасности.

7.2.2 Требования

7.2.2.1 Необходимо собрать подробную информацию об УО, требуемых функциях управления и окружающей среде.

7.2.2.2 Необходимо определить потенциальные источники опасностей, опасных ситуаций и вредных событий.

7.2.2.3 Необходимо получить информацию об установленных опасностях (например, продолжительности, интенсивности, токсичности, пределах воздействия, механических усилиях, взрывоопасности, 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, опасные ситуации и вредные события в связи с другим оборудованием или системами (установленными или которые будут установлены) вблизи рассматриваемого УО (установленного или которое будет установлено).

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

7.3 Определение области распространения всей системы безопасности

Примечание — Эта стадия представлена на рисунке 2 блоком 2.

7.3.1 Цели

7.3.1.1 Первая цель требований данного подраздела состоит в определении границ УО и системы управления УО.

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

7.3.2 Требования

7.3.2.1 Границы УО и системы управления УО должны быть определены таким образом, чтобы было включено все оборудование и системы (включая людей в соответствующих случаях), связанные с соответствующими опасностями и опасными событиями.

Примечание — Может понадобиться несколько итераций между определением области распространения всей системы безопасности и анализом опасностей и рисков.

7.3.2.2 Должно быть определено физическое оборудование, включая УО и системы управления УО, которое входит в область распространения анализа опасностей и рисков.

Примечание — См. [12] и [13].

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

7.3.2.4 Должны быть определены системы и оборудование, связанные с опасностями и рисками.

7.3.2.5 Должны быть определены типы событий, приводящие к инцидентам, которые должны быть учтены (например, отказы компонентов, отказы процедур, человеческие ошибки, механизмы зависимости отказов, которые могут привести к опасным событиям).

7.3.2.3 Требования 7.3.2.1—7.3.2.5 и результаты их выполнения должны быть документально оформлены.

7.4 Анализ опасностей и рисков

Примечание — Данная стадия представлена на рисунке 2 блоком 3.

7.4.1 Цели

7.4.1.1 Первая цель требований данного подраздела состоит в определении опасностей, опасных событий и опасных ситуаций, относящихся к УО и системе управления УО (во всех режимах работы) для всех обоснованных предсказуемых случаев, включая условия появления отказов и предсказуемое неправильное применение аппаратных средств и программного обеспечения (см. 3.1.14 МЭК 61508-4).

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

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

Примечания

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

2 В тех областях применения, в которых могут быть сделаны достоверные предположения о рисках, относящихся к опасным событиям и их последствиям, анализ, требуемый данным подразделом (и подразделом 7.5), может быть выполнен разработчиками версий настоящего стандарта, предназначенных для конкретных областей применения, и может быть встроен в упрощенные графические требования. Примеры таких методов приведены в [7], приложения E и G.

7.4.2 Требования

7.4.2.1 Должен быть проведен анализ опасностей и рисков, который учитывает информацию, полученную на стадии определения области распространения всей системы безопасности (см. 7.3). Если на более поздних стадиях жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности принимаются решения, которые могут изменить базис, на котором основывались предыдущие решения, то должен быть проведен дальнейший анализ опасностей и рисков.

Примечания

1 Руководящие указания см. в [12] и [13].

2 В качестве примера необходимости проводить углубленный анализ опасностей и рисков в ходе жизненного цикла всей системы безопасности рассмотрим анализ УО, которое 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 УО, 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 Должны быть рассмотрены возможности исключения или сокращения опасностей.

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

7.4.2.3 Опасности, опасные события и опасные ситуации, связанные с УО и системой управления УО, должны быть определены для всех разумно предсказуемых условий (включая условия возникновения отказов, разумно предсказуемое неправильное использование и злонамеренные или несанкционированные действия). В этот круг входят все случаи, связанные с человеческим фактором. Особое внимание должно быть уделено аномальным и редким режимам работы УО. Если анализ опасных факторов показал, что злонамеренные или несанкционированные действия, представляющие угрозу безопасности, являются разумно предсказуемыми, тогда должен быть выполнен анализ угроз безопасности.

Примечания

1 Разумно предсказуемое неправильное использование см. в МЭК 61508-4 (пункт 3.1.14).

2 Руководство по обнаружению опасностей, включая руководство по представлению и анализу проблем, связанных с человеческим фактором, см. [14].

3 Руководство по анализу угроз безопасности см. в [5].

4 Злонамеренные или несанкционированные действия охватывают угрозы безопасности.

5 Анализ опасностей и рисков должен также рассмотреть вопрос о том, что активация функции безопасности по запросу или из-за ложных действий может привести к новой опасности. В такой ситуации может быть необходимо разработать новые функции безопасности в целях борьбы с новой опасностью.

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

Примечания

1. Последовательности событий должны рассматриваться с учетом политики безопасности и решений по управлению рисками.

2. 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.

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

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

7.4.2.8 Требования 7.4.2.1—7.4.2.7 могут быть удовлетворены путем применения методов качественного или количественного анализа опасностей и рисков (МЭК 61508-5 [7]).

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

- конкретные опасности и их последствия;
- сложность УО и систем управления УО;
- область применения и принятая в ней практика, считающаяся «хорошей»;
- требования норм правового и технического регулирования в области безопасности;
- риски УО;
- 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;
- допустимый риск для каждого опасного события;
- меры, предпринимаемые для сокращения или исключения опасностей и рисков;
- допущения, сделанные при анализе рисков, включая оцененные значения интенсивностей запросов и интенсивностей отказов оборудования; должна быть детализирована степень доверия к ограничениям в работе и вмешательству человека.

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

7.4.2.12 Информация и результаты анализа опасностей и рисков для УО и системы управления УО должны поддерживаться на полном жизненном цикле всей системы безопасности, начиная со стадии анализа опасностей и рисков и до вывода из эксплуатации или утилизации.

Примечание — Поддержка информации, вытекающей из результатов стадии анализа опасностей и рисков, является основным средством отслеживания прогресса по нерешенным вопросам анализа опасностей и рисков.

7.5 Требования ко всей системе безопасности

Примечание — Эта стадия представлена на рисунке 2 блоком 4.

7.5.1 Целью требований данного подраздела является разработка спецификации требований ко всей системе безопасности, выраженных в требованиях к функциям безопасности всей системы безопасности и требованиях к полноте безопасности всей системы безопасности, относящихся к Э/Э/ПЭ системам, связанным с безопасностью, и другим мерам 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, требуемый данным подразделом (и подразделом 7.4), может быть выполнен разработчиками версий настоящего стандарта, предназначенных для областей применения, и может быть встроен в упрощенные графические требования. Примеры таких методов приведены в МЭК 61508-5 (приложения E и F) [7].

7.5.2 Требования

7.5.2.1 Набор всех необходимых функций безопасности всей системы безопасности должен быть разработан на основе опасных событий, полученных в результате анализа опасностей и рисков. Они должны формировать спецификацию требований к функциям безопасности всей системы безопасности.

Примечания

1 Для каждого опасного события для всей системы безопасности необходимо создать функцию безопасности.

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

Пример — Предотвращение повышения температуры в сосуде X выше 250 °C, предотвращение роста скорости диска Y выше 3000 об/мин — это примеры функций безопасности всей системы.

7.5.2.2 Если были обнаружены нарушения безопасности, то должен быть проведен анализ уязвимостей в целях определения требований к безопасности.

Примечание — Руководство приведено в МЭК 62443 [5].

7.5.2.3 Для каждой функции безопасности всей системы безопасности должны определяться целевые требования полноты безопасности в результате удовлетворения допустимого риска. Каждое требование может быть определено количественным и/или качественным методом. Они должны составлять спецификацию требований к полноте безопасности всей системы безопасности.

Примечания

1 Спецификация требований к полноте безопасности всей системы безопасности является промежуточным этапом на пути к определению целевых мер отказов и соответствующих уровней полноты безопасности для функций безопасности, которые должны быть реализованы Э/Э/ПЭ системами, связанными с безопасностью. Некоторые из качественных методов, используемых для определения уровней полноты безопасности (см. [7], приложения E и F), содержат переход непосредственно от параметров риска к уровням полноты безопасности. В таких случаях требования к полноте безопасности являются неявными, то есть не формируются явным образом, поскольку они интегрированы в сам метод.

2 Риск УО может быть снижен либо путем сокращения последствий опасных событий (что предпочтительнее) или путем снижения интенсивности опасных событий УО и системы управления УО (см. 7.5.2.4)

3 Требуемое снижение частоты опасных событий может быть достигнуто путем принятия дополнительных мер, включающих Э/Э/ПЭ системы, связанные с безопасностью, и/или других мер по снижению риска, включающих системы, связанные с безопасностью, использующие другие технологии, или мер по управлению такими параметрами как время освобождения, время заполнения соответствующих зон или время нахождения в них.

4. В целях удовлетворения критериям допустимого риска при определении целевого уровня полноты безопасности для каждой функции безопасности может быть необходимо учитывать, что люди могут быть подвержены рискам из других источников.

5. Если для областей применения существуют международные стандарты, которые включают подходящие методы для непосредственного определения требований полноты безопасности, то их можно применять для удовлетворения требованиям данного пункта.

7.5.2.4 Требования к полноте безопасности всей системы безопасности могут быть определены в терминах либо:

- необходимого снижения риска для достижения допустимого риска, либо
- допустимой интенсивности опасных событий, удовлетворяющей допустимому риску.

7.5.2.5 Если при оценке риска УО средняя частота опасных отказов отдельной функции системы управления УО оказалась ниже, чем 10^{-5} опасных отказов в час, то такая система управления УО считается системой управления, связанной с безопасностью, и должна удовлетворять требованиям настоящего стандарта.

Примечание — Например, если указанная для системы управления УО интенсивность опасного отказа находится между 10^{-6} и 10^{-5} опасных отказов в час, то тогда система управления УО рассматривается как Э/Э/ПЭ система, связанная с безопасностью, и для нее должны быть выполнены соответствующие требования уровня полноты безопасности 1.

7.5.2.6 Когда отказы системы управления УО относятся к одной или нескольким Э/Э/ПЭ системам, связанным с безопасностью, и/или к другим средствам снижения риска и когда система управления УО не позиционируется как система, связанная с безопасностью, то должны применяться следующие требования:

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

- данными о фактической работе системы управления УО 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 УО, должна быть не ниже, чем 10^{-5} отказов в час.

Примечание — См. 7.5.2.5;

c) все разумно предсказуемые режимы опасных отказов системы управления УО должны быть учтены при разработке спецификации требований к безопасности всей системы безопасности;

d) система управления УО должна быть независимой от Э/Э/ПЭ систем, связанных с безопасностью, и других средств снижения риска.

Примечания

1 Если системы, связанные с безопасностью, проектировались для обеспечения соответствующей полноты безопасности с учетом обычной интенсивности запросов от системы управления УО, то не требуется позиционировать систему управления УО как систему, связанную с безопасностью (и, следовательно, ее функции не будут рассматриваться 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 УО 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.

