ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р МЭК 61508-5— 2007**

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

## Часть 5

## Рекомендации по применению методов определения уровней полноты безопасности

IEC 61508-5:1998
Functional safety of electrical/electronic/programmable electronic safety-related systems —
Part 5: Examples of methods for the determination of safety integrity levels
(IDT)

Издание официальное

БЗ 3—2006/39

Москва
Стандартинформ
2008

gost.e-ecolog.ru

## Предисловие

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

**Сведения о стандарте**

1 ПОДГОТОВЛЕН обществом с ограниченной ответственностью «Корпоративные электронные системы» и Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков» на основе собственного аутентичного перевода стандарта, указанного в пункте 4

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

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

4 Настоящий стандарт идентичен международному стандарту МЭК 61508-5:1998 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности» (IEC 61508-5:1998 «Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5. Examples of methods for the determination of safety integrity levels», IDT).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2008

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

## Содержание

1 Область применения . . . . . 1
2 Нормативные ссылки . . . . . 3
3 Термины и определения . . . . . 3
Приложение A (обязательное) Риск и полнота безопасности. Основные концепции . . . . . 4
Приложение B (обязательное) ALARP и концепции допустимого риска . . . . . 9
Приложение C (обязательное) Определение уровней полноты безопасности: количественный метод . . . . . 12
Приложение D (обязательное) Определение уровней полноты безопасности. Качественный метод: графы риска . . . . . 14
Приложение E (обязательное) Определение уровней полноты безопасности. Количественный метод: матрица тяжести опасных событий . . . . . 18
Приложение F (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . . . 20
Библиография . . . . . 21

# Введение

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

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

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

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

Настоящий стандарт:

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

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

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

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

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

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

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

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

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

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

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

## Часть 5

## Рекомендации по применению методов определения уровней полноты безопасности

Functional safety of electrical, electronic, programmable electronic safety-related systems.
Part 5. Guidelines for methods of the determination of safety integrity levels

**Дата введения — 2008—06—01**

## 1 Область применения

1.1 Настоящий стандарт предоставляет информацию:

- о концепциях, лежащих в основе понятия риска, а также о связи риска и полноты безопасности (приложение А);
- о ряде методов, позволяющих определить уровни полноты безопасности для E/E/PE систем, связанных с безопасностью, основанных на других технологиях, и для внешних средств снижения риска (приложения В, С, D и Е).

1.2 Выбор метода зависит от области применения и от конкретных обстоятельств. Приложения В, С, D и Е иллюстрируют количественный и качественный подходы с некоторыми упрощениями, позволяющими продемонстрировать основные принципы. Эти приложения были включены для того, чтобы продемонстрировать общие принципы нескольких методов, они не дают полного описания этих методов. Те, кто собирается использовать методы, указанные в приложениях, должны обратиться к рекомендуемым источникам.

Примечание — Более подробная информация, описанная в приложениях В, D и Е, приведена соответственно в [4], [2] и [3]. Еще один подход описан в [5].

1.3 МЭК 61508-1 — МЭК 61508-4 являются основополагающими стандартами по безопасности, хотя этот статус не применим в контексте E/E/PE систем, связанных с безопасностью, имеющих низкую сложность [МЭК 61508-4 (пункт 3.4.4)]. В качестве основных стандартов по безопасности они предназначены для использования техническими комитетами при подготовке стандартов в соответствии с требованиями МЭК Руководство 104 и ИСО/МЭК Руководство 51. Одной из обязанностей технического комитета является использование, где это возможно, основных стандартов по безопасности при подготовке своих собственных стандартов. МЭК 61508 предназначен также и для использования в качестве отдельного стандарта.

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

1.4 На рисунке 1 показана общая структура частей МЭК 61508-1 — МЭК 61508-7 и указана роль, которую играет МЭК 61508-5 в достижении функциональной безопасности E/E/PE систем.

**Издание официальное**

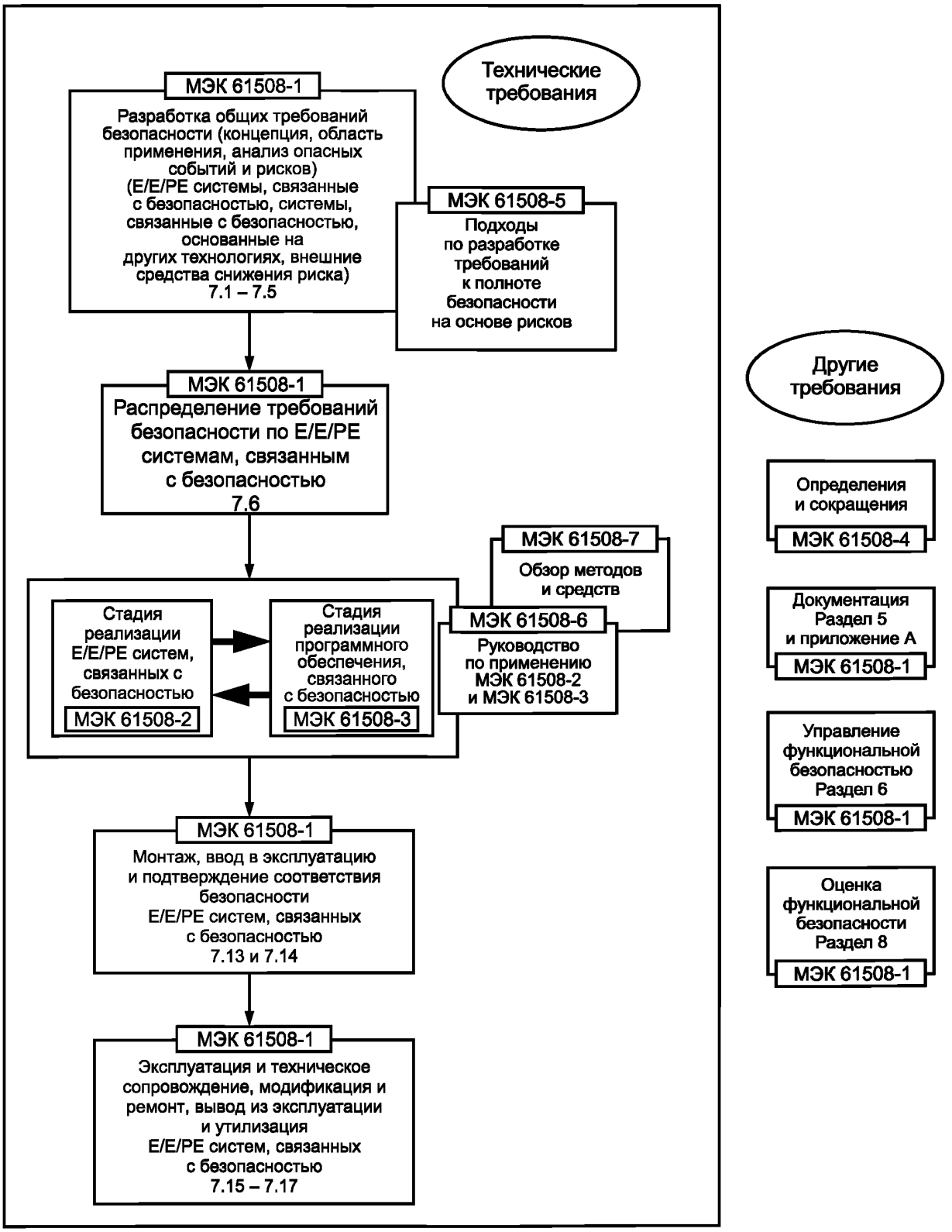



Рисунок 1 — Общая структура настоящего стандарта

## 2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

МЭК 61508-1:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

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

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

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

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

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

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

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

## 3 Термины и определения

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

**Приложение А**
**(обязательное)**

## Риск и полнота безопасности. Основные концепции

### А.1 Общие положения

Настоящее приложение предоставляет информацию о концепциях, лежащих в основе понятия риска, а также о связи между риском и полнотой безопасности.

### А.2 Требуемое уменьшение риска

Требуемое уменьшение риска [МЭК 61508-4 (пункт 3.5.14)] представляет собой уменьшение риска, необходимое для того, чтобы риск в конкретной ситуации стал допустимым (что может быть установлено с помощью качественных[1)] или количественных методов[2)]). Понятие требуемого уменьшения риска имеет фундаментальное значение при разработке спецификаций требований к E/E/PE системам, связанных с безопасностью (в частности той части спецификации, которая посвящена требованиям к полноте безопасности). Цель определения допустимого риска для конкретного опасного события состоит в том, чтобы сформулировать разумные критерии для частоты (или вероятности) опасного события и его последствий. Системы, связанные с безопасностью, предназначены для того, чтобы уменьшить частоту (или вероятность) опасных событий и/или последствия опасных событий.

Допустимый риск зависит от многих факторов (например, от тяжести травм, числа людей, подвергающихся опасности, от того, насколько часто человек или люди подвергаются опасности, а также от периода времени, в течение которого люди подвергаются опасности). К числу важных факторов относятся осознание опасности и отношение к ней тех, кто подвергается действию опасного события. При выработке мнения о том, что представляет собой допустимый риск для конкретного приложения, учитываются:

- руководящие указания органов власти, осуществляющих регулирование в области безопасности;
- обсуждения и соглашения между различными сторонами, участвующими в конкретной области применения;
- промышленные стандарты и руководства;
- международные обсуждения и соглашения; роль национальных и международных стандартов в выработке критериев для определения допустимого риска становится все более важной;
- лучшие независимые промышленные, экспертные и научные рекомендации консультативных органов;
- законодательные требования как общие, так и те, которые непосредственно относятся к конкретной области применения.

### А.3 Роль E/E/PE систем безопасности

E/E/PE системы, связанные с безопасностью, способствуют достижению требуемого уменьшения риска, делающего его допустимым. Системы, связанные с безопасностью:

- реализуют функции безопасности, необходимые для достижения или поддержания безопасного состояния управляемого оборудования, и
- используя собственные средства, или в совокупности с другими E/E/PE системами, связанными с безопасностью, с системами, связанными с безопасностью, основанными на других технологиях, или с внешними средствами уменьшения риска достигают необходимой полноты безопасности для требуемых функций [МЭК 61508-4 (пункт 3.4.1)].

Примечания

1 В первом перечислении отмечается, что система, связанная с безопасностью, должна выполнять функции, которые могут быть определены в спецификациях требований к функциям безопасности. Например, спецификация требований к функциям безопасности может содержать требование о том, что, когда температура достигает значения *x*, должен открываться клапан *y*, который позволяет воде поступать в сосуд.

2 Во втором перечислении отмечается, что функции безопасности должны выполняться системами, связанными с безопасностью, со степенью надежности, достаточной для достижения в конкретной области применения допустимого риска.

В состав E/E/PE системы, связанные с безопасностью, могут входить люди. Например, человек может получать с экрана дисплея информацию о состоянии EUC и выполнять действия, основываясь на этой информации. E/E/PE системы, связанные с безопасностью, могут работать в режиме низкой интенсивности запросов либо в режиме высокой интенсивности запросов или непрерывных запросов [МЭК 61508-4 (пункт 3.5.12)].

---

[1)] При достижении приемлемого риска должно быть установлено требуемое уменьшение риска. В приложениях D и E описываются качественные методы, хотя в приведенных примерах требуемое уменьшение риска содержится в неявном виде и не формулируется явно.

[2)] Например, что опасное событие, ведущее к конкретному последствию, не должно происходить с частотой, превышающей один раз за $10^8$ час.

### А.4 Полнота безопасности

Полнота безопасности определяется как вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех установленных условиях в течение установленного периода времени [МЭК 61508-4 (пункт 3.5.2)]. Полнота безопасности относится к характеристикам, описывающим способность систем, связанных с безопасностью, выполнять функции безопасности, которые должны быть определены в спецификации требований к функциям безопасности.

Считается, что полнота безопасности должна рассматриваться как состоящая из двух элементов:

- полноты безопасности аппаратуры; эта часть полноты безопасности связана со случайными отказами аппаратуры, проявляющимися в опасном режиме [МЭК 61508-4 (пункт 3.5.5)]. Достижение заданного уровня полноты безопасности аппаратуры, предназначенной для обеспечения безопасности, может быть оценено с разумной степенью точности, следовательно, требования могут быть распределены между подсистемами в соответствии с нормальными законами для вероятностей совместных событий. Для достижения адекватной полноты безопасности аппаратуры может потребоваться использование избыточной архитектуры;

- полноты безопасности, связанной с систематическими отказами; эта часть полноты безопасности обусловлена систематическими отказами, проявляющимися в опасном режиме [МЭК 61508-4 (пункт 3.5.4)]. Хотя средняя интенсивность систематических отказов может поддаваться оценке, данные, полученные из анализа конструктивных отказов и отказов с общей причиной, свидетельствуют о том, что распределение отказов спрогнозировать трудно. Это приводит к увеличению неопределенности расчетов вероятности отказов для конкретной ситуации (например, вероятности отказа системы защиты). Поэтому необходимо выбирать методы, которые минимизируют эту неопределенность. Следует учитывать, что мероприятия по уменьшению вероятности случайных отказов аппаратуры не всегда приводят к уменьшению вероятности систематических отказов. Такие методы, как избыточные каналы идентичной аппаратуры, очень эффективные для регулирования случайных отказов аппаратуры, мало влияют на уменьшение систематических отказов.

Уровень полноты безопасности E/E/PE систем, связанных с безопасностью, систем, связанных с безопасностью, основанных на других технологиях, и внешних средств уменьшения риска должен гарантировать, что:

- частота отказов систем, связанных с безопасностью, будет достаточно низкой, чтобы предотвратить превышение частоты опасных событий, соответствующей допустимому риску и/или, что

- системы, связанные с безопасностью, изменяют последствия отказов в такой степени, что риск становится допустимым.

На рисунке А.1 представлены основные концепции, связанные с уменьшением риска. В общей модели предполагается, что:

- имеется EUC и система управления EUC;
- имеются факторы, связанные с человеком;
- средства защиты включают в себя:
  внешние средства уменьшения риска,
  E/E/PE системы, связанные с безопасностью,
  системы, связанные с безопасностью, основанные на других технологиях.

Примечание — На рисунке А.1 представлена обобщенная модель риска, предназначенная для демонстрации основных принципов. Модель риска для конкретного приложения должна разрабатываться с учетом конкретного способа, которым будет достигаться требуемое уменьшение риска E/E/PE системами, связанными с безопасностью, системами, связанными с безопасностью, основанными на других технологиях, и внешними средствами уменьшения риска. Поэтому итоговая модель риска может отличаться от модели, представленной на рисунке А.1.

В число рисков, представленных на рисунке А.1, входят:

- риск EUC: риск определенных опасных событий, связанных с EUC, с системами управления EUC и с человеческим фактором — при определении этого риска не учитываются планируемые средства защиты [МЭК 61508-4 (пункт 3.2.4)];

- допустимый риск: риск, который допустим в заданном контексте в соответствии с существующими в обществе ценностями [МЭК 61508-4 (пункт 3.1.6)];

- остаточный риск: риск заданных опасных событий, связанных с EUC, системой управления EUC, факторами, зависящими от человека, который сохраняется после добавления внешних средств уменьшения риска, E/E/PE систем, связанных с безопасностью, и систем, связанных с безопасностью, основанных на других технологиях [МЭК 61508-4 (пункт 3.1.7)].

Риск EUC зависит от факторов риска, создаваемых непосредственно EUC, а также от снижения риска, обеспечиваемого системой управления EUC. Чтобы предотвратить появление необоснованных оценок полноты безопасности для систем управления EUC, настоящий стандарт ограничивает такие оценки [МЭК 61508-1 (пункт 7.5.2.5)].

Требуемое уменьшение риска достигается объединением всех мер увеличения безопасности. На рисунке А.1 показано уменьшение риска от исходного уровня, соответствующего риску EUC, до уровня, отвечающего заданному допустимому риску.




Рисунок А.1 — Уменьшение риска: основные понятия

### А.5 Риск и полнота безопасности

Важно понимать различие между риском и полнотой безопасности. Риск представляет собой меру вероятности и одновременно меру тяжести последствий заданного опасного события. Он может быть оценен для различных ситуаций [риск EUC, риск, допустимый риск, остаточный риск (см. рисунок А.1)]. Понятие допустимого риска определяется на социальной основе, оно учитывает социальные и политические факторы. Понятие полноты безопасности применяется только к E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам уменьшения риска. Полнота безопасности представляет собой оценку вероятности того, что рассматриваемые системы/средства обеспечат требуемое уменьшения риска для функций безопасности. Однажды установленный допустимый риск и оцененное необходимое сокращение риска позволяют распределить требования к полноте безопасности систем, связанных с безопасностью [МЭК 61508-4 (пункты 7.4 — 7.6)].

Примечание — Для того чтобы получить оптимальную систему, связанную с безопасностью, удовлетворяющую различным требованиям, распределение должно быть итеративным.

Роль систем, связанных с безопасностью, в достижении требуемого уменьшения риска показана на рисунках А.1 и А.2.

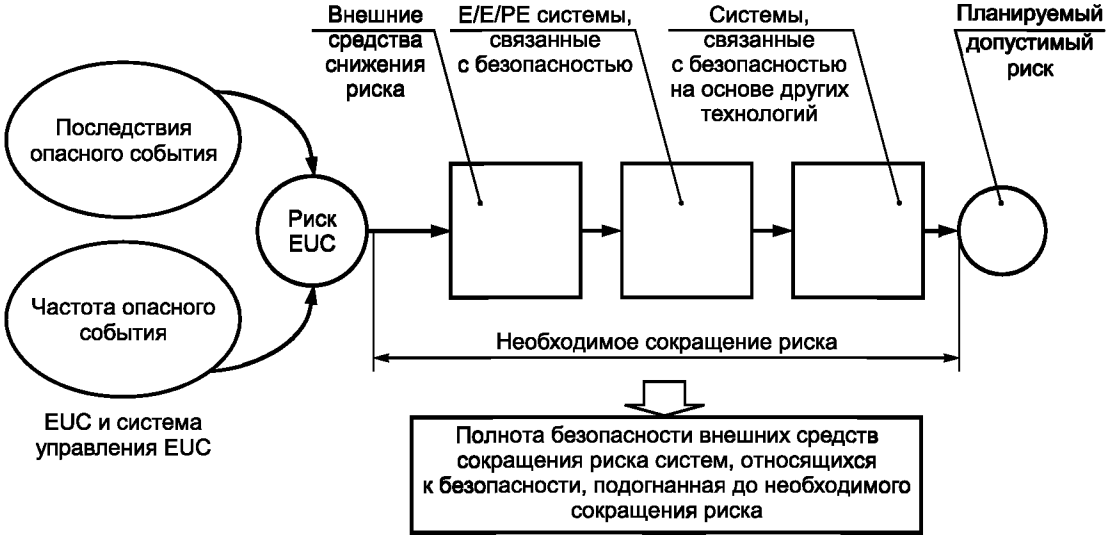



Рисунок А.2 — Понятия риска и полноты безопасности

### А.6 Уровни полноты безопасности и уровни полноты безопасности программного обеспечения

Для удовлетворения широкого диапазона необходимых снижений риска, которые должны обеспечивать системы, связанные с безопасностью, целесообразно иметь в распоряжении ряд уровней безопасности в качестве мер для удовлетворения требований полноты безопасности функций безопасности, распределенных по системам, связанным с безопасностью. Уровни полноты безопасности программного обеспечения используются как база для спецификации требований полноты безопасности функций безопасности, выполняемых программным обеспечением, связанным с безопасностью. Спецификация требований к полноте безопасности должна определять уровни полноты безопасности для E/E/PE систем, связанных с безопасностью.

В настоящем стандарте определены четыре уровня полноты безопасности, наивысшим является уровень 4, наиболее низким — уровень 1.

Количественные характеристики интенсивности отказов для четырех уровней полноты безопасности приведены в МЭК 61508-1 (таблицы 2 и 3). Определены два параметра, один — для систем, связанных с безопасностью, работающих в режиме низкой интенсивности запросов, другой — для систем, связанных с безопасностью, работающих в режиме высокой интенсивности запросов или в непрерывном режиме.

Примечание — Для систем, связанных с безопасностью, работающих в режиме низкой интенсивности запросов, в качестве меры полноты безопасности представляет интерес вероятность отказов выполнения функций безопасности по запросам. Для систем, действующих в режиме высокой частоты запросов, или с непрерывными запросами, в качестве меры полноты безопасности представляет интерес средняя вероятность отказов в час [МЭК 61508-4 (пункты 3.5.12 и 3.5.13)].

### А.7 Распределение требований безопасности

Распределение требований безопасности (как требований к функциям безопасности, так и требований к полноте безопасности), предъявляемых к E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам уменьшения риска показано на рисунке А.3, который идентичен рисунку 6 в МЭК 61508-1. Требования по распределению требований безопасности по фазам приведены в МЭК 61508-1 (пункт 7.6).

Методы, используемые для распределения требований полноты безопасности по E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и внешним средствам снижения риска, зависят, в первую очередь, от того, задается ли требуемое снижение риска явно в количественной или в качественной форме. Эти подходы получили названия соответственно количественного и качественного методов (приложения В — Е).

Примечания

1 Требования к полноте безопасности связываются с каждой функцией безопасности до распределения [МЭК 61508-1 (пункт 7.5.2.6)].

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

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

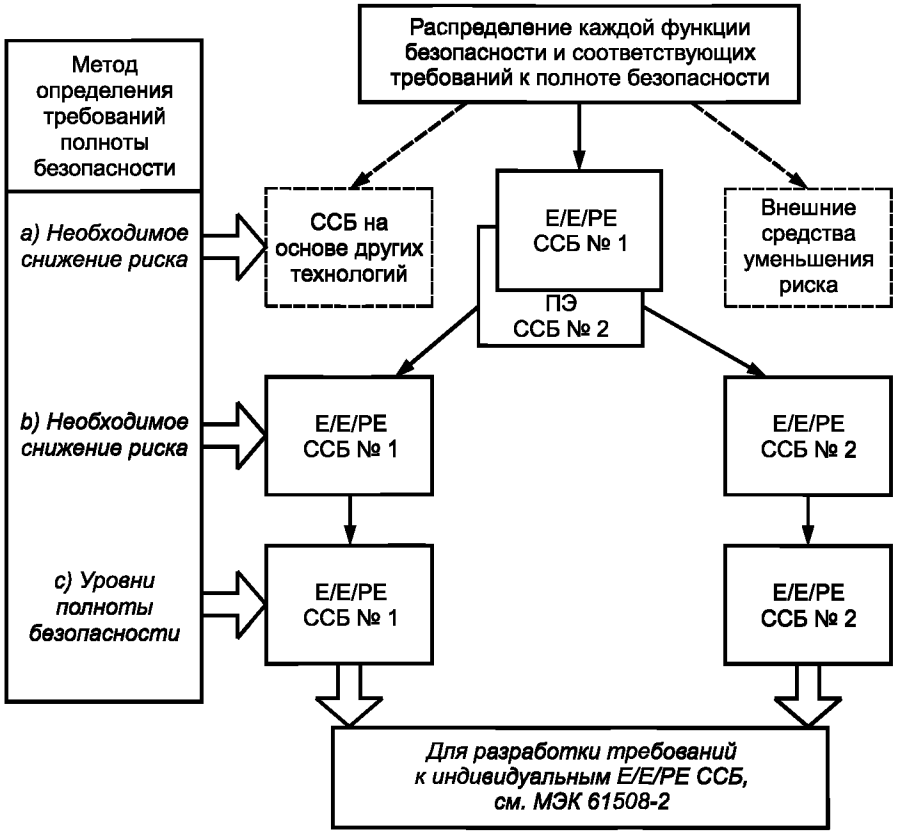



Рисунок А.3 — Распределение требований безопасности по E/E/PE системам, связанным с безопасностью, системам, связанным с безопасностью, основанных на других технологиях, и внешним средствам снижения риска

**Приложение В**
**(обязательное)**

# ALARP и концепции допустимого риска

## В.1 Общие положения

В настоящем приложении рассматривается один частный подход к достижению допустимого риска. В приложении нет подробного описания метода, даны только основные принципы. Тем, кто собирается применять методы, описываемые в настоящем приложении, рекомендуется обратиться к источникам [1] — [5].

## В.2 Модель ALARP

### В.2.1 Введение

В А.2 описаны основные проверки, применяемые при управлении промышленными рисками, и выполнение которых определенно показывает:

a) является ли риск настолько большим, что он должен быть отвергнут полностью, или

b) риск является (или может быть сделан) столь малым, что может считаться незначительным, или

c) риск попадает в промежуток между двумя категориями, определенными в перечислениях a) и b), и уменьшается до самого низкого реального уровня с учетом полученных от этого выгод и учетом затрат на любое дальнейшее его снижение.

Что касается перечисления c), принцип ALARP требует, чтобы любой риск был уменьшен настолько (или до столь низкого уровня), насколько это практически осуществимо (последняя фраза на английском языке «as low as reasonably practicable» и образует аббревиатуру ALARP). Если риск находился между областью недопустимого риска и областью допустимого риска и был использован принцип ALARP, то результирующий риск является допустимым риском для конкретного приложения. Такой подход, использующий три области, показан на рисунке В.1.

Риск, превышающий определенный уровень, считается недопустимым и не может быть оправдан при обычных обстоятельствах.

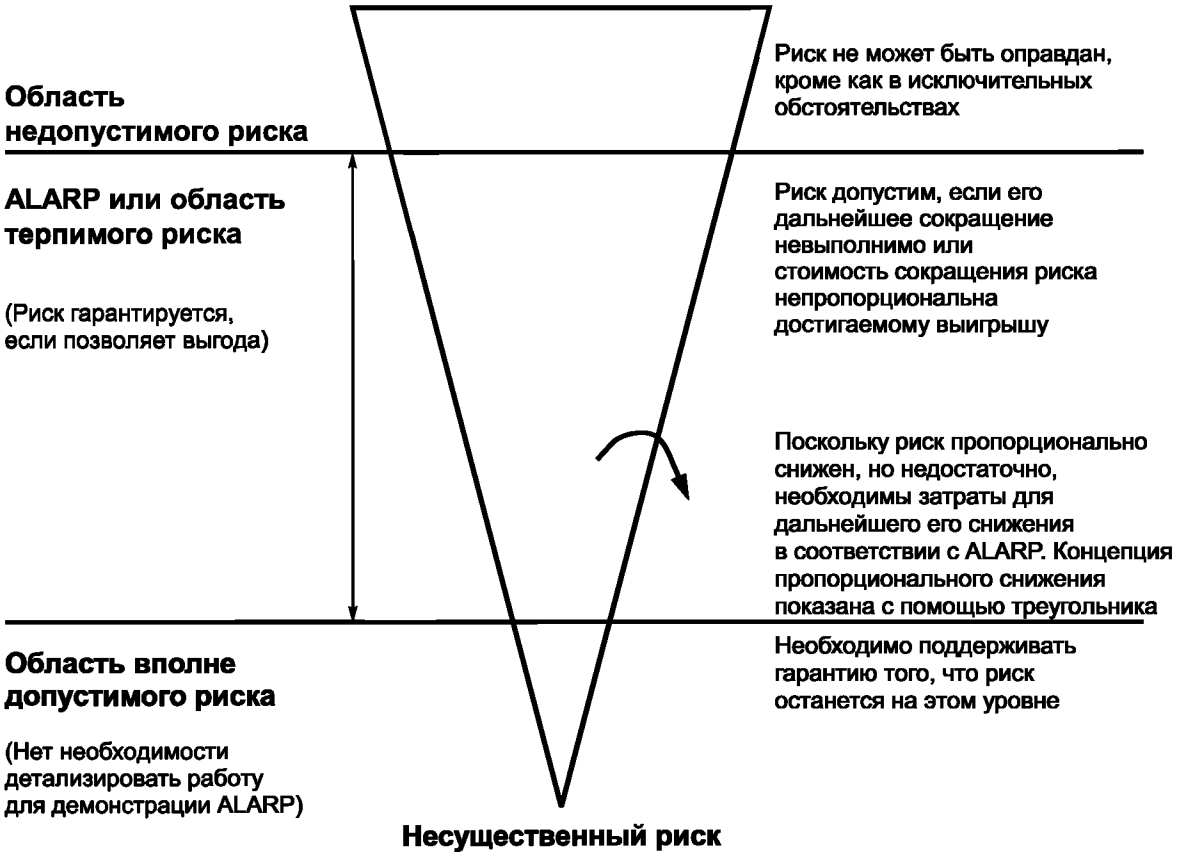



Рисунок В.1 — Допустимый риск и ALARP

Ниже этого уровня находится область терпимого риска, в которой деятельность может производиться при условии, что риски будут сделаны настолько малыми, насколько это практически возможно. Терпимый риск отличается от допустимого риска: он указывает готовность мириться с риском, поскольку это приносит определенные выгоды, в то же самое время надеясь на то, что риск будет находиться под наблюдением и будет уменьшен, как только это станет возможным. В этой ситуации требуется оценка стоимости выгод, которая может быть явной или неявной, позволяющая определить стоимость и необходимость дополнительных мер безопасности. Чем выше риск, тем более высоких затрат следует ожидать для его снижения. На границе области терпимого риска затраты оказываются в большой диспропорции по отношению к ожидаемым выгодам. В этой зоне риск по определению будет значительным, и беспристрастный анализ говорит о том, что даже для достижения минимально необходимого уменьшения риска потребуются значительные усилия.

Там, где риск является менее значительным, на его снижение потребуются меньшие затраты, и на другом краю области терпимого риска баланс между затратами и выгодами может оказаться удовлетворительным.

Ниже области терпимого риска уровни риска считаются настолько незначительными, что их дальнейшего снижения не требуется. Это область общей допустимости, для которой риски являются малыми в сравнении с повседневными рисками. В области общей допустимости не требуется детальной проработки для демонстрации ALARP; однако требуется сохранять бдительность для того, чтобы риск оставался на данном уровне.

Концепция ALARP может быть использована тогда, когда приняты качественные или количественные планы для риска. В В.2.2 описан метод количественной оценки риска. (В приложении С описывается количественный метод, а в приложениях D и Е — качественные методы определения требуемого уменьшения риска для конкретной опасности; указанные методы могут включать концепцию ALARP на стадии принятия решений).

Примечание — Более подробная информация об ALARP приведена в [4].

**В.2.2 Планируемый допустимый риск**

Один из путей получения плана допустимого риска состоит в том, что для ряда последствий, которые должны быть определены, назначаются допустимые для них частоты. Такое согласование последствий и допустимых частот достигается обсуждением и выработкой соглашения между заинтересованными сторонами (например, органами, осуществляющими техническое регулирование в области безопасности, теми, чья деятельность является источником рисков, и теми, кто подвергается действию рисков).

С учетом концепции ALARP связь последствий с допустимыми частотами может быть получена путем использования классов рисков. Примером является таблица В.1, где показаны четыре класса рисков (I, II, III, IV) для ряда последствий и частот. В таблице В.2 каждый класс рисков интерпретируется с использованием концепции ALARP. Это означает, что описание каждого из четырех классов рисков основано на рисунке В.1. Риски в определениях этих классов соответствуют случаю, когда приняты требуемые меры снижения риска. Соответствие между рисунком В.1 и классами рисков является следующим:

- I класс рисков соответствует области недопустимого риска;
- II и III классы рисков находятся в области ALARP, II класс находится целиком внутри области ALARP;
- IV класс рисков находится в области общей допустимости рисков.

Для каждой конкретной ситуации или для сравнимых промышленных отраслей может быть разработана таблица, аналогичная таблице В.1, учитывающая широкий диапазон социальных, политических и экономических факторов. Каждому последствию может быть поставлена в соответствие частота и, таким образом, таблица будет заполнена классами рисков. Например, «частое» в таблице В.1 может обозначать событие, которое будет встречаться постоянно и частота которого может быть определена как превышающая 10 раз в год. Критическое последствие может быть одной смертью и/или многочисленными тяжелыми травмами, или профессиональными заболеваниями.

Таблица В.1 — Пример классификации рисков по частоте несчастных случаев

| Частота | Последствия | | | |
|---|---|---|---|---|
| | катастрофические | критические | граничные | незначительные |
| Частые | I | I | I | II |
| Вероятные | I | I | II | III |
| Случайные | I | II | III | III |
| Редкие | II | III | IV | IV |
| Невероятные | III | III | IV | IV |

*Окончание таблицы В.1*

| Частота | Последствия | | | |
|---|---|---|---|---|
| | катастрофические | критические | граничные | незначительные |
| Неправдоподобные | IV | IV | IV | IV |

Примечания

1 Фактическое содержание I, II, III и IV классов рисков зависит от отрасли, а также от реальных частот для таких категорий, как «частые», «вероятные» и т.д. Данная таблица должна, следовательно, рассматриваться как пример содержания подобных таблиц, а не как руководство для будущего использования.

2 Определение уровней полноты безопасности по частотам, приведенным в настоящей таблице, описано в приложении С.

Таблица В.2 — Интерпретация классов

| Класс риска | Интерпретация |
|---|---|
| Класс I | Недопустимый риск |
| Класс II | Нежелательный риск может быть допустим, только если снижение риска невозможно или если затраты на снижение существенно непропорциональны достигаемому улучшению |
| Класс III | Риск допустим, если цена уменьшения риска превосходит достигаемый выигрыш |
| Класс IV | Незначительный риск |

**Приложение С**
**(обязательное)**

## Определение уровней полноты безопасности: количественный метод

### С.1 Общие положения

В настоящем приложении описывается, как могут быть определены уровни полноты безопасности с использованием количественного подхода, и показывается, как может быть использована информация, содержащаяся в таблице В.1 и подобных ей таблицах. Количественный подход приобретает особое значение, когда:

- допустимый риск описан на количественном уровне (например, что конкретное последствие не должно происходить с частотой, превышающей один случай на $10^4$ лет);
- для уровней полноты безопасности в системах безопасности определены количественные ориентиры. Такие ориентиры определены в настоящем стандарте [МЭК 61508-1 (таблицы 2 и 3)].

Настоящее приложение не представляет собой систематического описания метода, оно предназначено для того, чтобы проиллюстрировать основные принципы. Данный метод применим, в частности, когда используется модель риска, показанная на рисунках А.1 и А.2.

### С.2 Общее описание метода

Данная модель используется для того, чтобы проиллюстрировать основные принципы, показанные на рисунке А. 1. Основные шаги при использовании метода перечислены ниже, они должны выполняться для каждой функции безопасности, которая должна быть реализована E/E/PE системой, связанной с безопасностью:

- определить допустимый риск из таблицы, подобной таблице В.1;
- определить риск EUC;
- определить уменьшение риска, необходимое для того, чтобы сделать его допустимым;
- распределить требуемое уменьшение риска между E/E/PE системами, связанными с безопасностью, системами, связанными с безопасностью, основанными на других технологиях, и внешними средствами уменьшения риска [МЭК 61508-1 (пункт 7.6)].

Таблица В.1 содержит частоты рисков и позволяет определить числовое значение планируемого допустимого риска (*Ft*).

Частота, связанная с риском, создаваемым EUC, включая систему управления EUC и вопросы, связанные с человеческим фактором (риск EUC), но без учета каких-либо мер защиты, может быть определена с использованием количественных методов оценки риска. Частота возникновения опасного события в отсутствие средств защиты $F_{np}$ представляет собой один из двух компонентов риска EUC; другим компонентом является последствие опасного события. $F_{np}$ может быть определена с помощью:

- анализа интенсивности отказов в схожих ситуациях;
- данных из соответствующих баз данных;
- расчетов с применением соответствующих методов прогноза.

Настоящий стандарт накладывает ограничения на минимальную интенсивность отказов, которая может быть предъявлена для системы управления EUC [МЭК 61508-1 (пункт 7.5.2.5)]. Если задано, что система управления EUC имеет интенсивность отказов меньше минимальной, то система управления EUC должна рассматриваться как система, связанная с безопасностью, и должна быть объектом всех требований к системам, связанным с безопасностью, содержащихся в настоящем стандарте.

### С.3 Пример расчетов

На рисунке С.1 представлен пример того, как может быть рассчитана необходимая полнота безопасности для единичной системы безопасности. Для этого примера

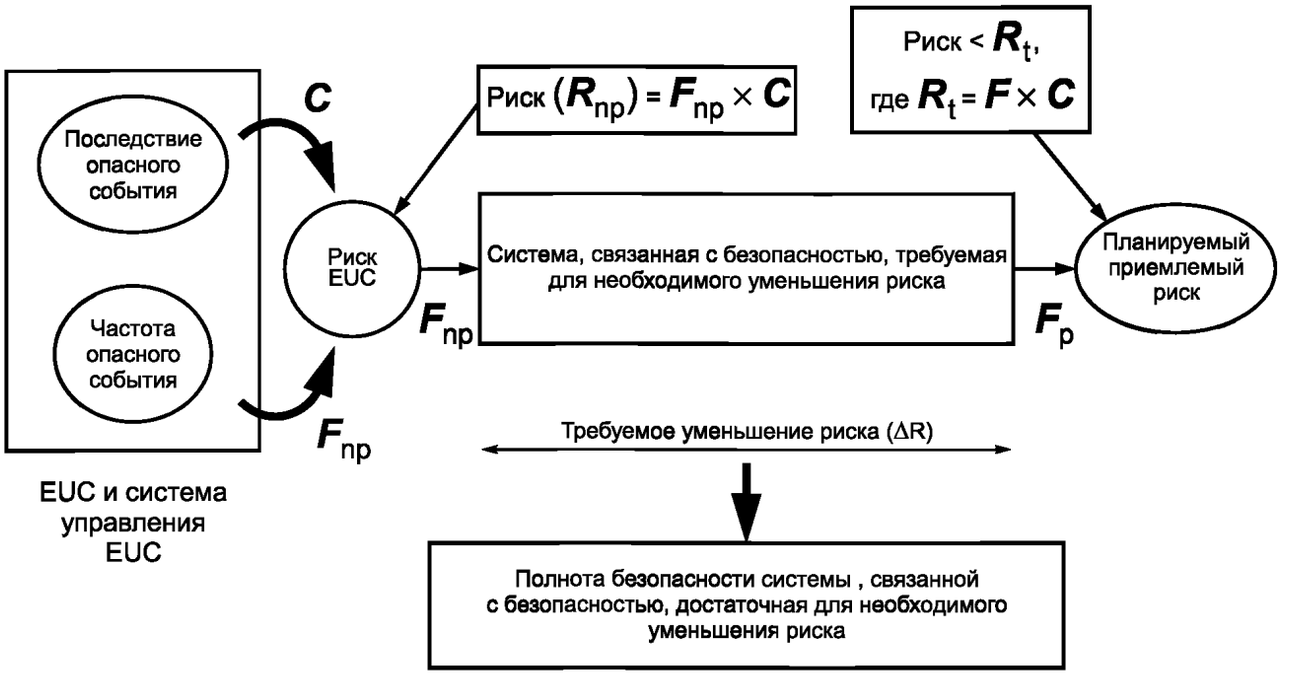
$$PFD_{avg} \le F_t/F_{np},$$

где $PFD_{avg}$ — средняя вероятность отказа при выполнении системой, связанной с безопасностью, операции по запросу. Эта величина представляет собой меру полноты безопасности по отношению к отказам для системы, связанной с безопасностью, работающей в режиме низкой интенсивности запросов [МЭК 61508-1 (таблица 2) и МЭК 61508-4 (пункт 3.5.12)];

$F_t$ — частота для допустимого риска;

$F_{np}$ — интенсивность запросов к системе, связанной с безопасностью.

Определение $F_{np}$ для EUC является важным благодаря связи с $PFD_{avg}$ и, следовательно, с уровнем полноты безопасности системы, связанной с безопасностью.




*C* — последствие опасного события;
$F_р$ — частота для риска при установленных средствах защиты.

Рисунок С.1 — Назначение полноты безопасности: пример для системы, связанной с безопасностью

Шаги, которые должны быть выполнены при определении уровня полноты безопасности (когда последствие *C* остается неизменным), приведены ниже (они также показаны на рисунке С.1):

- определить частотную составляющую риска EUC без учета каких-либо средств защиты $F_{пр}$;
- определить последствие *C* без учета каких-либо средств защиты;
- определить, используя таблицу В.1, достигается ли для частоты $F_{пр}$ и последствия *C* допустимый уровень риска. Если при использовании таблицы В.1 получен I класс риска, то требуется дальнейшее снижение риска. Риски IV или III классов могут быть допустимыми рисками. Риск II класса требует дальнейших исследований.

Примечание — Таблица В.1 используется для того, чтобы проверить, нужны ли меры по дальнейшему снижению риска, поскольку может оказаться возможным достигнуть допустимого риска без применения каких-либо средств защиты;

- определить вероятность отказа системы, связанной с безопасностью, при работе по запросу $PFD_{avg}$, состоящего в невозможности достичь требуемого снижения риска $\Delta R$. Для постоянных последствий в описанной конкретной ситуации $PFD_{avg} = (F_t/F_{пр}) = \Delta R$;
- для $PFD_{avg} = (F_t/F_{пр})$ уровень полноты безопасности может быть получен из таблицы 2 МЭК 61508-1 (например, для $PFD_{avg} = 10^{-2} — 10^{-3}$ уровень полноты безопасности равен 2).

Эти шаги соответствуют случаю, когда все требуемое снижение риска достигается за счет одной системы, связанной с безопасностью, которая должна уменьшить интенсивность возникновения опасностей, как минимум, с $F_{пр}$ до $F_t$.

**Приложение D**
**(обязательное)**

## Определение уровней полноты безопасности. Качественный метод: графы риска

### D.1 Общие положения

Количественный метод, описанный в приложении С, не применим в тех ситуациях, где риск (или его частотная составляющая) не может быть охарактеризован количественно. В настоящем приложении описывается метод графов риска, представляющий собой качественный метод, позволяющий определять уровень полноты безопасности для систем, связанных с безопасностью, на основе знания факторов риска, связанных с EUC и системой управления EUC. Он применим, в частности, когда модель риска соответствует той, которая показана на рисунках А.1 и А.2.

При качественном подходе для упрощения вводится несколько параметров, описывающих природу опасной ситуации, возникающей при отказе или недоступности систем, связанных с безопасностью. Выбирается по одному параметру из каждого из четырех наборов; после этого выбранные параметры объединяются для определения уровня полноты безопасности, назначаемого системе, связанной с безопасностью. Эти параметры:

- позволяют произвести осмысленную классификацию рисков и
- содержат ключевые факторы для оценки рисков.

В приложении нет подробного описания метода, а даны его основные принципы. Тем, кто собирается применять методы, указанные в настоящем приложении, рекомендуется обратиться к [1] — [5].

### D.2 Построение графа риска

Упрощенная процедура, описываемая ниже, основывается на следующем уравнении:

$$R = f \cdot C,$$

где $R$ — риск при отсутствии системы, связанной с безопасностью;
$f$ — частота опасного события при отсутствии системы, связанной с безопасностью;
$C$ — последствие опасного события (последствия должны быть связаны с причинением вреда здоровью и безопасности или с причинением вреда из-за нанесения ущерба окружающей среде).

Считается, что на частоту опасного события $f$ в данном случае влияют три фактора:

- частота и время нахождения в опасной зоне;
- возможность избежать опасного события;
- вероятность возникновения опасного события при отсутствии систем, связанных с безопасностью (но при наличии внешних средств уменьшения риска), эта вероятность называется вероятностью нежелательного события.

Из этих факторов следуют четыре параметра, характеризующих риск:

$C$ — последствие опасного события;
$F$ — частота и время нахождения в опасной зоне;
$P$ — вероятность того, что не удастся избежать опасного события;
$W$ — вероятность нежелательного события.

### D.3 Другие возможные параметры риска

Описанные выше параметры риска достаточно общие, с широким диапазоном применений. Однако могут существовать приложения, характеризующиеся аспектами, требующими введения дополнительных параметров риска. В качестве примера можно привести использование новых технологий в EUC и в системах управления EUC. Целью новых параметров может быть более точная оценка требуемого уменьшения риска (рисунок А.1).

### D.4 Построение графа риска: общая схема

Объединение параметров риска, описанных выше, позволяет построить граф риска, подобный тому, который показан на рисунке D.1. Для этого графа справедливы следующие соотношения: $C_A < C_B < C_C < C_D$; $F_A < F_B$; $P_A < P_B$; $W_1 < W_2 < W_3$. Граф рисков можно пояснить следующим образом.

Использование параметров риска $C$, $F$ и $P$ приводит к появлению выходных параметров $X_1$, $X_2$,..., $X_N$ (точное число зависит от конкретной прикладной области, для которой строится граф риска). На рисунке D.1 показана ситуация, когда для более серьезных последствий не используются дополнительные весовые коэффициенты. Каждый из этих выходных параметров отображается на одну из трех шкал ($W_1$, $W_2$ или $W_3$). Каждая точка на этих шкалах указывает на требуемую полноту безопасности, которая должна быть достигнута рассматриваемой E/E/PE системой, связанной с безопасностью. На практике могут встречаться ситуации, когда одна E/E/PE система, связанная с безопасностью, не может обеспечить требуемого уменьшения риска.

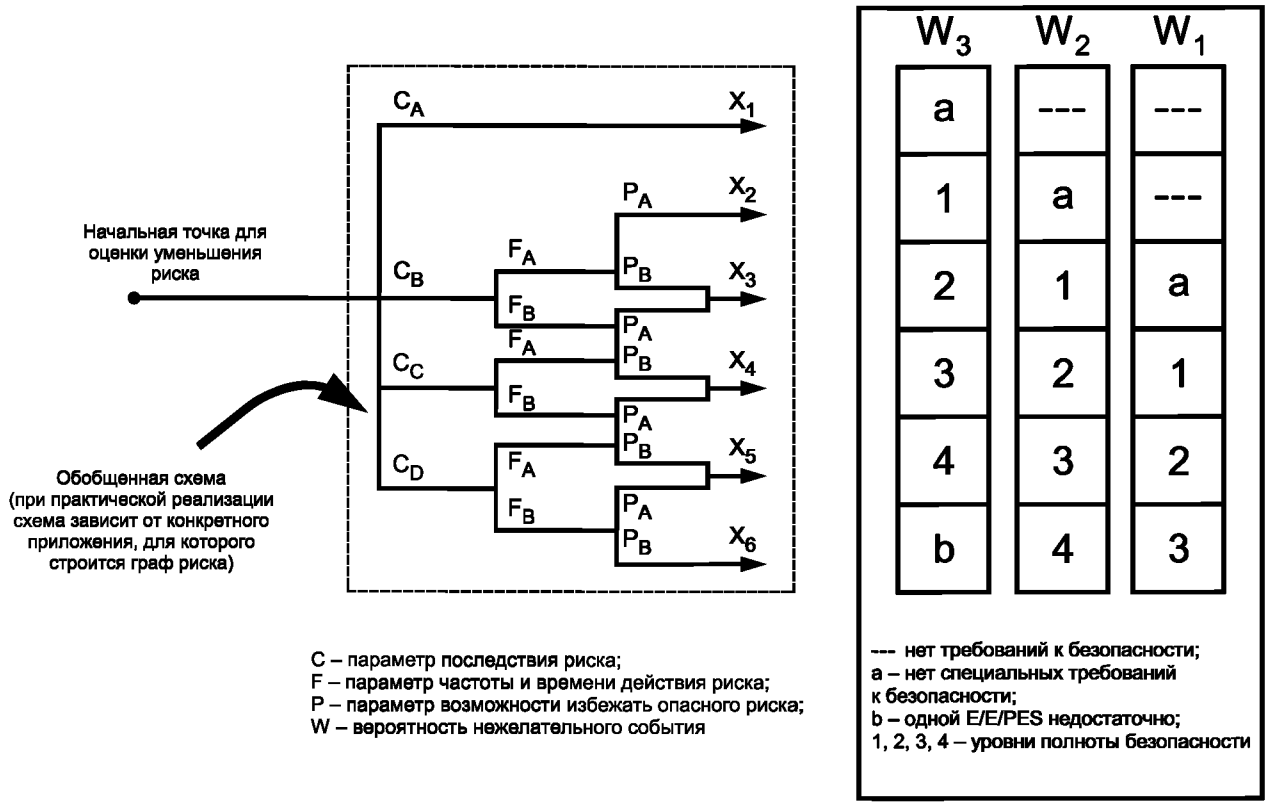



Рисунок D.1 — Граф риска: общая схема

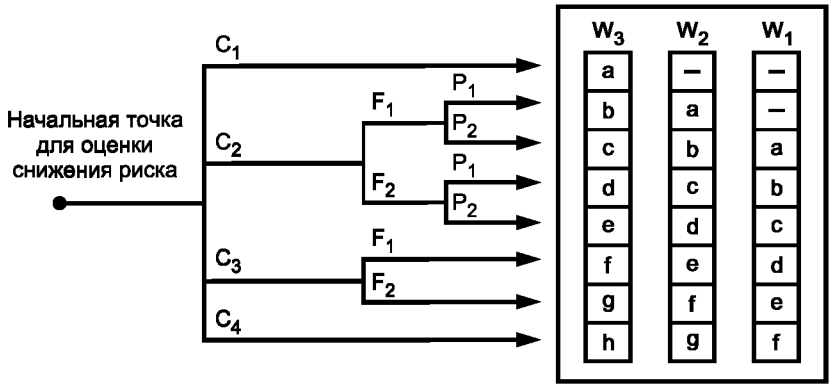
Отображение на $W_1$, $W_2$ или $W_3$ позволяет учесть вклад других мер по снижению риска. Смещение шкал $W_1$, $W_2$ и $W_3$ позволяет учесть три различных уровня уменьшения риска, обеспечиваемого другими мерами. Так шкала $W_3$ дает минимальное уменьшение риска за счет других мер (т.е. наибольшую вероятность того, что произойдет нежелательное событие), шкала $W_2$ соответствует промежуточному по величине вкладу других мер, а шкала $W_1$ — наибольшему вкладу. Для конкретных промежуточных выходных значений графа рисков (т. е $X_1$, $X_2$,... или $X_6$) и для конкретной шкалы W (т. е. $W_1$, $W_2$ или $W_3$) конечные значения графа рисков являются уровнями полноты безопасности E/E/PE систем, связанных с безопасностью, (т.е. 1, 2, 3 или 4), они представляют собой оценку требуемого уменьшения риска для данной системы. Это уменьшение риска вместе с уменьшением риска, достигаемым другими средствами (например, с помощью систем, связанных с безопасностью, основанных на других технологиях и внешних средств уменьшения риска) и учитываемым с помощью механизма шкалы W, дает требуемое уменьшение риска для конкретной ситуации.

Параметры, указанные на рисунке D.1 ($C_A$, $C_B$, $C_C$, $C_D$, $F_A$, $F_B$, $P_A$, $P_B$, $W_1$, $W_2$, $W_3$), и соответствующие им веса должны быть точно определены для каждой конкретной ситуации или для сравнимых отраслей. Может также потребоваться их определение в международных стандартах для прикладных отраслей.

### D.5 Пример графа рисков

Пример графа рисков, основанный на данных, приведенных в таблице D.1, показан на рисунке D.2. Использование параметров риска *C*, *F* и *P* приводит к одному из восьми выходных параметров. Каждый из этих параметров отображается на одну из трех шкал ($W_1$, $W_2$ и $W_3$). Каждая точка на этих шкалах (a, b, c, d, e, f, g и h) указывает на требуемое снижение риска, которое должно быть обеспечено системой, связанной с безопасностью.

Примечание — Дополнительная информация по использованию графов риска содержится в [2].




**a, b, c, d, e, f, g, h представляют требуемое минимальное снижение риска. В таблице показаны связи между требуемым минимальным снижением риска и уровнем полноты безопасности**

C — параметр последствий риска;

F — параметр частоты и времени действия риска;

P — параметр риска, связанный с возможностью избежать опасности;

W — вероятность нежелательного события;

a, b, c, … , h — оценки требуемого уменьшения риска для E/E/PE систем, связанных с безопасностью

| Требуемое минимальное снижение риска | Уровень полноты безопасности |
|---|---|
| — | Нет требований к безопасности |
| a | Нет специальных требований к безопасности |
| b, c | 1 |
| d | 2 |
| e, f | 3 |
| g | 4 |
| h | E/E/PE системы, связанной с безопасностью, недостаточно |

Рисунок D.2 — Граф риска: пример (показывает только общие принципы)

Таблица D.1 — Данные для графа рисков (рисунок D.2)

| Параметр риска | | Классификация | Комментарии |
|---|---|---|---|
| Последствие *C* | $C_1$<br>$C_2$<br><br>$C_3$<br>$C_4$ | Небольшая травма.<br>Серьезная постоянная травма у одного или нескольких человек.<br>Смерть нескольких человек.<br>Смерть очень многих людей | Данная система классификации основана на травмах и смерти людей. Для случая ущерба окружающей среде или материального ущерба может потребоваться разработка других схем классификации.<br>Для интерпретации параметров $C_1$, $C_2$, $C_3$ и $C_4$, необходимо принимать во внимание последствия несчастных случаев и обычное лечение |
| Частота и продолжительность пребывания в опасной зоне *F* | $F_1$<br>$F_2$ | От редкого до более частого пребывания в опасной зоне.<br>От частого до постоянного пребывания в опасной зоне | Данная система классификации основана на травмах и смерти людей. Для случая ущерба окружающей среде или материального ущерба может потребоваться разработка других схем классификации |
| Возможность избежать опасного события *P* | $P_1$<br><br>$P_2$ | Возможно при определенных обстоятельствах.<br>Почти невозможно | Данный параметр учитывает:<br>- тип операций процесса: контролируемых (т.е. управляемых подготовленным или неподготовленным персоналом) или неконтролируемых;<br>- скорость развития опасного события (например, внезапное, быстрое или медленное);<br>- легкость распознавания опасности (например, видна сразу, обнаруживается техническими средствами или обнаруживается без использования технических средств); |

*Окончание таблицы D.1*

| Параметр риска | | Классификация | Комментарии |
|---|---|---|---|
| | | | - возможность избежать опасного события (например, возможно отступление, отступление невозможно либо отступление возможно при определенных обстоятельствах);<br>- реальный опыт в области техники безопасности (такой опыт может быть для идентичного EUC, для сходного EUC либо отсутствовать) |
| Вероятность нежелательного события $W$ | $W_1$<br><br><br><br>$W_2$<br><br><br>$W_3$ | Весьма незначительная вероятность нежелательного события, возможно только небольшое число таких событий.<br>Небольшая вероятность нежелательного события, возможно небольшое число таких событий.<br>Относительно высокая вероятность наступления нежелательного события, вероятны частые повторения нежелательного события | Назначение параметра $W$ состоит в том, чтобы оценить частоту нежелательных событий в условиях отсутствия каких-либо систем, связанных с безопасностью (E/E/PE систем или систем, основанных на других технологиях), но с учетом внешних средств уменьшения риска.<br>При отсутствии или незначительности опыта использования EUC или систем управления EUC оценка параметра $W$ может быть проведена с помощью расчетов, которые в таком случае должны представлять собой прогноз для наихудшего случая |

**Приложение Е**
**(обязательное)**

# Определение уровней полноты безопасности Количественный метод: матрица тяжести опасных событий

## Е.1 Общие положения

Количественный метод, описанный в приложении С, не применим в тех случаях, где риск (или его частотная составляющая) не может быть охарактеризован количественно. В настоящем приложении описывается метод матрицы тяжести опасных событий, представляющий собой количественный метод, позволяющий определить уровень полноты безопасности E/E/PE системы, связанной с безопасностью, на базе знания факторов риска, связанных с EUC и системой управления EUC. Он применим, в частности, для модели риска, показанной на рисунках А.1 и А.2 (приложение А).

В схеме, описываемой в настоящем приложении, предполагается, что каждая система, связанная с безопасностью, и каждое внешнее средство уменьшения риска являются независимыми.

Настоящее приложение не представляет собой систематического описания метода, оно предназначено для того, чтобы продемонстрировать общие принципы формирования подобных матриц теми, кто обладает детальной информацией о конкретных параметрах, имеющих существенное значение для рассматриваемой конструкции. Тем, кто собирается использовать методы, рассматриваемые в настоящем приложении, следует обратиться к [1] — [5].

Примечание — Более подробная информация о матрице опасных событий содержится в [3].

## Е.2 Матрица тяжести опасных событий

В основе матрицы лежат следующие требования, соблюдение каждого из которых необходимо для того, чтобы применение метода было корректным:

- системы, связанные с безопасностью (E/E/PE и основанные на других технологиях), а также внешние средства уменьшения риска являются независимыми;

- каждая система, связанная с безопасностью (E/E/PE и основанная на другой технологии), а также каждое внешнее средство уменьшения риска рассматривается как отдельный уровень защиты, обеспечивающий своими собственными средствами частичное уменьшение риска, как показано на рисунке А.1.

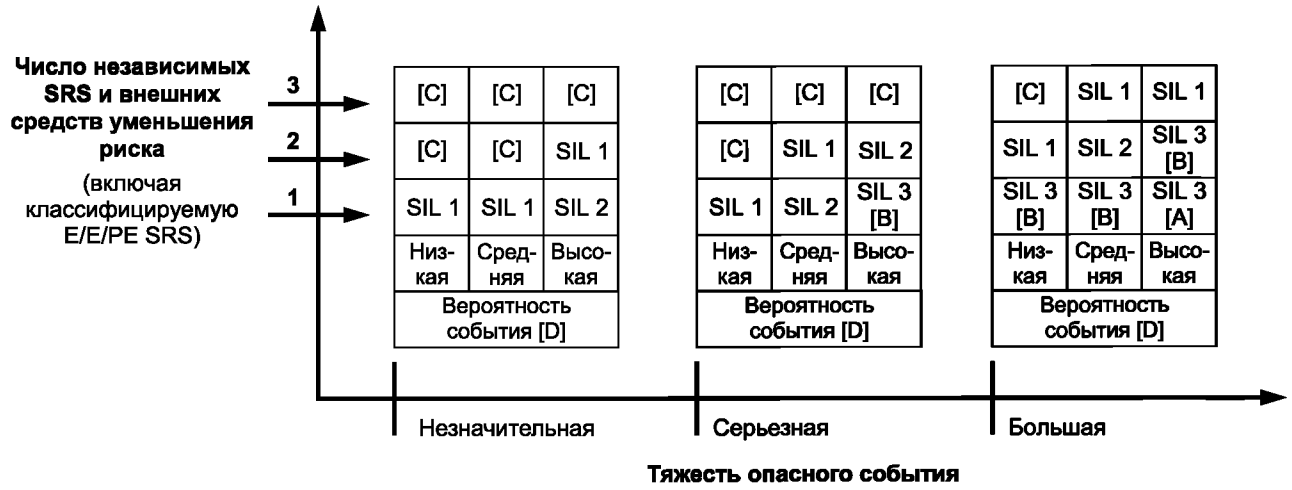
Примечание — Это предположение является справедливым только при условии выполнения систематических контрольных проверок уровней защиты;

- при добавлении одного уровня защиты (см. перечисление b)) полнота безопасности увеличивается на порядок.

Примечание — Это предположение является справедливым только в том случае, когда системы, связанные с безопасностью, и внешние средства уменьшения риска являются в достаточной степени независимыми;

- используется только одна E/E/PE система, связанная с безопасностью (однако она может применяться в сочетании с системами, связанными с безопасностью, основанными на других технологиях, и/или с внешними средствами уменьшения риска), для которой данный метод устанавливает необходимый уровень полноты безопасности.

Приведенный выше анализ приводит к матрице тяжести опасных событий, показанной на рисунке Е.1. Необходимо отметить, что данные, содержащиеся в матрице, представляют собой только пример, иллюстрирующий основные принципы. Для каждой конкретной ситуации или для близких промышленных приложений должна быть разработана своя матрица, аналогичная той, которая приведена на рисунке Е.1.




A — одна E/E/PE система, связанная с безопасностью, с уровнем полноты безопасности SIL = 3 не обеспечивает достаточного уменьшения риска для данного уровня риска. Требуются дополнительные меры по уменьшению риска.

B — одна E/E/PE система, связанная с безопасностью, с уровнем полноты безопасности SIL = 3 может не обеспечить достаточного уменьшения риска для данного уровня риска. Требуется провести анализ опасностей и рисков для того, чтобы определить, нужны ли дополнительные меры по уменьшению риска.

C — независимая E/E/PE система, связанная с безопасностью, по-видимому, не требуется.

D — вероятность события представляет собой вероятность того, что опасное событие произойдет в условиях отсутствия каких-либо систем, связанных с безопасностью, и внешних средств уменьшения риска.

SRS — система, связанная с безопасностью. Вероятность события и общее число независимых уровней защиты определяется в зависимости от конкретного приложения.

Рисунок Е.1 — Пример матрицы тяжести опасных событий (иллюстрирует только основные принципы)

**Приложение F**
**(справочное)**

## Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица F.1

| Обозначение ссылочного международного стандарта | Обозначение и наименование соответствующего национального стандарта Российской Федерации |
|---|---|
| МЭК 61508-1:1998 | ГОСТ Р МЭК 61508-1—2006 (МЭК 61508-1—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования |
| МЭК 61508-2:2000 | * |
| МЭК 61508-3:1998 | ГОСТ Р МЭК 61508-3—2006 (МЭК 61508-3—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению |
| МЭК 61508-4:1998 | ГОСТ Р МЭК 61508-4—2006 (МЭК 61508-4—1998) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения |
| МЭК 61508-6:2000 | * |
| МЭК 61508-7:2000 | * |
| ИСО/МЭК Руководство 51:1990 | ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты |
| МЭК Руководство 104:1997 | * |
| * Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. | |

## Библиография

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

[2] Фундаментальные аспекты безопасности, которые должны учитываться при разработке средств защиты для систем измерения и управления. Schutzeinrichtungen DIN V 19250, Beuth Verlag, Berlin, FRG, 1994

[3] Guidelines for safe automation of chemical process, published by the Center for Chemical Process safety of the American Institute of Chemical Engineering, ISBN 0-8969-0554-1, 1993

[4] Tolerability of risk from nuclear power stations, Health and Safety Executive (UK) publication, ISBN 011 886368 1

[5] Development guidelines for vehicle based software, The Motor Industry Reliability Association, Watling St, Nuneation, Warwickshire, CV10 OTU, United Kingdom, 1994, ISBN 09524156 0 7

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

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

Редактор *Р.Г. Говердовская*
Технический редактор *Л.А. Гусева*
Корректор *В.И. Варенцова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 22.04.2008. Подписано в печать 29.05.2008. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 3,26. Уч.-изд. л. 2,25. Тираж 248 экз. Зак. 583.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru