ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61508-5— 2012

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

Часть 5

Рекомендации по применению методов определения уровней полноты безопасности

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

(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 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. № 590-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61508-5:2010 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности» (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»).

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

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

5 ВЗАМЕН ГОСТ Р МЭК 61508-5–2007

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 ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть 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 2
3 Термины и определения 3
Приложение A (справочное) Полнота безопасности и оценка рисков. Основные концепции 4
Приложение B (справочное) Выбор методов для определения требований к уровню полноты безопасности 13
Приложение C (справочное) ALARP и концепции допустимого риска 15
Приложение D (справочное) Определение уровней полноты безопасности. Количественный метод 18
Приложение E (справочное) Определение уровней полноты безопасности. Методы, основанные на графе рисков 20
Приложение F (справочное) Полуколичественный метод, использующий анализ слоя защиты 26
Приложение G (справочное) Определение уровней полноты безопасности. Количественный метод. Матрица тяжести опасных событий 30
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 32
Библиография 32

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 «программируемые электронные системы»), применяемые во всех прикладных отраслях для выполнения функций, не связанных с безопасностью, во все более увеличивающихся количествах 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 всего 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 разработки рациональной и последовательной технической политики для всех электрических систем обеспечения безопасности. При этом основной целью 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].

Обычно 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 применения, отличающихся различной степенью сложности, возможными рисками и опасностями. В каждом конкретном применении необходимые меры безопасности будут зависеть от многочисленных факторов, специфичных для конкретного применения. Настоящий стандарт, являясь базовым, позволит формулировать такие меры для областей применения будущих международных стандартов, а также для последующих редакций уже существующих стандартов.

Настоящий стандарт:

- рассматривает все соответствующие стадии жизненного цикла безопасности систем в целом, а также подсистем Э/Э/ПЭ системы и программного обеспечения (например, от первоначальной концепции, через проектирование, внедрение, эксплуатацию и техническое обеспечение 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 будущих разработок;
- делает возможной разработку стандартов областей применения, в которых используются Э/Э/ПЭ системы, связанные с безопасностью; разработка стандартов для 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 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 для определения целевого уровня полноты безопасности для функций безопасности, которые должны быть реализованы Э/Э/ПЭ системами, связанными с безопасностью.

Примечание – Настоящий стандарт не устанавливает требований к уровню полноты безопасности для любой функции безопасности и не определяет то, как устанавливается уровень полноты безопасности. Однако настоящий стандарт формирует основанный на риске концептуальный подход и приводит 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 «стойкость к систематическим отказам», применяемое к элементу, характеризующее уверенность в том, что полнота безопасности, касающаяся систематических отказов элемента, соответствует 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 «безопасный отказ». В то же время, понятия «безопасный отказ» и «безопасный в своей основе отказ» могут быть использованы, но для этого необходимо обеспечить соответствующие требования в конкретных разделах стандарта, которым эти понятия должны соответствовать.

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 – 2013–08–01

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);
- ряде методов, позволяющих определить уровни полноты безопасности для Э/Э/ПЭ систем, связанных с безопасностью (приложения С, D, E, F и G).

Выбор метода зависит от области применения и от конкретных обстоятельств. Приложения С, D, E, F и G иллюстрируют количественный и качественный подходы с некоторыми упрощениями, позволяющими продемонстрировать основные принципы. Эти приложения были включены, чтобы продемонстрировать общие принципы нескольких методов, но они не дают полного описания этих методов. При намерении применить методы, указанные в этих приложениях, необходимо обратиться к рекомендуемым источникам.

Примечание – Более подробная информация о подходах, описанных в приложениях В и Е, приведена в [4] и [5]. Дополнительный подход описан в [6].

1.2 МЭК 61508-1, МЭК 61508-2, МЭК 61508-3 и 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 (см. пункт 3.4.3 МЭК 61508-4). В качестве базовых стандартов по безопасности они предназначены для использования техническими комитетами при подготовке стандартов в соответствии с принципами, изложенными в руководстве МЭК 104, 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, удовлетворяющему требованиям серии горизонтальных стандартов МЭК 60601 [7].

1.3 В круг обязанностей технического комитета входит использование там, 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 этим техническим комитетом.

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

Издание официальное

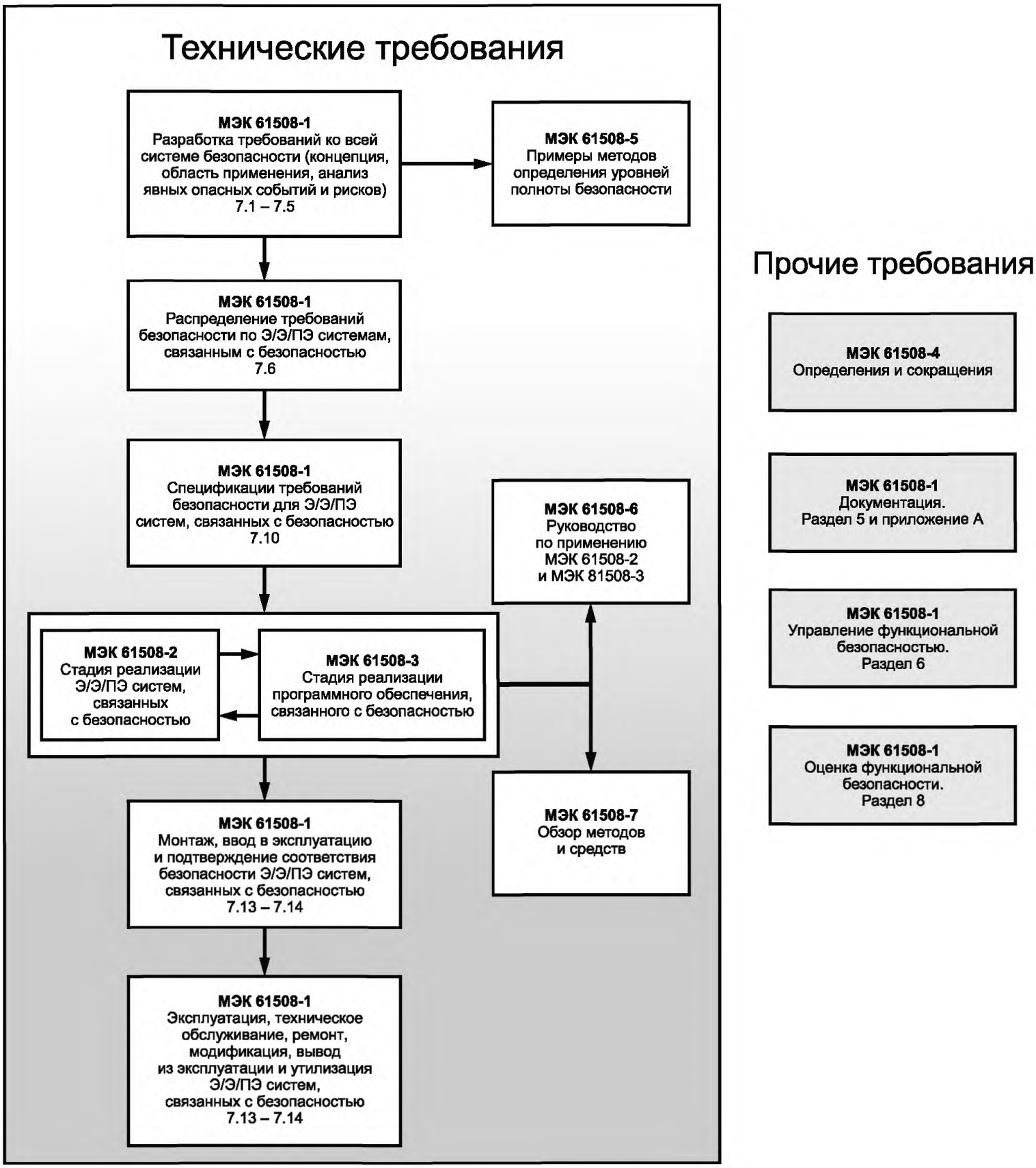


Рисунок 1 – Общая структура серии МЭК 61508

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 61508-1:2010 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

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

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. Термины и определения (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 применимы термины и определения по МЭК 61508-4.

Приложение А
(справочное)

Полнота безопасности и оценка рисков. 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 Необходимое снижение риска

Необходимая степень снижения риска (см. МЭК 61508-4, пункт 3.5.14) представляет собой такое снижение риска, которое должно быть обеспечено для достижения уровня риска, приемлемого в конкретной ситуации (которое может быть установлено качественно[1)] либо количественно[2)]). Концепция необходимого снижения риска является фундаментально важной при разработке спецификации требований к безопасности для Э/Э/ПЭ систем, связанных с безопасностью (в частности, той части спецификации, которая посвящена требованиям к полноте безопасности). Цель определения приемлемого риска для конкретного опасного события состоит в установлении величины «разумного» риска, учитывающего как частоту (или вероятность) возникновения опасных событий, так и их специфические последствия. Системы, связанные с безопасностью, предназначены для того, чтобы уменьшить частоту (или вероятность) опасных событий и/или последствия опасных событий.

Допустимый (приемлемый) 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). Важными факторами являются восприятие и точки зрения тех лиц, которые подвергаются опасности. При определении допустимого риска для конкретного применения необходимо учитывать:

- общие законодательные требования и законодательные требования, которые непосредственно относятся к конкретной области применения;
- 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 приемлемого риска становится все более важной;
- лучшие независимые промышленные, экспертные и научные рекомендации консультативных органов.

При определении требований полноты безопасности Э/Э/ПЭ системы (систем), связанной(ых) с безопасностью, и других мер по снижению риска, для того, чтобы достичь приемлемой частоты опасного события, необходимо учитывать характеристики риска, существенные в данном применении. Приемлемая частота зависит от законодательных требований страны применения, а также от критериев, определенных организацией-потребителем. Аспекты, которые, возможно, необходимо будет учесть, а также способ их применения в Э/Э/ПЭ системах, связанных с безопасностью, приведены ниже.

А.2.1 Индивидуальный риск

Для работников и членов общества обычно определяются разные целевые риски. Целевой индивидуальный риск для сотрудников применим к наиболее подверженному опасности человеку и может быть выражен в общем (суммарном) риске в год, возникающем в течение его рабочей деятельности. Целевой риск применяется к гипотетическому человеку и, следовательно, необходимо учесть процент времени, которое человек проводит на работе. Целевой риск применим ко всем рискам, которым подвержен человек, и для допустимого риска в связи с конкретной функцией безопасности необходимо учитывать и другие риски.

Убедиться в том, что уровень общего риска уменьшен до уровня ниже заданного целевого риска, можно несколькими способами. Один из способов заключается в выявлении и суммировании всех рисков для наиболее подверженного рискам человека. Такой метод может вызвать затруднения, если человек подвержен слишком многим рискам, а для разработки системы необходимы решения на ранних стадиях. Альтернативный подход состоит в распределении общего целевого индивидуального риска в процентном отношении между всеми рассматриваемыми

[1] При достижении допустимого риска должно быть установлено требуемое снижение риска. В приложениях D и E описываются качественные методы, хотя в приведенных примерах требуемое снижение риска косвенно включено в спецификацию требований по УПБ, а не указано в явном виде числовое значение требуемого снижения риска.

[2] Например, опасное событие, приводящее к определенным последствиям, не должно происходить с частотой, превышающей один раз за 10^8 час.

мыми функциями безопасности. Распределение процентов обычно можно осуществить, основываясь на опыте работы с ранее использованными средствами.

Целевой риск, определенный для отдельной функции безопасности, должен также учитывать консерватизм используемого метода анализа риска. Все качественные методы, такие как графы риска, включают в себя оценку критических параметров, увеличивающих риски. Факторы, повышающие риски, являются следствием опасного события и его частоты. В определении этих факторов необходимо учитывать некоторые параметры рисков, такие как уязвимость перед опасным событием, количество людей, попадающих в область действия опасного события, вероятность того, что человек окажется там и тогда, где и когда происходит опасное событие (например, место пребывания людей) и вероятность избежания (уклонения от) опасного события.

Количественные методы обычно определяют, находится ли параметр в определенном диапазоне. При использовании таких методов формируемые критерии должны иметь высокий уровень уверенности в том, что целевые риски не превышены. Для обеспечения безопасности это может означать установление границ диапазона для всех параметров таким образом, чтобы применения при граничных значениях всех параметров удовлетворяли заданным критериям риска. Этот подход установления границ очень консервативен, так как существует очень мало приложений, в которых все параметры будут иметь наихудшие значения в своем диапазоне. Если риску отказа Э/Э/ПЭ систем, связанных с безопасностью, подвергаются члены общества, то обычно используется несколько меньшее значение целевого риска.

А.2.2 Социальный риск

Социальный риск возникает, когда единичное событие влечет за собой многочисленные жертвы. Такие события называются социальными, так как они вызывают социально-политический отклик. К событиям с серьезными последствиями может быть выражена серьезная общественная и организационная антипатия; в некоторых случаях это необходимо учитывать. Критерий социального риска обычно выражается как максимальная накопленная частота травм со смертельным исходом определенного количества человек. Этот критерий обычно выражен одной или несколькими линиями на графике F от N, где F – кумулятивная частота опасностей, а N – количество несчастных случаев с фатальным исходом в результате опасных событий. В логарифмической шкале это соотношение обычно представляет собой прямую линию. Наклон линии будет показывать, насколько организация не предрасположена к риску с более тяжелыми последствиями. Требование состоит в обеспечении того, чтобы кумулятивная частота определенного количества несчастных случаев с фатальным исходом была ниже, чем кумулятивная частота на графике F от N (см. [7]).

А.2.3 Постоянное улучшение

Принципы снижения риска, насколько это практически осуществимо, описаны в приложении В.

А.2.4 Профиль риска

При определении того, какой критерий риска будет применен к определенной угрозе, может понадобиться рассмотреть профиль риска на протяжении срока службы имущества. Остаточный риск может варьироваться от низкого, сразу после контрольных проверок или произведенного ремонта, до максимального, непосредственно перед контрольными проверками. Это необходимо учитывать организациям, которые определяют применяемые критерии риска. Если промежутки времени между контрольными проверками значительные, может быть целесообразно указать максимальную вероятность опасности непосредственно перед контрольной проверкой, или что $PFD(t)$ или $PFH(t)$ ниже верхней границы УПБ на протяжении большего процента времени, чем тот, что задан (например, 90 %).

А.3 Роль Э/Э/ПЭ систем, связанных с безопасностью

Э/Э/ПЭ системы, связанные с безопасностью, вносят вклад в достижение требуемого снижения риска для достижения приемлемого риска. Система, связанная с безопасностью:

- реализует функции безопасности, необходимые для достижения или поддержания безопасного состояния управляемого оборудования, и
- предназначена для достижения самостоятельно, либо при помощи других Э/Э/ПЭ систем, связанных с безопасностью, либо при помощи других мер по снижению рисков необходимой полноты безопасности для требуемых функций безопасности (см. МЭК 61508-4, пункт 3.5.1).

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 приемлемого риска.

В состав Э/Э/ПЭ системы, связанной с безопасностью, могут входить люди. Например, человек может получать с экрана дисплея информацию о состоянии УО и выполнять действия, основываясь на этой информации.

Э/Э/ПЭ системы, связанные с безопасностью, могут работать в режиме низкой интенсивности запросов либо в режиме высокой интенсивности запросов или непрерывного запроса (см. МЭК 61508-4, пункт 3.5.12).

А.4 Полнота безопасности

Полнота безопасности определяется как вероятность системы, связанной с безопасностью, удовлетворительно выполнять требуемые функции безопасности при установленных условиях в течение заданного периода времени (см. МЭК 61508-4, пункт 3.5.2). Полнота безопасности относится к характеристикам, описывающим способность систем, связанных с безопасностью, выполнять функции безопасности (функции безопасности должны быть определены в спецификации требований к функциям безопасности).

Считается, что полнота безопасности состоит из следующих двух компонентов:

- полноты безопасности аппаратных средств; эта часть полноты безопасности связана со случайными отказами аппаратных средств, причем относящимся к опасным отказам (см. МЭК61508-4, п. 3.5.5). Достижение заданного уровня полноты безопасности аппаратных средств, связанных с безопасностью, может быть установлено с разумной степенью точности. Следовательно, требования могут быть распределены между подсистемами в соответствии с нормальными законами для вероятностей совместных событий. Для достижения требуемой полноты безопасности аппаратных средств может потребоваться использование избыточной архитектуры;

- систематической полноты безопасности; эта часть полноты безопасности обусловлена систематическими отказами, относящимися к опасным отказам

(см. МЭК 61508-4, пункт 3.5.4). Хотя влияние отдельных систематических отказов на полноту безопасности можно оценить, данные по отказам, вызванным ошибками при проектировании, и отказам по общей причине указывают на то, что влияние этих отказов бывает сложно предсказать. При этом увеличивается неопределенность в расчетах вероятности отказов в конкретной ситуации (например, вероятности отказа системы защиты, связанной с безопасностью). Следовательно, необходимо решить, какие способы минимизации этой неопределенности окажутся наиболее эффективными. Следует учитывать, что меры, принятые для уменьшения вероятности случайных отказов аппаратных средств, не должны обязательно приводить к снижению вероятности систематических отказов. Такие технические решения, как резервирование в виде организации параллельных каналов с идентичным оборудованием, которые являются весьма эффективными для случайных отказов аппаратных средств, мало полезны для уменьшения таких систематических отказов, как ошибки в программном обеспечении.

А.5 Режимы работы и определение УПБ

Режим работы связан с тем, как будет использоваться функция безопасности в зависимости от частоты запросов к ней на обслуживание:

- режим с низкой частотой запросов к функции безопасности; частота запросов к функции безопасности не более, чем раз в год, или

- режим с высокой частотой запросов к функции безопасности; частота запросов к функции безопасности более, чем раз в год, или

- режим с непрерывным запросом; запрос к функции безопасности существует постоянно.

Таблицы 2 и 3 МЭК 61508-1 задают целевые меры отказов, связанные с четырьмя уровнями полноты безопасности, для каждого из режимов работы. Далее описаны эти режимы работы.

А.5.1 Полнота безопасности и снижение риска в режиме с низкой частотой запросов

Требуемый уровень полноты безопасности Э/Э/ПЭ систем, связанных с безопасностью, и других мер по снижению рисков должен быть таким, чтобы обеспечить:

- среднюю вероятность отказов по запросу систем, связанных с безопасностью, достаточную для того, чтобы частота опасных событий не превышала бы значения, соответствующего приемлемому риску и/или

- возможность системы, связанной с безопасностью, так изменить последствия отказов, чтобы риск не превышал значение приемлемого риска.

Рисунок А.1 иллюстрирует общую концепцию снижения риска. Общая модель предполагает следующее:

- имеется УО и система управления УО;
- существует связанный с процессом человеческий фактор;
- средства защиты включают в свой состав:
- Э/Э/ПЭ системы, связанные с безопасностью,
- другие средства снижения риска.

Примечание – На рисунке А.1 представлена обобщенная модель риска, иллюстрирующая общие принципы. Модель риска для конкретного применения должна разрабатываться с учетом конкретного способа, при помощи которого будет достигаться требуемое снижение риска Э/Э/ПЭ системами, связанными с безопасностью, и/или другими средствами снижения риска. Поэтому результирующая модель риска может отличаться от модели, представленной на рисунке А.1.

В число рисков, представленных на рисунках А.1 и А.2, входят:

- Связанный с УО риск. Это риск наличия конкретного опасного события для УО. При этом учитывается наличие системы управления УО и человеческого фактора. При определении этого риска не рассматриваются какие бы то ни было специальные средства защиты безопасности (см. МЭК 61508-4, пункт 3.1.9);

- Приемлемый риск. Риск, который считается приемлемым в данном контексте на основе принятой в обществе системы ценностей (см. МЭК 61508-4, пункт 3.1.7);

- Остаточный риск. В контексте настоящего стандарта это риск возникновения опасных событий, связанных с УО, системой управления УО, факторами, зависящими от человека, который сохраняется после добавления Э/Э/ПЭ систем, связанных с безопасностью, и других мер по снижению рисков (см. МЭК 61508-4, пункт 3.1.7).

Связанный с УО риск является функцией от риска, связанного с самим УО, но учитывающего также снижение риска, достигнутое благодаря применению системы управления УО. Чтобы избежать неразумных требований к полноте безопасности основной системы управления УО, настоящий стандарт устанавливает ограничения на возможные требования (см. МЭК 61508-1 подпункт 7.5.2.5).

Необходимое снижение риска достигается комбинацией всех способов увеличения безопасности. Процесс необходимого снижения риска, обеспечивающий достижение конкретного приемлемого риска от начального значения риска УО, показан на рисунке А.1 (относится к функции безопасности, работающей в режиме с низкой частотой запросов).

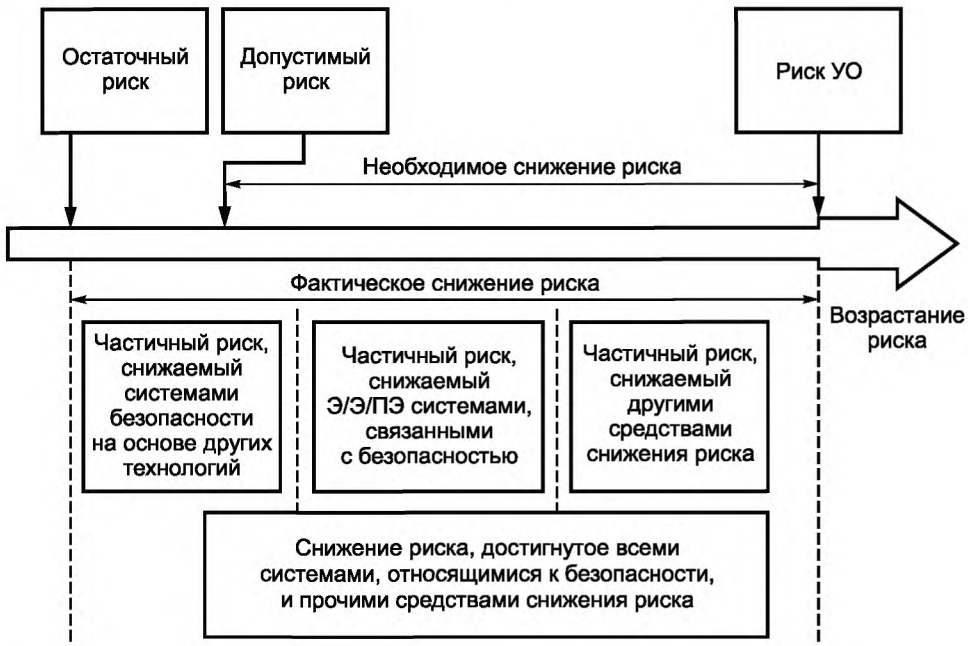


Рисунок А.1 – Снижение риска: основные понятия (режим с низкой частотой запросов)

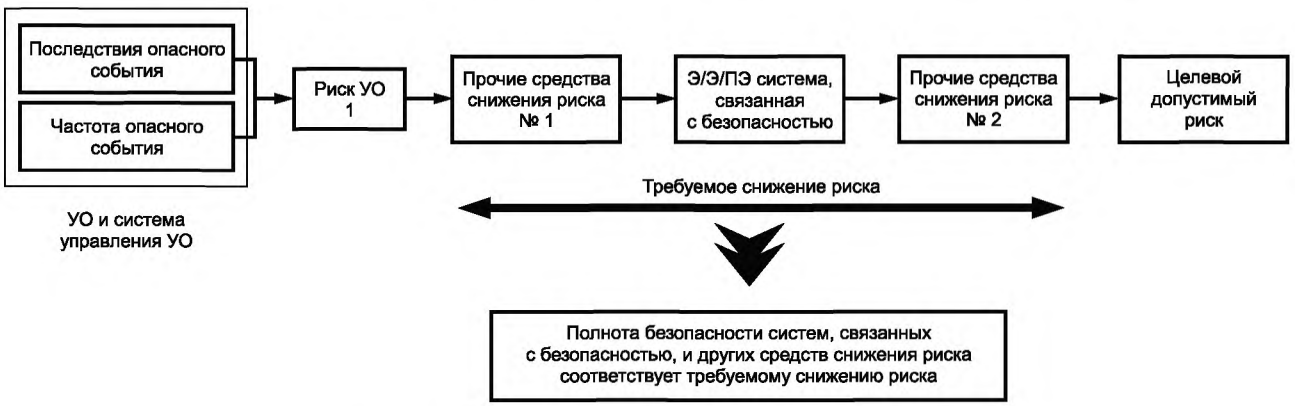


Рисунок А.2 – Понятия риска и полноты безопасности

А.5.2 Полнота безопасности в режиме с высокой частотой запросов

Требуемый уровень полноты безопасности Э/Э/ПЭ систем, связанных с безопасностью, и других мер по снижению рисков должен быть таким, чтобы обеспечить:

- среднюю вероятность отказов по запросу систем, связанных с безопасностью, достаточно низкую для того, чтобы частота опасных событий не превышала бы значения, соответствующего приемлемому риску, и/или
- среднюю вероятность отказа в час системы, связанной с безопасностью, достаточно низкую для того, чтобы частота опасных событий не превышала бы значения, соответствующего приемлемому риску.

Рисунок А.3 иллюстрирует основные понятия для применений, работающих в режиме с высокой частотой запросов. Общая модель предполагает следующее:

- имеется УО и система управления УО;
- существует связанный с процессом человеческий фактор;
- средства защиты безопасности включают в свой состав:
- Э/Э/ПЭ системы, связанные с безопасностью, работающие в режиме с высокой частотой запросов;
- другие меры по снижению рисков.

Различные запросы к Э/Э/ПЭ системе, связанной с безопасностью, могут быть следующими:

- общие запросы от управляемого оборудования;
- запросы, возникающие вследствие отказов системы управления для управляемого оборудования;
- запросы, возникающие вследствие отказов по причине человеческого фактора.

Если общая интенсивность запросов, состоящая из всех запросов к системе, превышает один в год, то критическим фактором является интенсивность опасных отказов Э/Э/ПЭ системы, связанной с безопасностью. Частота остаточных опасных событий никогда не может превзойти интенсивность опасных отказов Э/Э/ПЭ системы, связанной с безопасностью. Она может быть ниже, если другие меры по снижению риска уменьшают вероятность ущерба.

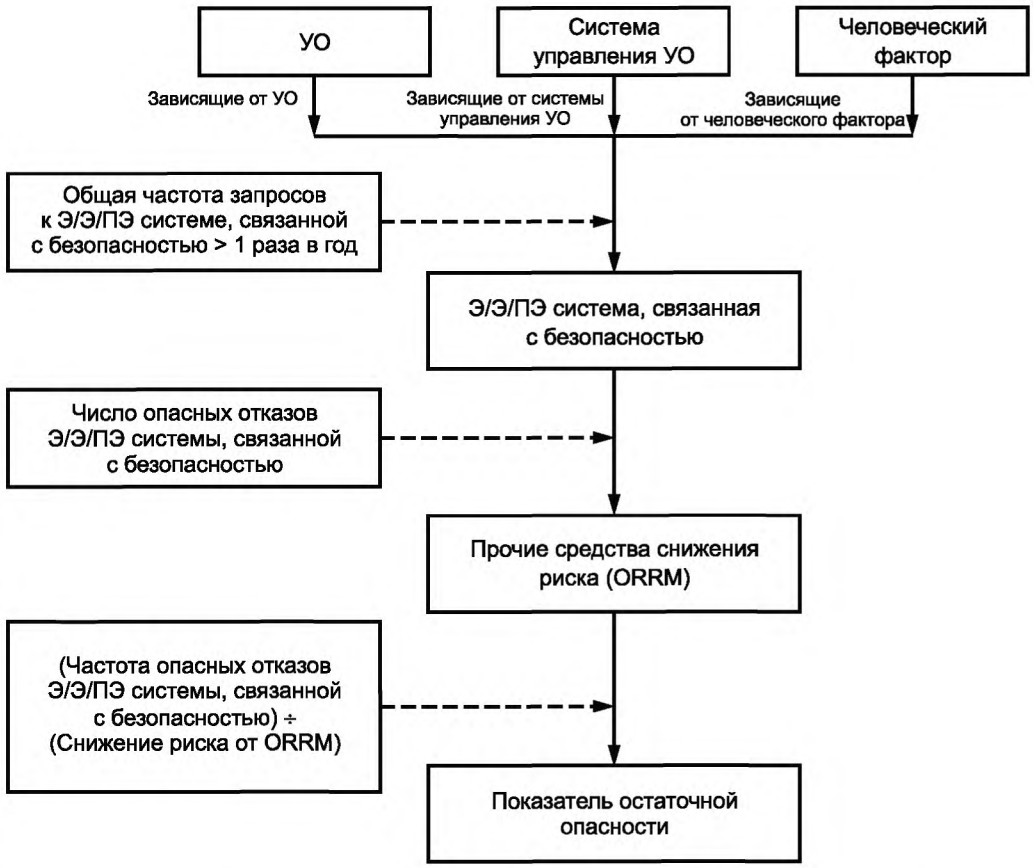


Рисунок А.3 – Диаграмма риска для применений, работающих в режиме с высокой частотой запросов к функции безопасности

А.5.3 Полнота безопасности для режима с непрерывным запросом

Требуемый уровень полноты безопасности Э/Э/ПЭ систем, связанных с безопасностью, и других мер по снижению риска должен быть таким, чтобы обеспечить среднюю вероятность опасных отказов в час системы, связанной с безопасностью, достаточно низкой для того, чтобы частота опасных событий не превышала бы значения, соответствующего приемлемому риску.

Вместе с Э/Э/ПЭ системой, связанной с безопасностью, другие меры по снижению риска могут снизить частоту остаточных опасных событий, обеспечивая соответствующее снижение риска. Модель показана на рисунке А.4.

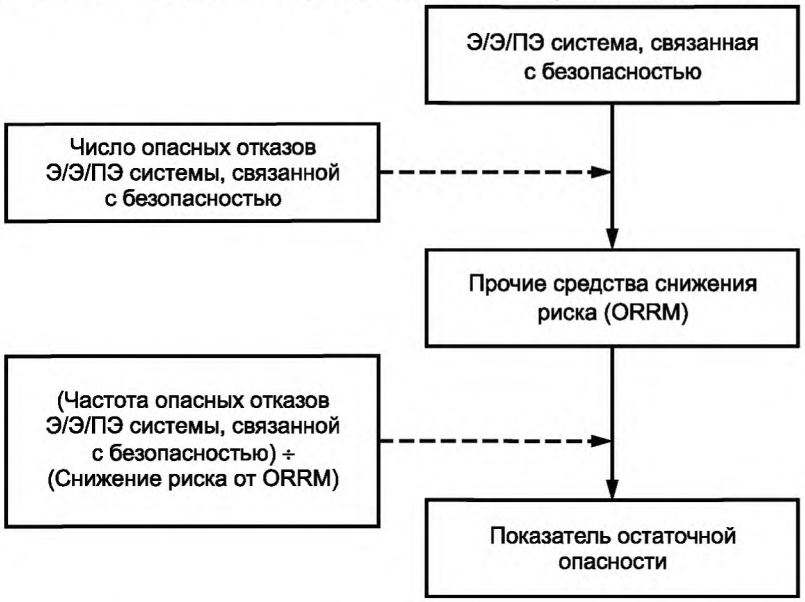


Рисунок А.4 – Диаграмма риска для применений, работающих в непрерывном режиме запросов на обслуживание

А.5.4 Отказы по общей причине и зависимые отказы

При определении уровней полноты безопасности важно учесть отказы по общей причине и зависимые отказы. Модели, показанные на рисунках А.1, А.2, А.3 и А.4, составлены на основании того, что каждая система безопасности, соответствующая конкретной опасности, полностью независима. Во многих применениях такая независимость отсутствует. Например, в случаях:

1) Когда опасный отказ элемента в системе управления УО может вызвать запрос к системе, связанной с безопасностью, а система, связанная с безопасностью, использует элемент, отказавший по той же причине. Например, если датчики систем управления и защиты разделены, но они оба могут отказать по общей причине (см. рисунок А.5).

2) Когда в каждой из нескольких систем, связанных с безопасностью, применяется некоторое однотипное оборудование, каждое из которых отказало по общей причине. Например датчик одного и того же типа используется в двух отдельных системах защиты, обеспечивающих снижение риска от одной и той же опасности (см. рисунок А.6).

3) Когда в нескольких различных используемых системах защиты контрольные проверки проводятся для всех систем синхронно. В таких случаях фактическая средняя вероятность опасных отказов по запросу (PFD_{avg}), достигаемая комбинацией различных систем, будет значительно выше, чем PFD_{avg}, получаемая умножением значений PFD_{avg} для отдельных систем.

4) Когда один и тот же конкретный элемент используется как в системе управления, так и в системе, связанной с безопасностью.

5) Когда в некотором количестве нескольких используемых систем защиты применяется одинаковый элемент.

В таких случаях должно учитываться влияние общей причины/зависимости отказов. Необходимо рассмотреть, сможет ли окончательная структура (архитектура) соответствовать требуемой стойкости к систематическим отказам и требуемой вероятности случайных опасных отказов аппаратных средств, связанных с общим необходимым снижением риска. Влияние отказа по общей причине сложно определить; обычно это требует построения специальных моделей (например, дерева отказов или модели Маркова).

Влияние общей причины, скорее всего, будет более значимым в применениях с высокими уровнями полноты безопасности. Для минимизации влияния общей причины в некоторых применениях может быть необходимо внести разнообразие. Однако необходимо отметить, что использование разнообразия может привести к проблемам на стадиях разработки, технического обслуживания и модификации. Внесение разнообразия может привести к ошибкам вследствие неосведомленности и недостатка опыта работы персонала с различными устройствами.

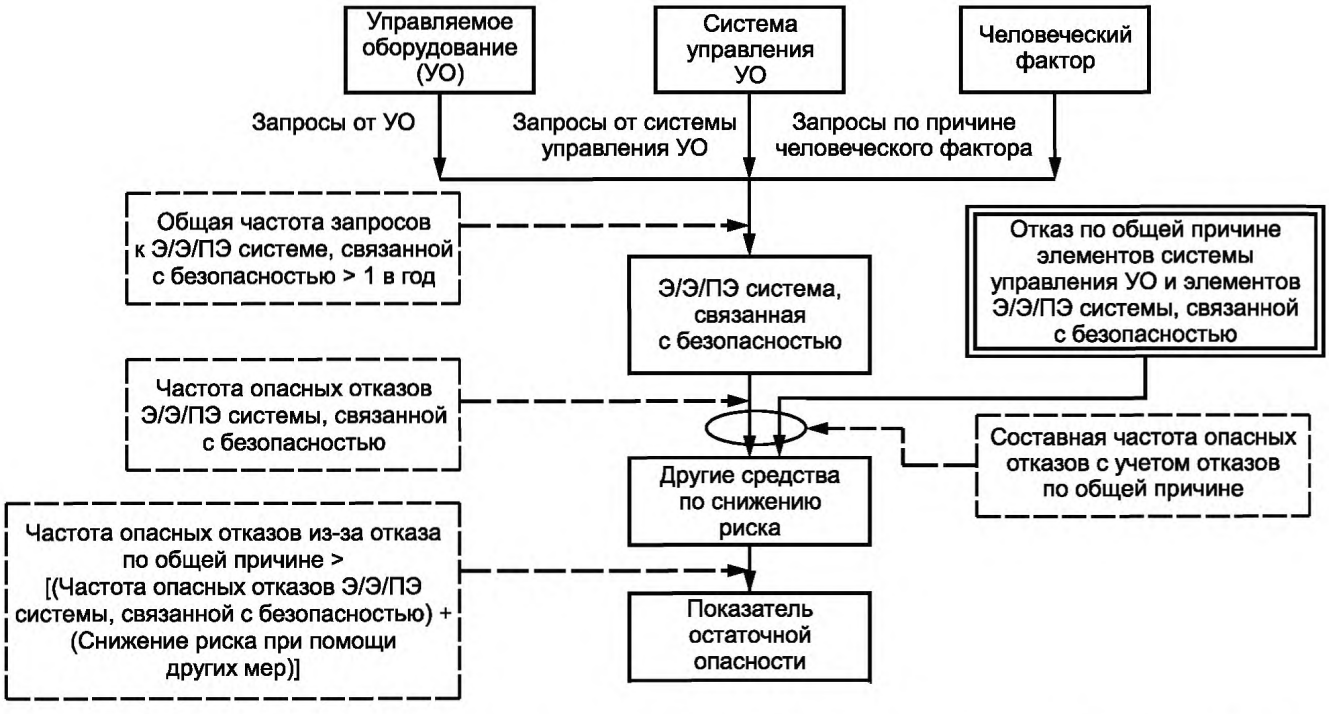


Рисунок А.5 – Иллюстрация отказов по общей причине элементов в системе управления УО и элементов Э/Э/ПЭ системы, связанной с безопасностью

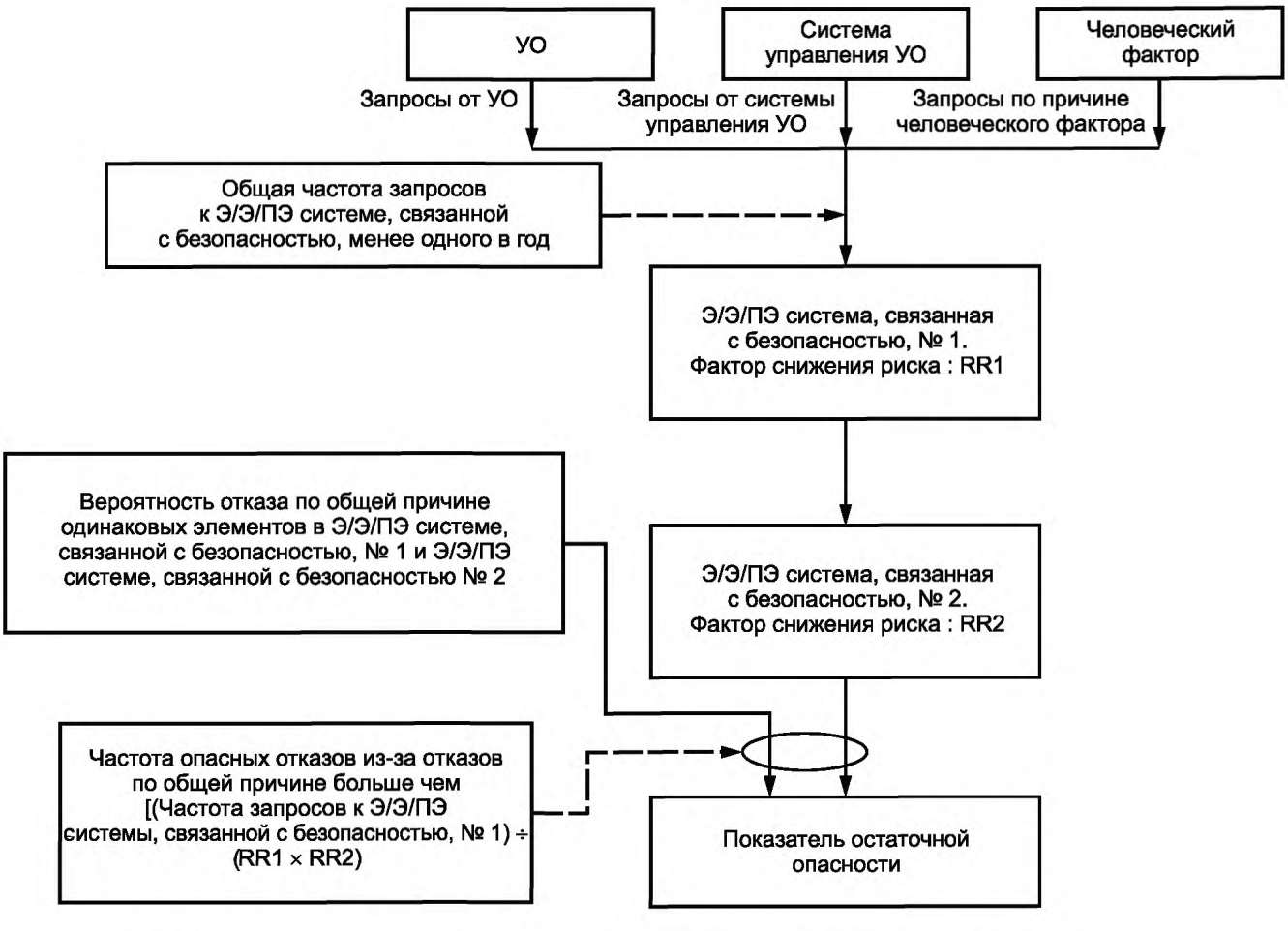


Рисунок А.6 – Общая причина между двумя Э/Э/ПЭ системами, связанными с безопасностью

А.5.5 Уровни полноты безопасности в случае нескольких слоев защиты

В случае применения нескольких слоев защиты для достижения допустимого уровня риска между системами, а также между системами и причинами запросов может возникнуть взаимодействие. Как упоминалось выше в п. А.5.4, всегда существуют проблемы с (де)синхронизацией тестов и отказами по общим причинам, так как они могут быть значимыми факторами, если требования общего снижения рисков высокие или частота запросов низкая. Оценка взаимодействия между слоями безопасности и между слоями безопасности и причинами запросов может быть сложной и потребовать разработки целостной модели (как описано в ИСО/МЭК 31010 [8]) и основываться, например, на методе нисходящего проектирования с корневым событием в виде допустимой частоты опасных событий. Модель может включать все слои безопасности для расчета фактического снижения риска и все причины запросов для расчета фактической частоты опасных событий. Это позволяет идентифицировать минимальные сечения (то есть сценарии отказа), определить слабые места (то есть кратчайшие минимальные сечения: единичные, двойные отказы, и т. д.) в структуре систем и способствовать улучшению системы с помощью анализа чувствительности к опасным событиям.

А.6 Риск и полнота безопасности

Важно понимать различие между риском и полнотой безопасности. Риск – это мера частоты появления и последствий конкретного опасного события. Его можно оценить для различных ситуаций [риск УО, требуемое снижение риска для достижения приемлемого риска, фактический риск (см. рисунок А.1)]. Понятие приемлемого риска определяется рассмотрением вопросов, описанных в А.2. Полнота безопасности применима только к Э/Э/ПЭ системам, связанным с безопасностью, и другим мерам по снижению риска. Полнота безопасности представляет собой меру вероятности того, что рассматриваемые системы/средства удовлетворительно обеспечат требуемое снижение риска для заданных функций безопасности. Только после того, как допустимый риск установлен и получена оценка величины необходимого снижения риска, можно определить требования к полноте безопасности систем, связанных с безопасностью (см. МЭК 61508-4, подразделы 7.4 – 7.6).

Примечание – Такая процедура может носить итеративный характер, что позволит осуществить оптимизацию