2 О значении независимости см. 7.6.2.7.

7.5.2.7 Если требования 7.5.2.6 [перечисления a) — d)] не могут быть соблюдены, то система управления УО должна рассматриваться как система, связанная с безопасностью. Уровень полноты безопасности функций системы управления УО должен быть определен на основе интенсивности опасных отказов, объявленной для системы управления УО в соответствии с таблицей 3 (см. примечание 3 к 7.6.2.9). В таких случаях требования настоящего стандарта, относящиеся к назначаемому уровню полноты безопасности, должны применятся к системе управления УО.

Примечание — См. также 7.5.2.5 и 7.6.2.10.

7.6 Распределение требований к безопасности по всей системе безопасности

Примечание — Эта стадия представлена на рисунке 2 блоком 5.

7.6.1 Цели

7.6.1.1 Первой целью требований данного подраздела является распределение функций безопасности всей системы безопасности, содержащихся в спецификации требований к безопасности всей

системы безопасности (включающей требования к функциям безопасности всей системы безопасности и требования к полноте безопасности всей системы безопасности), по назначенным Э/Э/ПЭ системам, связанным с безопасностью, и другим средствам снижения риска.

Примечание — Другие меры по снижению риска рассматриваются при необходимости, когда распределение по Э/Э/ПЭ системам, связанным с безопасностью, не может быть выполнено без них.

7.6.1.2 Второй целью требований данного подраздела является распределение целевых мер отказов и соответствующих уровней полноты безопасности для каждой функции безопасности, реализуемой Э/Э/ПЭ системой, связанной с безопасностью.

7.6.2 Требования

7.6.2.1 Должны быть определены назначенные системы, связанные с безопасностью, которые будут использоваться для достижения требуемой функциональной безопасности. Допустимый риск может быть достигнут за счет:

- Э/Э/ПЭ систем, связанных с безопасностью, и/или
- других мер по снижению риска.

Примечание — Настоящий стандарт применим, только если допустимый риск хотя бы частично достигается за счет Э/Э/ПЭ системы, связанной с безопасностью.

7.6.2.2 При распределении функций безопасности всей системы безопасности по назначенным Э/Э/ПЭ системам, связанным с безопасностью, и другим мерам по снижению риска, должны быть учтены возможности и ресурсы всех стадий жизненного цикла всей системы 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 то же время обладать рядом преимуществ из-за уменьшившейся сложности Э/Э/ПЭ системы.

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

7.6.2.3 Каждая функция безопасности всей системы безопасности вместе с относящимся к ней общим требованием к полноте безопасности всей системы безопасности, разработанным в соответствии с 7.5, должна быть распределена по одной или нескольким назначенным Э/Э/ПЭ системам, связанным с безопасностью, и другим мерам по снижению риска для достижения требуемого снижения уровня риска для этой функции безопасности. Это распределение имеет итерационный характер. Если будет установлено, что требуемое снижение риска не может быть достигнуто, то спецификации для системы управления УО, назначенных Э/Э/ПЭ систем, связанных с безопасностью, и других мер по снижению риска должны быть изменены и распределение должно быть выполнено повторно.

Примечания

1 Решение о распределении конкретной функции безопасности всей системы безопасности по одной или нескольким Э/Э/ПЭ системам, связанным с безопасностью, или другим мерам по снижению риска, зависит от ряда факторов, но в особенности от требований к полноте безопасности всей системы безопасности. Чем более обременительны требования к полноте безопасности, тем больше вероятность того, что функция будет распределена между более чем одной Э/Э/ПЭ системой, связанной с безопасностью, и/или другой мерой по снижению риска.

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 всей системы безопасности были распределены и были определены целевые меры отказов для каждой функции безопасности (в том числе требования, определенные в 7.6.2.10).

7.6.2.5 Требования к полноте безопасности для каждой функции безопасности должны быть сформулированы в терминах:

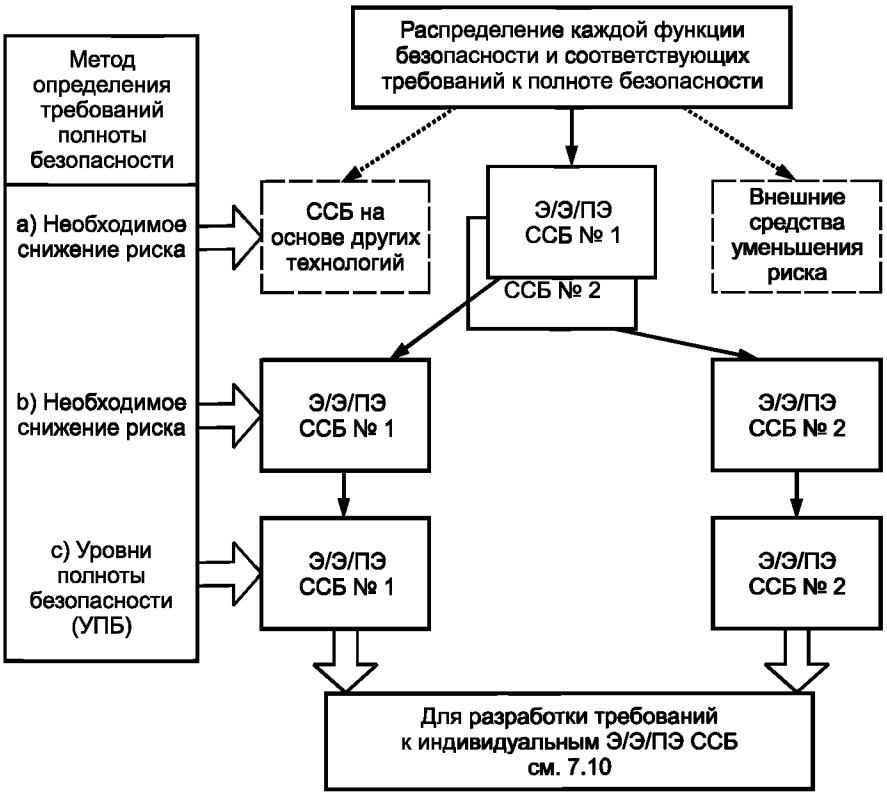
- средней вероятности опасных отказов функции безопасности по запросу для режима работы с низкой частотой или
- средней частоты опасных отказов функции безопасности [h^{-1}] для режима работы с высокой частотой запросов или режима с непрерывным запросом.

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

Примечания

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

2 Если для достижения допустимого риска необходимы несколько Э/Э/ПЭ систем, связанных с безопасностью, и/или другие меры по снижению риска, то реально достигнутый риск будет зависеть от систематических зависимостей между Э/Э/ПЭ системами, связанными с безопасностью, и/или другими мерами по снижению риска (более подробно о зависимостях и их анализе см. МЭК 61508-5, подраздел А.5.4 [7]).



Примечания

1 Требования к полноте безопасности всей системы безопасности связываются с каждой функцией безопасности всей системы безопасности до распределения (см. 7.5.2.3).

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

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

Рисунок 6 — Распределение требований ко всей системе безопасности по Э/Э/ПЭ системам, связанным с безопасностью, и другим средствам снижения риска

7.6.2.7 Распределение следует проводить с учетом вероятности отказов по общей причине. Если система управления УО, Э/Э/ПЭ системы, связанные с безопасностью, и другие меры по снижению риска должны рассматриваться при распределении как независимые, они:

- должны быть независимыми настолько, чтобы вероятность одновременного отказа двух или более из этих различных систем или мер была достаточно низкой по сравнению с требуемой полнотой безопасности;
- 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 по общей причине, например, авиационным катастрофам или землетрясениям;

- 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, технического обслуживания или тестирования.

Примечание — Настоящий стандарт касается именно реализации требований безопасности, распределенных по Э/Э/ПЭ системам, связанным с безопасностью, и требования в нем определены так, как они должны быть заданы для этих систем. Реализация требований безопасности, распределенных по другим мерам снижения риска, в настоящем стандарте подробно не рассматривается.

При анализе общей причины должны быть проверены ограничения и условия ограничений для реализации Э/Э/ПЭ систем, связанных с безопасностью, такие как необходимое разделение различных каналов Э/Э/ПЭ системы, подсистемы или элемента, например пространственное. Возможно, это нельзя реализовать, например, для двух каналов или микропроцессоров на одной плате, либо для ИС с избыточностью на одном кристалле (см. МЭК 61508-2, приложение Е).

7.6.2.8 Если не все требования 7.6.2.7 могут быть выполнены, то Э/Э/ПЭ системы, связанные с безопасностью, и другие средства по снижению риска не должны считаться независимыми при распределении уровней полноты безопасности. Вместо этого при распределении необходимо учитывать соответствующие отказы по общей причине между системой управления УО, Э/Э/ПЭ системой, связанной с безопасностью, и другими средствами снижения риска.

Примечания

1 Более подробную информацию по вопросу анализа зависимых отказов см. в [15] и [16].

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

3 Как показано в 7.6.2.3, распределение является итеративным процессом, и если анализ, включающий анализ отказов по общей причине, показывает, что допустимый риск не может быть достигнут, исходя из начальных допущений, то могут понадобиться изменения в проекте (дальнейшие указания см. в [7], подраздел А.5.4).

7.6.2.9 При завершении проработки распределения требования к полноте безопасности для каждой функции безопасности, распределенные по Э/Э/ПЭ системе(ам), связанной(ым) с безопасностью, должны быть выражены в терминах полноты безопасности в соответствии с таблицами 2 и 3 и должны быть пригодны, чтобы показать, является ли целевая мера отказов:

- средней вероятностью опасных отказов по запросу функции безопасности (PFD_{avg}) для режима работы с низкой частотой запросов (таблица 2), или
- средней вероятностью опасных отказов функции безопасности в час (PFH), для режима работы с высокой частотой запросов (таблица 3), или
- средней вероятностью опасных отказов функции безопасности в час (PFH), для режима работы с непрерывным запросом (таблица 3).

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

Уровень полноты безопасности	Средняя вероятность опасного отказа функции безопасности по запросу (PFD_{avg})
4	$> 10^{-5} — < 10^{-4}$
3	$> 10^{-4} — < 10^{-3}$
2	$> 10^{-3} — < 10^{-2}$
1	$> 10^{-2} — < 10^{-1}$

Таблица 3 — Уровни полноты безопасности: целевая мера отказов для функции безопасности, работающей в режиме высокой интенсивности запросов или в режиме с непрерывным запросом

Уровень полноты безопасности	Средняя частота опасных отказов функции безопасности [h^{-1}] (PFH)
4	$> 10^{-9} — < 10^{-8}$
3	$> 10^{-8} — < 10^{-7}$
2	$> 10^{-7} — < 10^{-6}$
1	$> 10^{-6} — < 10^{-5}$

Примечания

1 Определение терминов «режим работы с низкой интенсивностью запросов» и «режим работы с высокой интенсивностью запросов» или «режим с непрерывным запросом» см. в МЭК 61508-4, пункт 3.5.16.

2. Руководящие указания по режимам работы, связывающих целевые меры отказов с анализом опасностей и рисков, см. в [7].

3 Таблицы 2 и 3 связывают целевые меры отказов, распределенные для функции безопасности, реализуемой Э/Э/ПЭ системой, связанной с безопасностью, с уровнем полноты безопасности. Допускается, что может оказаться невозможным предсказать количественно полноту безопасности для всех аспектов Э/Э/ПЭ систем, связанных с безопасностью. В этом случае по отношению к мерам предосторожности, необходимым для достижения целевых мер отказов, должны быть применены качественные методы, меры и обоснования. Это особенно относится к случаю систематической полноты безопасности (см. МЭК 61508-4, пункт 3.5.4), где для заданного уровня полноты безопасности по отношению к мерам предосторожности, необходимым для достижения требуемой систематической полноты безопасности, должны быть применены качественные методы и обоснования (см. МЭК 61508-2, пункты 7.4.2.2 перечисление с), 7.4.3, 7.4.6, 7.4.7 и МЭК 61508-3).

4 Для полноты безопасности аппаратных средств необходимо применять количественные методы оценки надежности для того, чтобы оценить целевую полноту безопасности, которую необходимо достигнуть, как это определено в ходе оценки риска, принимая во внимание отказы оборудования (см. МЭК 61508-2, пункт 7.4.5).

5 Если уровень полноты безопасности определяется с использованием качественного метода (например, граф риска, качественный метод), то либо таблица 2, либо таблица 3, при необходимости дает количественные меры отказа, которые устанавливают ограничения для полноты безопасности аппаратных средств.

6 Если используются две или более Э/Э/ПЭ системы, связанные с безопасностью, то полнота безопасности, которая может быть заявлена, может оказаться лучше той, которая приведена в таблице 2, при условии, что достигнут надлежащий уровень независимости между системами. Например, это будет актуально, если заданная функция безопасности выполняется двумя Э/Э/ПЭ системами, связанными с безопасностью, когда между ними достигнут достаточный уровень независимости.

7 Для Э/Э/ПЭ системы, связанной с безопасностью, действующей в режиме высокой интенсивности запросов или в режиме с непрерывным запросом, 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 определяется необходимый уровень полноты безопасности.

7.6.2.10 Для Э/Э/ПЭ 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 Если в результате распределения требований к безопасности Э/Э/ПЭ система, связанная с безопасностью, должна реализовать функцию безопасности с УПБ 4, то необходимо выполнить следующее:

a) Необходимо провести повторный анализ применения, чтобы выяснить, могут ли быть изменены какие-либо параметры риска, так чтобы требования УПБ 4 для функции безопасности можно было избежать. Анализ должен выяснить, можно ли:

- ввести дополнительные системы, связанные с безопасностью и другие меры снижения риска, не основанные на Э/Э/ПЭ системах, связанных с безопасностью;
- уменьшить тяжесть последствий;
- уменьшить вероятность указанных последствий.

b) Если после повторного анализа приложения было принято решение реализовывать функцию безопасности с УПБ 4, то дальнейшая оценка рисков должна осуществляться с использованием количественного метода, который учитывает возможные отказы по общей причине между Э/Э/ПЭ системой, связанной с безопасностью, и:

- любыми другими системами, отказ которых проявится при запросе, и
- любой другой системой, связанной с безопасностью.

7.6.2.12 Ни одна одиночная функция безопасности Э/Э/ПЭ системы, связанной с безопасностью, не должна быть размещена по величине 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 опасного отказа функции безопасности по запросу, равная 10^{-5};

- в режиме высокой интенсивности запросов или в режиме с непрерывным запросом в качестве нижней границы принимается средняя частота опасных отказов, равная 10^{-9} в час.

Примечание — В настоящее время можно проектировать системы, связанные с безопасностью, с более низкими значениями целевой полноты безопасности для несложных систем, но считается, что эти пределы представляют значения, достижимые относительно сложными системами (например, программируемыми электронными системами, связанными с безопасностью).

7.6.2.13 Информация и результаты распределения требований к безопасности всей системы безопасности, полученные в 7.6.2.1—7.6.2.12, вместе с любыми сделанными допущениями и обоснованиями должны быть документально оформлены (включая предположения относительно других мер снижения риска, которые должны осуществляться на протяжении всего периода жизни УО).

Примечание — Для каждой Э/Э/ПЭ системы, связанной с безопасностью, должен быть достаточный объем информации по функциям безопасности и связанными с ними уровнями полноты безопасности. Эта информация формирует основу требований системы безопасности для Э/Э/ПЭ систем, связанных с безопасностью, определяемых в 7.10.

7.7 Планирование эксплуатации и технического обслуживания всей системы безопасности

Примечания

1 Данная стадия представлена блоком 6 на рисунке 2.

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

3 Пример модели управления эксплуатацией и техническим обслуживанием показан на рисунке 8.

4 Требования 7.7.2 являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер снижения риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться на протяжении всего срока службы УО.

5 Для достижения функциональной безопасности аналогичные требования необходимы для всех других мер снижения риска.

7.7.1 Цель

Целью требований данного подраздела является разработка плана эксплуатации и сопровождения Э/Э/ПЭ 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 Э/Э/ПЭ 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 небезопасное состояние, уменьшения запросов к Э/Э/ПЭ системе, связанной с безопасностью, либо ослабления последствий опасных событий.

Примечание — С Э/Э/ПЭ системами, связанными с безопасностью, связаны следующие ограничения, условия и действия:

1) ограничения на работу УО при сбое Э/Э/ПЭ систем, связанных с безопасностью;

2) ограничения на работу УО в период обслуживания Э/Э/ПЭ систем, связанных с безопасностью;

3) когда могут быть отменены ограничения на работу УО;

4) процедуры возврата к нормальной работе;

5) процедуры подтверждения того, что достигнут нормальный режим работы;

6) обстоятельства, при которых функции, реализуемые Э/Э/ПЭ системой, связанной с безопасностью, могут быть пропущены при пуске, во время выполнения специальных операций или при тестировании;

7) процедуры, которым необходимо следовать до, во время и после отключения Э/Э/ПЭ 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 обо всех опасных событиях и всех инцидентах, 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 технического обслуживания (см. 7.15).

Примечания

1 Большинство Э/Э/ПЭ систем, связанных с безопасностью, имеет некоторые виды отказов, которые могут быть обнаружены только при тестировании во время стандартного технического обслуживания. Если тестирование не будет проводиться с достаточной частотой, требования к полноте безопасности для Э/Э/ПЭ системы, связанной с безопасностью, не будут достигнуты.

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 технического обслуживания системы, связанной с безопасностью. Эти процедуры включают в себя подготовительные процедуры для любой модификации программного обеспечения, которые могут быть результатом потребностей, возникших в период эксплуатации или технического обслуживания (см. также МЭК 61508-3, подраздел 7.6). Реализация этих процедур — по МЭК 61508-3, подраздел 7.8. Процедуры подготовки к будущим изменениям программного обеспечения, которые являются результатом потребностей в изменении систем, связанных с безопасностью, рассматриваются в МЭК 61508-3, подраздел 7.6. Реализация этих процедур — по МЭК 61508-2, подраздел 7.8.

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

7.7.2.2 Если какая-либо подсистема Э/Э/ПЭ системы, связанной с безопасностью, с отказоустойчивостью аппаратных средств, равной нулю, выключается для тестирования, то план должен гарантировать, чтобы безопасность УО обеспечивалась постоянно с помощью дополнительных мер и ограничений. Полнота безопасности, обеспечиваемая дополнительными мерами и ограничениями, должна быть как минимум равна полноте безопасности, обеспечиваемой этой Э/Э/ПЭ системой, связанной с безопасностью, во время ее нормальной работы. Если у какой-либо подсистемы Э/Э/ПЭ системы, связанной с безопасностью, отказоустойчивость аппаратных средств больше нуля, то по крайней мере один канал Э/Э/ПЭ системы, связанной с безопасностью, должен оставаться в рабочем режиме в процессе тестирования, а тестирование должно быть завершено в пределах MTTR, принятого в вычислениях для определения соответствия с целевой мерой отказов.

Примечание — Об отказоустойчивости аппаратных средств см. МЭК 61508-2, пункт 7.4.4.1.

7.7.2.3 Стандартные действия по техническому обслуживанию, которые выполняются для выявления необнаруженных отказов, должны быть выполнены на основе систематического анализа.

Примечание — Если необнаруженные отказы не выявлены, они могут:

a) в случае применения Э/Э/ПЭ систем, связанных с безопасностью, или других средств снижения риска привести к отказам при работе по запросу;

b) в случае применения систем, не связанных с безопасностью, привести к появлению запросов к Э/Э/ПЭ системам, связанным с безопасностью, или к другим средствам снижения риска.

7.7.2.4 План обслуживания Э/Э/ПЭ систем, связанных с безопасностью, должен быть согласован с теми, кто несет ответственность за будущую эксплуатацию и техническое обслуживание:

- Э/Э/ПЭ систем, связанных с безопасностью;
- других средств снижения риска;
- систем, не связанных с безопасностью, которые могут приводить к появлению запросов к системам, связанным с безопасностью, или к другим средствам снижения риска.

7.8 Планирование подтверждения соответствия всей системы безопасности

Примечания

1 Данная стадия представлена на рисунке 2 блоком 7.

2 Требования данного подраздела являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

3 Для достижения функциональной безопасности аналогичные требования необходимы для всех других мер снижения риска.

7.8.1 Цель

Целью требований настоящего подраздела является разработка плана подтверждения соответствия Э/Э/ПЭ систем, связанных с безопасностью, безопасности всей системы.

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 УО с указанием их отношения к Э/Э/ПЭ системе, связанной с безопасностью, учитывая, где это необходимо:

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

d) спецификацию Э/Э/ПЭ систем, связанных с безопасностью, которые требуют подтверждения соответствия для каждого режима работы УО 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 требований к функциям безопасности всей системы безопасности и
- спецификации требований к полноте безопасности всей системы 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 подтверждения соответствия всей системы следует учесть работы, планируемые для подтверждения соответствия безопасности Э/Э/ПЭ системы и подтверждения соответствия безопасности программного обеспечения согласно требованиям МЭК 61508-2 и МЭК 61508-3. Важно обеспечить, чтобы было учтено взаимодействие между двумя и более Э/Э/ПЭ системами, связанными с безопасностью, и прочими мерами по снижению 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 документально оформлена и должна формироваться в соответствии с планом подтверждения соответствия Э/Э/ПЭ систем, связанных с безопасностью, безопасности всей системы.

7.9 Планирование установки и ввода в эксплуатацию всей системы безопасности

Примечания

1 Данная стадия представлена на рисунке 2 блоком 8.

2 Требования данного подраздела являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

3 Для достижения функциональной безопасности аналогичные требования необходимы для всех других мер снижения риска.

7.9.1 Цели

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

7.9.2 Требования

7.9.2.1 Должен быть разработан план установки Э/Э/ПЭ 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 Э/Э/ПЭ систем, связанных с безопасностью, а также критерии для декларирования завершения установки;
- процедуры по устранению отказов и несовместимостей.

7.9.2.2 Должен быть разработан план по вводу в эксплуатацию Э/Э/ПЭ систем, связанных с безопасностью, определяющий:

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

7.9.2.3 Планирование установки и ввода в эксплуатацию всей системы безопасности должно быть документально оформлено.

7.10 Спецификация требований к Э/Э/ПЭ системе безопасности

Примечание — Данная стадия представлена на рисунке 2 блоком 9.

7.10.1 Цель

Целью требований данного подраздела является определение требований к Э/Э/ПЭ системе безопасности в терминах требований к функциям безопасности Э/Э/ПЭ системы и требований к полноте безопасности Э/Э/ПЭ системы в целях достижения необходимой функциональной безопасности.

7.10.2 Требования

7.10.2.1 Спецификация требований к Э/Э/ПЭ системе безопасности должна быть получена из распределения требований к безопасности, специфицированного в 7.6, вместе со всей соответствующей информацией, относящейся к применению. Эта информация должна быть доступна для разработчика Э/Э/ПЭ системы, связанной с безопасностью.

7.10.2.2 Спецификации требований к Э/Э/ПЭ системе безопасности должны содержать требования к функциям безопасности и к связанным с ними уровням полноты безопасности.

Примечание — Цель состоит в описании в терминах, не характерных для оборудования, функций безопасности и требуемых ими характеристик функциональной безопасности. Спецификация может быть верифицирована относительно требований ко всей системе безопасности и этапов распределения требований по всей системе безопасности, а также использоваться в качестве основы для реализации Э/Э/ПЭ системы (см. МЭК 61508-2, подраздел 7.2). Разработчики оборудования могут использовать эти спецификации в качестве основы для выбора оборудования или архитектуры.

7.10.2.3 Спецификация требований к Э/Э/ПЭ системе безопасности должна быть доступна для разработчиков Э/Э/ПЭ систем, связанных с безопасностью.

7.10.2.4 Спецификация требований к Э/Э/ПЭ системе безопасности должна быть выражена и структурирована таким образом, чтобы:

a) быть ясной, четкой, однозначной, поддающейся проверке, поддающейся тестированию, обслуживаемой и выполнимой;

b) быть понятной для тех, кто, вероятно, будет использовать эту информацию на любом этапе жизненного цикла Э/Э/ПЭ системы безопасности;

c) быть выраженной на естественном или формальном языке и/или логическом языке в виде причинно-следственных диаграмм или диаграмм влияния, чтобы определить необходимые функции безопасности, отдельно определяя каждую функцию безопасности.

7.10.2.5 Спецификация требований к Э/Э/ПЭ системе безопасности должна содержать требования к функциям безопасности Э/Э/ПЭ системы (см. 7.10.2.6) и требования к полноте безопасности Э/Э/ПЭ системы (см. 7.10.2.7).

7.10.2.6 Спецификация требований к функциям безопасности Э/Э/ПЭ системы должна содержать:

a) описание всех функций безопасности, которые необходимы для достижения требуемой функциональной безопасности, которое для каждой функции безопасности:

- обеспечивает всеобъемлющие подробные требования, достаточные для проектирования и разработки Э/Э/ПЭ систем, связанных с безопасностью;
- включает в себя то, как Э/Э/ПЭ системы, связанные с безопасностью, используются для достижения или поддержания безопасного состояния УО;
- указывает, требуется ли постоянный контроль, а также на какой период, для достижения или поддержания безопасного состояния УО, и
- указывает, применима ли функция безопасности к Э/Э/ПЭ системам, связанным с безопасностью, работающим в режиме низкой частоты запросов, высокой частоты или с непрерывным запросом;

b) значение времени отклика (т. е. время, которое необходимо для выполнения функции безопасности);

c) операторский интерфейс и интерфейс Э/Э/ПЭ системы, связанной с безопасностью, которые необходимы для достижения требуемой функциональной безопасности;

d) всю информацию, относящуюся к функциональной безопасности, которая может повлиять на проектирование Э/Э/ПЭ системы, связанной с безопасностью;

e) все интерфейсы между Э/Э/ПЭ системами, связанными с безопасностью, и другими системами (и внутри, и снаружи УО), необходимыми для функциональной безопасности;

f) все соответствующие режимы работы УО, включая:

- подготовку к использованию, включая установку и регулировку;
- запуск, обучение, автоматический, ручной, полуатоматический и установившийся режимы работы;
- стационарное нерабочее состояние, перезапуск, выключение, техническое обслуживание;
- разумно предсказуемые ненормальные условия.

Примечание — Для определенных режимов работы могут быть необходимы дополнительные функции безопасности (например, для установки, пусконаладки или технического обслуживания), чтобы обеспечить безопасность работы в этих режимах;

g) все требуемые режимы поведения Э/Э/ПЭ систем, связанных с безопасностью, должны быть определены. В особенности поведение при отказе и требуемая реакция Э/Э/ПЭ систем, связанных с безопасностью, на событие отказа (например, сигнал тревоги, автоматическое выключение и т. д.).

7.10.2.7 Спецификация требований к полноте безопасности Э/Э/ПЭ системы должна содержать:

a) уровень полноты безопасности для каждой функции безопасности и, когда необходимо, указанное значение для целевой меры отказов.

Примечания

1. Указанное значение для целевой меры отказов может быть получено при помощи количественного метода (см. 7.5.2.3). Кроме того, когда требования к полноте безопасности разработаны с использованием метода качественной оценки и выражены как уровень полноты безопасности, то целевую меру отказов при необходимости можно получить из таблицы 2 или 3, в зависимости от уровня полноты безопасности. В этом случае указанная целевая мера отказов является наименьшей средней вероятностью отказа или частотой отказа для уровня полноты безопасности, если другое значение не было использовано для калибровки метода.

2. Для функции безопасности, выполняемой в режиме с низкой частотой запросов, целевая мера отказов будет выражена в терминах средней вероятности опасного отказа по запросу, как определено уровнем полноты безопасности функции безопасности (см. таблицу 2), пока требования в спецификации требований к полноте безопасности для функции безопасности Э/Э/ПЭ системы не достигнут определенной целевой меры отказов, иной, чем конкретный УПБ. Например, если целевая мера отказов равна $1{,}5 \times 10^{-2}$ (средняя вероятность опасного отказа по запросу), т. е. заданному значению для удовлетворения требуемого допустимого риска, то вероятность отказа по запросу функции безопасности, вызванного случайными отказами аппаратных средств, должна быть равна или менее $1{,}5 \times 10^{-2}$.

3 Для функции безопасности, выполняемой в режиме с высокой частотой запросов или с непрерывным запросом, целевая мера отказов будет выражена в терминах средней частоты опасного отказа в час, как определено уровнем полноты безопасности функции безопасности (см. таблицу 3), пока требования в спецификации требований к полноте безопасности для функции безопасности Э/Э/ПЭ системы не достигнут определенной целевой меры отказов, иной, чем конкретный УПБ. Например, если целевая мера отказов равна $1{,}5 \times 10^{-6}$ (средняя частота опасного отказа в час) и задана для выполнения требований по снижению риска, то средняя частота опасного отказа функции безопасности, вызванного случайными отказами аппаратных средств, должна быть равна или менее $1{,}5 \times 10^{-6}$ опасных отказов в час;

b) режим работы (с низкой частотой запросов, с высокой частотой запросов или непрерывный запрос) каждой функции безопасности;

c) требуемый цикл и срок службы;

d) требования, ограничения, функции и средства для того, чтобы тестирование аппаратных средств Э/Э/ПЭ было выполнено.

Примечание — При разработке спецификации требований к Э/Э/ПЭ системе безопасности, должна быть принята во внимание область применения Э/Э/ПЭ систем, связанных с безопасностью. Это особенно важно для технического обслуживания, где указанный интервал проверок для конкретного применения не должен быть меньше разумно ожидаемого для области применения. Например, время между обслуживанием, которое может быть реально достигнуто для серийно выпускаемых элементов, используемых населением, вероятно, будет больше, чем в более управляемом применении;

e) экстремальные значения всех условий окружающей среды, с которыми, вероятно, встретятся Э/Э/ПЭ системы безопасности во время их жизненного цикла, включая изготовление, хранение, транспортировку, тестирование, установку, ввод в действие, работу и обслуживание;

f) пределы электромагнитной устойчивости, необходимые для достижения функциональной безопасности. Эти пределы должны быть получены с учетом и электромагнитного окружения, и требуемых уровней полноты безопасности (см. [17]).

Примечания

1 Природа и физика электромагнитных явлений не позволяют установить простую, очевидную и доказуемую связь между необходимым уровнем устойчивости и уровнем полноты безопасности почти для всех случаев электромагнитных явлений. Поэтому в таких случаях невозможно и неразумно определять эффективные уровни устойчивости исключительно по требуемому УПБ. Могут использоваться альтернативные подходы, которые до некоторой степени определяют необходимый уровень устойчивости по требуемому УПБ, но также включают специальные средства тестирования или критерии проведения испытаний. См. [17].

2 См. также [18];

g) пределы и ограничения условий для реализации Э/Э/ПЭ систем, связанных с безопасностью, в случае возможных отказов по общей причине (см. 7.6.2.7).

7.11 Реализация Э/Э/ПЭ систем, связанных с безопасностью

Примечание — Эта стадия представлена на рисунке 2 блоком 10, а также блоками 10.1 и 10.6 на рисунках 3 и 4.

7.11.1 Цель

Целью требований данного подраздела является создание Э/Э/ПЭ систем, связанных с безопасностью, в соответствии со спецификацией требований к Э/Э/ПЭ системе безопасности (включая спецификацию требований к функциям безопасности Э/Э/ПЭ системы и спецификацию требований к полноте безопасности Э/Э/ПЭ системы). (См. МЭК 61508-2 и МЭК 61508-3.)

7.11.2 Требования

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

7.12 Другие меры по снижению риска. Спецификация и реализация

Примечание — Данная стадия представлена на рисунке 2 блоком 11.

7.12.1 Цель

Целью требований настоящего подраздела является создание других мер снижения риска, удовлетворяющих требованиям к функциям безопасности и требованиям к полноте безопасности, определенным для таких систем.

7.12.2 Требования

Спецификации подлежащих выполнению требований к функциям безопасности и полноте безопасности других мер снижения риска не охватываются настоящим стандартом.

Примечание — Другие меры снижения риска основываются на технологиях, отличных от электрических/электронных/программируемых электронных (например, гидравлических, пневматических и пр.), или могут быть физическими структурами (например, дренажной системой, брандмауэром или дамбой). Они должны быть включены в жизненный цикл всей системы безопасности для обеспечения снижения рисков от Э/Э/ПЭ систем, связанных с безопасностью, определяемых в контексте снижения рисков от других мер по снижению риска.

7.13 Установка и ввод в эксплуатацию всей системы безопасности

Примечания

1 Данная стадия представлена на рисунке 2 блоком 12.

2 Требования данного пункта являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

3 Для достижения функциональной безопасности похожие требования необходимы для всех других мер по снижению риска.

7.13.1 Цели

7.13.1.1 Первой целью требований настоящего подраздела является установка Э/Э/ПЭ систем, связанных с безопасностью.

7.13.1.2 Вторая цель требований настоящего подраздела состоит в вводе в эксплуатацию Э/Э/ПЭ систем, связанных с безопасностью.

7.13.2 Требования

7.13.2.1 Действия по установке должны выполняться в соответствии с планом по установке Э/Э/ПЭ систем, связанных с безопасностью (см. 7.9).

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 эксплуатацию следует выполнять в соответствии с планом по вводу в эксплуатацию Э/Э/ПЭ 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 эксплуатацию;
- ссылки на отчеты об отказах;
- информацию об устранении отказов и несовместимости.

7.14 Подтверждение соответствия всей системы безопасности

Примечания

1 Эта стадия представлена на рисунке 2 блоком 13.

2 Требования данного пункта являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

3 Для достижения функциональной безопасности похожие требования необходимы для всех других мер по снижению риска.

7.14.1 Цель

Целью требований настоящего подраздела является подтверждение соответствия того, что Э/Э/ПЭ системы, связанные с безопасностью, удовлетворяют требованиям к безопасности всей системы, выраженным в виде требований к функциям безопасности всей системы и к полноте безопасности всей системы с учетом распределения требований по Э/Э/ПЭ 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 подтверждения соответствия Э/Э/ПЭ систем, связанных с безопасностью, безопасности всей системы (см. 7.8).

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 документальному оформлению в период подтверждения соответствия, должна включать в себя:

- документацию в хронологической форме по действиям в период подтверждения соответствия;
- использовавшуюся версию требований ко всей системе 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 документально оформлено.

7.15 Эксплуатация, техническое обслуживание и ремонт всей системы безопасности

Примечания

1 Эта стадия представлена на рисунке 2 блоком 14.

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

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

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

5 Требования данного пункта являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

6 Для достижения функциональной безопасности похожие требования необходимы для всех других мер по снижению риска.

7.15.1 Цель

7.15.1.1 Первая цель требований данного подраздела состоит в осуществлении эксплуатации, технического обслуживания и ремонта Э/Э/ПЭ систем, связанных с безопасностью, таким образом, чтобы поддерживалась требуемая функциональная безопасность.

7.15.1.2 Второй целью требований данного подраздела является обеспечение того, чтобы технические требования, необходимые для эксплуатации, технического обслуживания и ремонта всей системы безопасности, были определены для Э/Э/ПЭ систем, связанных с безопасностью, и предоставлены лицам, ответственным за будущую эксплуатацию и техническое обслуживание Э/Э/ПЭ систем, связанных с безопасностью.

7.15.2 Требования

7.15.2.1 Должно быть реализовано следующее:

- план эксплуатации и технического обслуживания Э/Э/ПЭ систем, связанных с безопасностью (см. 7.7);
- процедуры, связанные с эксплуатацией, техническим обслуживанием и ремонтом Э/Э/ПЭ систем, связанных с безопасностью.

7.15.2.2 Реализация положений, указанных в 7.15.2.1, должна включать:

- реализацию процедур;
- следование графику технического обслуживания;
- поддержание документации;
- периодическое проведение аудита функциональной безопасности (см. 6.2.7);
- документальное оформление модификаций Э/Э/ПЭ систем, связанных с безопасностью.

Примечания

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

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

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

- результаты аудитов и тестирования функциональной безопасности;
- время и причины запросов к Э/Э/ПЭ системам, связанным с безопасностью (при эксплуатации), а также характеристики Э/Э/ПЭ систем, связанных с безопасностью, при обработке этих запросов и отказов, обнаруженных при обычном обслуживании;

- документацию по модификации УО, систем управления УО и Э/Э/ПЭ систем, связанных с безопасностью.

7.15.2.4 Точные требования к хронологической документации зависят от конкретной области применения или изделия и должны быть более детально описаны в международных стандартах этой области применения или продукции.

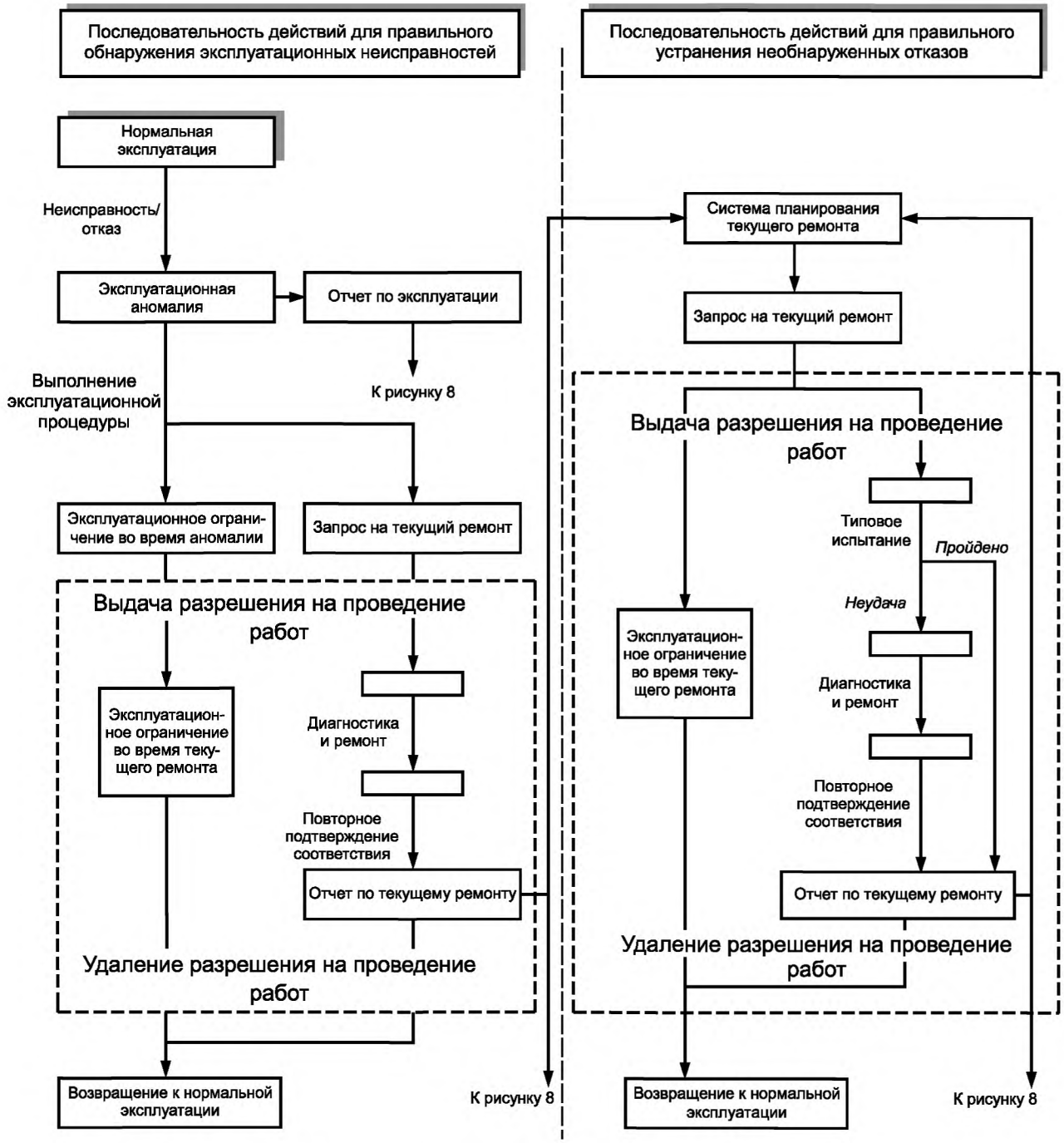
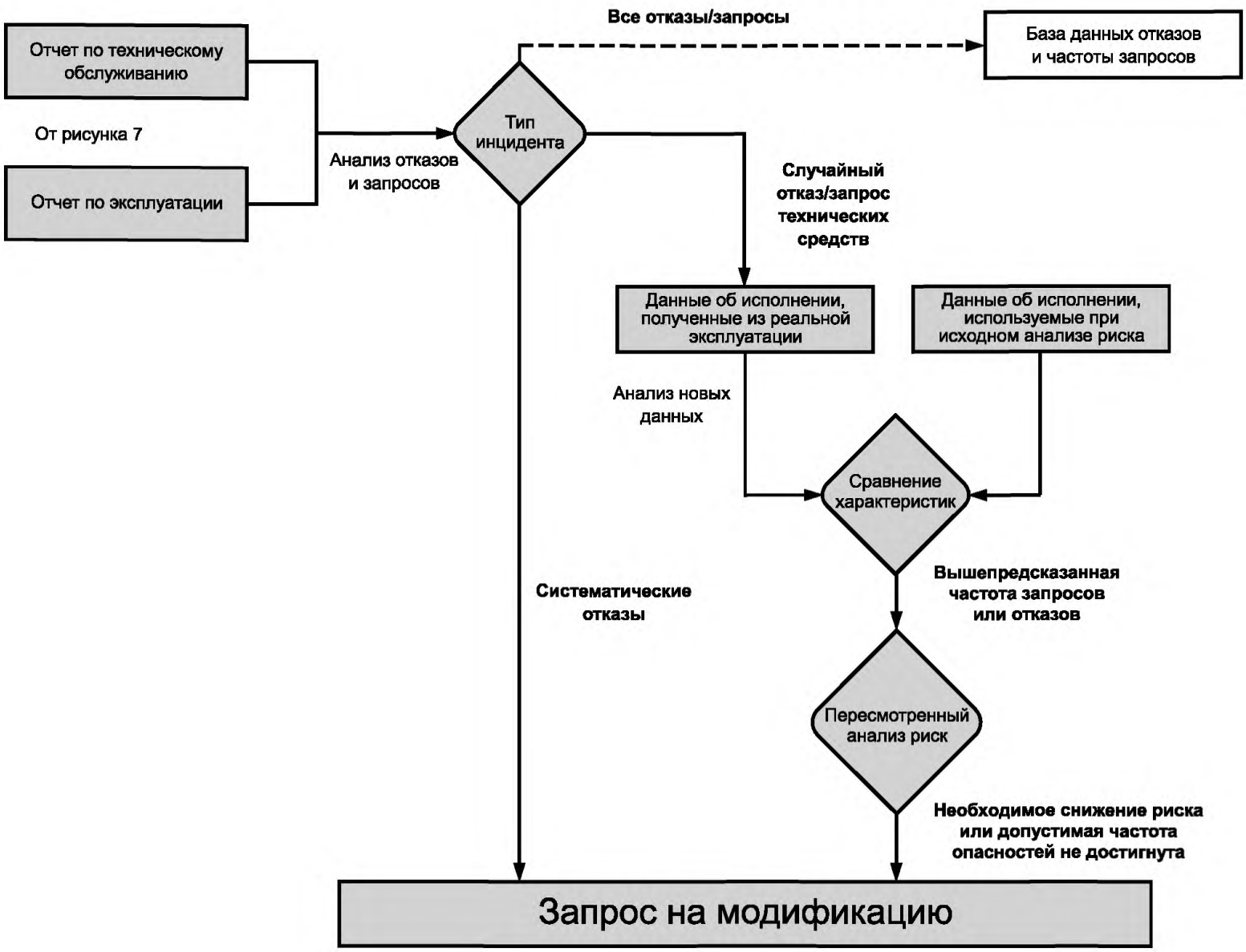


Рисунок 7 — Пример модели действий при эксплуатации и техническом обслуживании



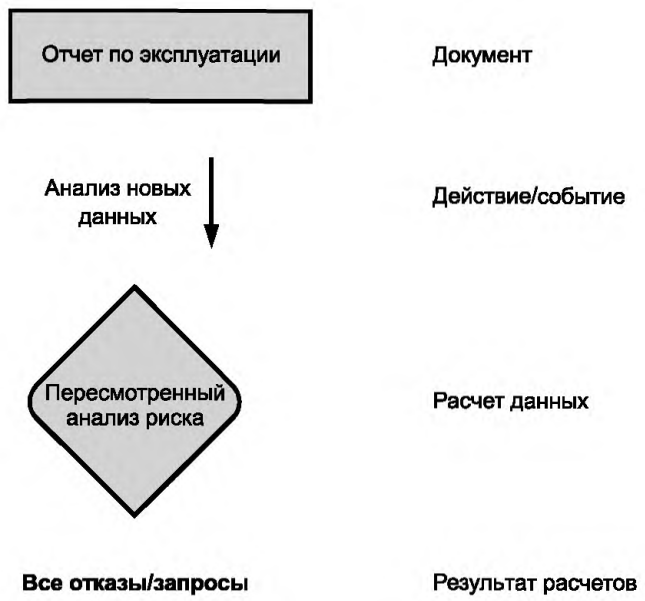


Рисунок 8 — Пример модели управления эксплуатацией и техническим обслуживанием

7.16 Модификация и изменение всей системы безопасности

Примечания

1 Данная стадия соответствует блоку 15 на рисунке 2.

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

3 Требования данного пункта являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

4 Для достижения функциональной безопасности похожие требования необходимы для всех других мер по снижению риска.

7.16.1 Цель

Цель требований настоящего подраздела состоит в том, чтобы определить процедуры, гарантирующие, что функциональная безопасность Э/Э/ПЭ 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. 6.2.8).

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. 6.2.8). 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;
- новое или измененное законодательство в области безопасности;
- модификации УО или способа его использования;
- модификации полных требований к безопасности;
- анализ эксплуатационных характеристик работы и характеристик технического 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 действий по модификации или изменениям на функциональную безопасность каждой Э/Э/ПЭ системы, связанной с безопасностью. Оценка должна включать анализ опасностей и рисков, достаточный для того, чтобы определить степень охвата и глубину последующих стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности, 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 документально оформлены.

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 Э/Э/ПЭ системы, связанной с безопасностью, должны приводить к возврату к соответствующей стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности. 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 функций безопасности, выполняемых Э/Э/ПЭ системами, связанными с безопасностью.

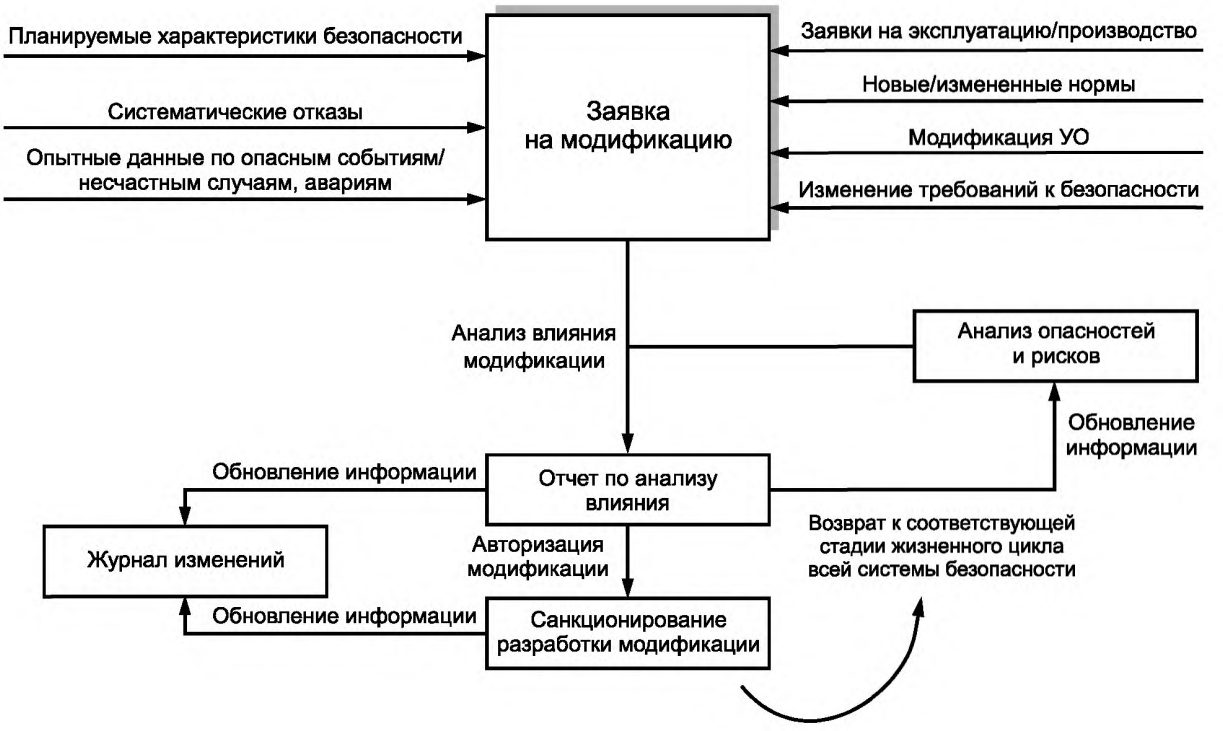


Рисунок 9 — Пример модели процедуры модификации

2 Не допускается, чтобы процедуры тестирования, разработанные для первоначальной установки и ввода в эксплуатацию, использовались без проверки подтверждения их соответствия и практической целесообразности при работе УО в неавтономном режиме.

7.16.2.7 Должна быть создана и далее поддерживаться в хронологическом порядке документация, 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 утилизация

Примечания

1 Эта стадия представлена блоком 16 на рисунке 2

2 Требования данного пункта являются специфичными для Э/Э/ПЭ систем, связанных с безопасностью. Их следует рассматривать в контексте других мер по снижению риска, в частности с учетом предположения, уже сделанного в отношении других мер по снижению риска, которые должны осуществляться в течение всего срока службы УО.

3 Для достижения функциональной безопасности похожие требования необходимы для всех других мер по снижению риска.

7.17.1 Цель

Целью требований настоящего подраздела является определение процедур, необходимых для обеспечения того, чтобы функциональная безопасность Э/Э/ПЭ систем, связанных с безопасностью, соответствовала обстоятельствам в течение и после действий по выводу из эксплуатации или утилизации УО.

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 Э/Э/ПЭ системы, связанной с безопасностью, имеющей отношение к УО, а также провести анализ влияния смежных УО и влияние на их Э/Э/ПЭ системы, связанные с безопасностью. Оценка

должна включать анализы опасностей и рисков, достаточные для определения необходимой широты и глубины охвата последующих стадий жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности.

7.17.2.2 Результаты требований, описанные в 7.17.2.1, должны быть документально оформлены.

7.17.2.3 Стадия вывода из эксплуатации или утилизации 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 утилизации должно зависеть от результатов анализа влияния.

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

- прекращению работы Э/Э/ПЭ систем, связанных с безопасностью;
- демонтажу Э/Э/ПЭ систем, связанных с безопасностью.

7.17.2.6 Если какие-либо действия по выводу из эксплуатации или утилизации оказывают влияние на функциональную безопасность любой из Э/Э/ПЭ систем, связанных с безопасностью, то должен быть инициирован возврат к соответствующей стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности. Все последующие стадии должны быть выполнены в соответствии с процедурами, определенными в настоящем стандарте для заданных уровней полноты безопасности Э/Э/ПЭ 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 функций безопасности, реализуемых Э/Э/ПЭ системами, связанными с безопасностью.

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

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

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

7.18 Верификация

7.18.1 Цель

Цель требований настоящего подраздела состоит в демонстрации для каждой стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (путем проверки, анализа и/или тестирования) того, что результаты верификации отвечают всем соответствующим целям и требованиям, определенным для этой стадии.

7.18.2 Требования

7.18.2.1 Для каждой стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности 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 и конкретной продукции. 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 собрать и документально оформить для того, чтобы засвидетельствовать, что во всех отношениях верификация завершена удовлетворительно.

8 Оценка функциональной безопасности

8.1 Цель

Целью требований настоящего раздела является определение действий, необходимых для изучения и вынесения решения по адекватности функциональной безопасности, достигнутой Э/Э/ПЭ системой(ами), связанной(ыми) с безопасностью, или применяемыми изделиями (например, элементами или подсистемами) на основе соблюдения соответствующих положений настоящего стандарта.

8.2 Требования

8.2.1 Для выполнения одной или более оценок функциональной безопасности необходимо назначить одно или более лиц, чтобы прийти к решению об адекватности:

- функциональной безопасности, достигаемой Э/Э/ПЭ системой, связанной с безопасностью в конкретной окружающей ее среде, соответствующим положениям настоящего стандарта;
- выполнения соответствующих положений настоящего стандарта элементами или подсистемами.

8.2.2 Те, кто выполняют оценку функциональной безопасности, должны иметь доступ ко всем лицам, выполняющим любые действия на всех стадиях жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности, а также ко всей информации и оборудованию (включая аппаратные средства и программное обеспечение).

Примечание — Следует признать, что лица, которые ранее участвовали в работах на различных стадиях жизненного цикла системы безопасности, не всегда доступны, поэтому ответственность должна быть возложена на лиц, в настоящее время имеющих соответствующие функции.

8.2.3 Оценку функциональной безопасности следует применять ко всем стадиям на протяжении жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, включая документацию, верификацию и управление функциональной безопасностью.

8.2.4 Лица, осуществляющие оценку функциональной безопасности, должны рассмотреть все выполняемые действия, а также все результаты, полученные в течение каждой стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности, и дать заключение о том, в какой степени выполнены цели и требования настоящего стандарта.

8.2.5 Все соответствующие заявления о соответствии, предоставленные поставщиками и другими сторонами, ответственными за достижение функциональной безопасности, должны быть включены в оценку функциональной безопасности.

Примечание — Такие заявления могут быть сделаны для действующей системы или для вклада действий и/или оборудования в функциональную безопасность на каждой стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности.

8.2.6 Оценка функциональной безопасности может выполняться после каждой стадии жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности или после нескольких стадий при условии выполнения основного требования: оценка функциональной безопасности должна осуществляться до возникновения выявленных опасностей.

8.2.7 Оценка функциональной безопасности должна включать в себя оценку доказательств того, что аудит функциональной безопасности был проведен (полностью или частично) в соответствии с его областью применения.

8.2.8 При оценке функциональной безопасности необходимо учитывать как минимум следующее:

- работы, выполненные со времени предыдущей оценки функциональной безопасности;
- планы или стратегию реализации последующих оценок функциональной безопасности для жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности;
- рекомендации предыдущих оценок функциональной безопасности и объем внесенных изменений.

8.2.9 Каждая оценка функциональной безопасности должна быть спланирована. План должен определять всю информацию, необходимую для проведения эффективной оценки, включая:

- область применения оценки функциональной безопасности;
- вовлеченные организации;
- требуемые ресурсы;

- лиц, осуществляющих оценку функциональной безопасности;
- уровень независимости лиц, выполняющих оценку функциональной безопасности;
- компетентность всех лиц, выполняющих оценку функциональной безопасности;
- выходные материалы при каждой оценке функциональной безопасности;
- как оценка функциональной безопасности соотносится и должна быть интегрирована с другими оценками функциональной безопасности в соответствующих случаях (см. 6.2.1).

Примечания

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

2 План может быть сформирован либо ответственными за оценку функциональной безопасности, либо ответственными за управление функциональной безопасностью, или его формирование может быть разделено между ними.

8.2.10 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.

8.2.11 В заключении об оценке функциональной безопасности лица, выполняющие оценку, должны документально оформить в соответствии с планами оценки и кругом полномочий:

- выполненные действия;
- полученные результаты;
- выводы;
- суждение об адекватности функциональной безопасности требованиям настоящего стандарта;
- рекомендации, вытекающие из оценки, в т. ч. рекомендации по принятию, условному принятию или отклонению.

8.2.12 Ответственным за любые действия на жизненных циклах всей системы безопасности, Э/Э/ПЭ системы безопасности или программного обеспечения системы безопасности, включая конструкторов и экспертов по Э/Э/ПЭ системам, связанным с безопасностью, должны быть доступны соответствующие результаты оценки функциональной безопасности применяемых изделий. Результаты оценки Э/Э/ПЭ системы, связанной с безопасностью, должны быть доступны для интегратора Э/Э/ПЭ системы.

Примечание — Применяемое изделие — это любое изделие (например, элемент), на которое распространяются требования серии стандартов МЭК 61508.

8.2.13 Результат оценки функциональной безопасности применяемого изделия должен включать следующую информацию для облегчения повторного использования результатов оценки для более крупной системы (см. МЭК 61508-2, приложение D, МЭК 61508-3, приложение D и МЭК 61508-4, пункт 3.8.17):

a) точное определение применяемого изделия, включая версии аппаратного и программного обеспечения.

Примечание — Если применяемое изделие рассматривается как часть более крупной системы или как семейство оборудования, то точное определение этой системы или семейства оборудования должно быть документально оформлено;

b) условия, предполагаемые в ходе оценки (например, условия использования Э/Э/ПЭ системы, связанной с безопасностью);

c) ссылку на документально оформленное доказательство, на котором основана заключительная оценка;

d) процедуры, методы и инструменты, используемые для оценки стойкости к систематическим отказам, вместе с обоснованием их эффективности;

e) процедуры, методы и инструменты, используемые для оценки полноты безопасности аппаратного обеспечения вместе с обоснованием используемого подхода и качества данных (например, интенсивность отказов или распределение источников данных);

f) оценку результатов, полученных в соответствии с требованиями настоящего стандарта и спецификации характеристик системы безопасности для применяемого изделия в соответствующем руководстве по безопасности;

g) принятые отклонения от требований МЭК 61508 с соответствующими разъяснениями и/или ссылками на доказательства, содержащиеся в документации.

8.2.14 Лица, которые осуществляют оценку функциональной безопасности, должны быть компетентными в выполняемых действиях, в соответствии с требованиями 6.2.13 — 6.2.15.

8.2.15 Минимальный уровень независимости выполняющих оценку функциональной безопасности должен соответствовать тому уровню, который указан в таблицах 4 и 5. Международные стандарты для конкретных областей применения и изделий могут определять отличные от указанных в таблицах 4 и 5 уровни независимости. Таблицы 4 и 5 следует интерпретировать следующим образом:

X: уровень независимости, определенный в качестве минимального для указанных последствий (см. таблицу 4) или уровня полноты безопасности/стойкости к систематическим отказам (см. таблицу 5). Если принят более низкий уровень независимости, то должно быть приведено подробное обоснование.

X1 и X2: см. 8.2.16.

Y: уровень независимости, определенный как недостаточный для указанных последствий (см. таблицу 4) или уровня полноты безопасности/стойкости к систематическим отказам (см. таблицу 5).

8.2.16 В контексте таблиц 4 и 5 в качестве основы для определения уровня независимости должны использоваться только X, X1, X2 и Y. Если выбраны X1 или X2, то применяется либо X1, либо X2 (но не оба вместе) в зависимости от ряда факторов, характерных для области применения. Обоснование выбора X1 или X2 должно быть подробным. Факторы, которые делают X2 более предпочтительным, чем X1 следующие:

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

Примечания

1 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 (по управлению и используемым ресурсам) от тех, которые несут ответственность за основную разработку, могут оказаться способными использовать свои собственные ресурсы, чтобы удовлетворить требованиям по независимости организации.

2 См. пункты 3.8.11, 3.8.12 и 3.8.13 МЭК 61508-4 для определения терминов «независимое лицо», «независимое подразделение» и «независимая организация» соответственно.

3 Лица, осуществляющие оценку функциональной безопасности, должны быть осторожны в предоставлении консультаций по какому-либо вопросу, связанному с оценкой, поскольку это может поставить под угрозу их независимость. Зачастую принято давать советы по различным аспектам, что может повлечь за собой решение о недостаточности безопасности, такое как недостаточность доказательств, но обычно не принято давать советы или рекомендации для конкретных средств защиты от тех или иных проблем.

8.2.17 Значения последствий для определенного уровня независимости в таблице 4 следующие:

последствие A: незначительные повреждения (например, временная потеря функции);

последствие B: серьезные увечья одному или нескольким лицам, смерть одного человека;

последствие C: смерть нескольких человек;

последствие D: смерть очень многих людей.

Указанные в таблице 4 последствия возникнут в случае выхода из строя всех мер по снижению рисков, включая Э/Э/ПЭ системы, связанные с безопасностью.

8.2.18 Минимальный уровень независимости (см. таблицу 5) должен основываться на функции безопасности, выполняемой Э/Э/ПЭ системой, связанной с безопасностью, имеющей наивысший уровень полноты безопасности для элементов/подсистем, наивысшую стойкость к систематическим отказам, определенную в терминах уровня полноты безопасности.

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

Минимальный уровень независимости	Последствие (см. 8.2.17)			
	A	B	C	D
Независимое лицо	X	X1	Y	Y
Независимое подразделение	—	X2	X1	Y
Независимая организация	—	—	X2	X
Примечание — См. 8.2.15, 8.2.16, 8.2.17 для интерпретации таблицы.				

Таблица 5 — Минимальные уровни независимости для выполняющих оценку функциональной безопасности (стадии 9 и 10 жизненного цикла всей системы безопасности, включая все стадии жизненных циклов Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности (см. рисунки 2—4))

Минимальный уровень независимости	Уровень полноты безопасности/Стойкость к систематическим отказам			
	A	B	C	D
Независимое лицо	X	X1	Y	Y
Независимое подразделение	—	X2	X1	Y
Независимая организация	—	—	X2	X
Примечание — См. 8.2.15, 8.2.16, 8.2.17 для интерпретации таблицы.				

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 жизненных циклов всей системы безопасности, Э/Э/ПЭ системы безопасности и программного обеспечения системы безопасности;
- управления функциональной безопасностью (раздел 6);
- оценки функциональной безопасности (раздел 8).

Понятие достаточности информации зависит от ряда факторов, включая сложность и размер Э/Э/ПЭ 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 Э/Э/ПЭ 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 [10].

Документ представляет собой структурированный набор информации, предназначенный для восприятия человеком, пригодный для использования в качестве единицы обмена между пользователями и/или системами [20]. 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 [20]; 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 системы безопасности

Таблицы А.1 — А.3 содержат пример структуры документации, предназначенной для структурирования информации в целях выполнения требований, указанных в разделе 5. Таблицы указывают стадии жизненного цикла

системы 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 всей системы безопасности

Стадия жизненного цикла всей системы безопасности	Информация
Концепция	Описание (концепция всей системы безопасности)
Определение области применения всей системы безопасности	Описание (определение области применения всей системы безопасности)
Анализ опасностей и рисков	Описание (анализ опасностей и рисков)
Требования ко всей системе безопасности	Спецификация (требования ко всей системе безопасности, включая: требования к функциям безопасности всей системы безопасности и требования к полноте безопасности всей системы безопасности)
Распределение требований по всей системе безопасности	Описание (распределение требований по всей системе безопасности)
Планирование эксплуатации и обслуживания всей системы безопасности	План (эксплуатация и обслуживание всей системы безопасности)
Планирование подтверждения соответствия всей системы безопасности	План (подтверждение соответствия всей системы безопасности)
Планирование установки и ввода в эксплуатацию всей системы безопасности	План (установка всей системы безопасности). План (ввод в эксплуатацию всей системы безопасности)
Требования к Э/Э/ПЭ системе безопасности	Спецификация (требования к Э/Э/ПЭ системе безопасности, включая требования к функциям безопасности Э/Э/ПЭ системы безопасности, и требования к полноте безопасности Э/Э/ПЭ системы безопасности)
Реализация Э/Э/ПЭ системы, связанной с безопасностью	См. таблицы А.2 и А.3
Установка и ввод в эксплуатацию	Отчет (установка всей системы безопасности). Отчет (ввод в эксплуатацию всей системы безопасности)
Подтверждение соответствия всей системы безопасности	Отчет (подтверждение соответствия всей системы безопасности)
Эксплуатация и техническое обслуживание всей системы безопасности	Журнал (эксплуатация и техническое обслуживание всей системы безопасности)

Окончание таблицы А.1

Стадия жизненного цикла всей системы безопасности	Информация
Модификация и изменения всей системы безопасности	Запрос (модификация всей системы безопасности). Отчет (анализ влияния модификации и изменений всей системы безопасности). Журнал (модификация и изменения всей системы безопасности)
Вывод из эксплуатации и ликвидация	Отчет (анализ влияния вывода из эксплуатации или ликвидации всей системы безопасности). План (вывод из эксплуатации или ликвидация всей системы безопасности). Журнал (вывод из эксплуатации или ликвидация всей системы безопасности)
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 Э/Э/ПЭ системы безопасности

Стадия жизненного цикла Э/Э/ПЭ системы безопасности	Информация
Планирование подтверждения соответствия Э/Э/ПЭ системы	План (подтверждение соответствия Э/Э/ПЭ системы безопасности)
Проектирование и создание Э/Э/ПЭ системы. Архитектура Э/Э/ПЭ системы.	Описание (проект архитектуры Э/Э/ПЭ системы, включая: архитектуру аппаратных средств и архитектуру программного обеспечения). Спецификация (комплексные испытания программируемой электроники). Спецификация (комплексные испытания программируемых электронных и непрограммируемых электронных устройств).
Архитектура аппаратных средств.	Описание (проект архитектуры аппаратных средств). Спецификация (комплексные испытания архитектуры аппаратных средств).
Разработка аппаратных модулей.	Спецификация (проект аппаратных модулей). Спецификации (испытания аппаратных модулей).
Конструирование и/или приобретение компонентов	Аппаратные модули. Отчет (проверки аппаратных модулей)
Интеграция программируемой электроники	Отчет (комплексные испытания программируемой электроники и программного обеспечения) (см. таблицу А.3)
Интеграция Э/Э/ПЭ системы	Отчет (комплексные испытания программируемой электроники и других аппаратных средств)
Процедуры эксплуатации и технического обслуживания Э/Э/ПЭ системы	Инструкция (пользователя). Инструкция (эксплуатация и техническое обслуживание)
Подтверждение соответствия безопасности Э/Э/ПЭ системы	Отчет (подтверждение соответствия безопасности Э/Э/ПЭ системы)
Модификация Э/Э/ПЭ системы	Инструкция (процедуры модификации Э/Э/ПЭ системы). Запрос (модификация Э/Э/ПЭ системы). Отчет (анализ влияния модификации Э/Э/ПЭ системы). Журнал (модификация Э/Э/ПЭ системы)

Окончание таблицы А.2

Стадия жизненного цикла Э/Э/ПЭ системы безопасности	Информация
Относится ко всем стадиям	План (для Э/Э/ПЭ системы безопасности) План (верификация Э/Э/ПЭ системы). Отчет (верификация Э/Э/ПЭ системы). План (оценка функциональной безопасности Э/Э/ПЭ системы). Отчет (оценка функциональной безопасности Э/Э/ПЭ системы)
Относится ко всем соответствующим стадиям	Руководство по безопасности для поставляемых изделий

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

Стадия жизненного цикла ПО системы безопасности	Информация
Требования к ПО системы безопасности	Спецификация (требования к ПО системы безопасности, включая требования к функциям безопасности ПО и к полноте безопасности ПО)
Планирование подтверждения соответствия ПО	План (подтверждение соответствия ПО системы безопасности)
Проектирование и создание ПО. Архитектура ПО. Разработка системы ПО. Разработка программных модулей. Кодирование. Тестирование программных модулей. Интеграция ПО	Описание (проект архитектуры ПО) (описание проекта архитектуры аппаратных средств см. в таблице А.2). Спецификация (комплексные испытания архитектуры ПО). Спецификация (комплексные испытания программи-руемой электроники и ПО). Инструкция (средства разработки и руководство по кодированию). Описание (проект системы ПО). Спецификация (комплексные испытания системы ПО). 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 системы ПО). Отчет (комплексные испытания архитектуры ПО)
Интеграция программируемой электроники	Отчет (комплексные испытания программируемой электроники и ПО)
Процедуры эксплуатации и сопровождения ПО	Инструкция (пользователя) Инструкция (по эксплуатации и сопровождению)
Подтверждение соответствия ПО системы безопасности	Отчет (подтверждение соответствия ПО системы безопасности)
Модификация ПО	Инструкция (процедуры модификации ПО). Запрос (модификация ПО). Отчет (анализ влияния модификации ПО). Журнал (модификация ПО)
Относится ко всем стадиям	План (для ПО системы безопасности). План (верификация ПО). Отчет (верификация ПО). План (оценка функциональной безопасности ПО). Отчет (оценка функциональной безопасности ПО)
Относится ко всем соответствующим стадиям	Руководство по безопасности для поставляемых изделий

А.3 Физическая структура документа

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

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 на 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 рисунке А.1. Например, в инженерном комплекте могут содержаться такие документы, как описание анализа опасностей и рисков, а также спецификация требований ко всей системе безопасности.

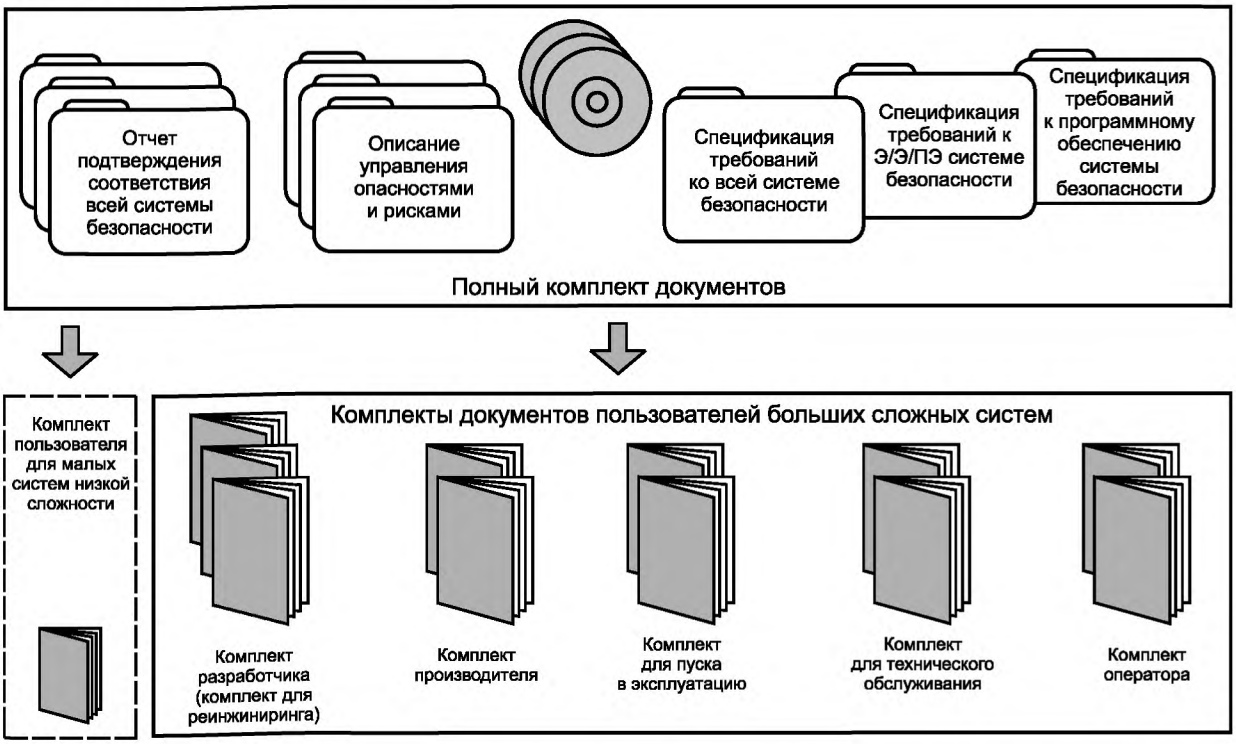


Рисунок А.1 — Структурирование информации в наборы документов для групп пользователей

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 ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898—2002 «Аспекты безопасности. Правила включения в стандарты»
МЭК Руководство 104:1997	—	*
МЭК 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
МЭК 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
МЭК 61508-3:2010	IDT	ГОСТ Р МЭК 61508-4— 2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»

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

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

- IDT — идентичные стандарты.

Библиография

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

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

[3] IEC 61800-5-2, Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional

[4] ISO/IEC/TR 19791, Information technology — Security techniques — Security assessment of operational systems

[5] IEC 62443(all parts), Industrial communication networks — Network and system security

[6] IEC 60601 (all parts), Medical electrical equipment

[7] IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels

[8] IEC 61508-6:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

[9] IEC 61508-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures

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

[11] Managing Competence for Safety-Related Systems, IET/BCS/HSE, 2007; (Part 1: Key guidance; Part 2 Supplementary material). HSE. 2007

[12] IEC 60300-3-1:2003, Dependability management — Part 3—1: Application guide — Analysis techniques for dependability — Guide on methodology

[13] IEC 61882:2001, Hazard and operability studies (HAZOP studies) — Application guide

[14] IEC 60300-3-9:1995, Dependability management — Part 3: Application guide — Section 9: Risk analysis of technological systems

[15] NUREG/CR-4780, Volume 1, January 1988, Procedures for treating common cause failures in safety and reliability studies — Procedural framework and examples

[16] NUREG/CR-4780, Volume 2, January 1989, Procedures for treating common cause failures in safety and reliability studies — Analytical background and techniques

[17] IEC/TS 61000-1-2, Electromagnetic compatibility (EMC) — Part 1—2: General — Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena

[18] IEC 61326-3-1, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — General industrial applications

[19] ISO 8613-1:1994, Information technology — Open Document Architecture (ODA) and Interchange Format: Introduction and general principles

[20] IEC 61355 (all parts), Classification and designation of documents for plants, systems and equipment

УДК 62-783:614.8:331.454:006.354 ОКС 25.040, 13.110, 29.020 Группа 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 *Т.С. Никифорова*
Технический редактор *А.И. Белов*
Корректор *Е.М. Бородулина*
Компьютерная верстка *А.С. Шаповаловой*

Сдано в набор 18.03.2014. Подписано в печать 07.04.2014. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 5.21. Тираж 71 экз. Зак. 2135.

Набрано в Издательском доме «Вебстер»
gost.e-ecolog.ru gost.e-ecolog.ru
Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru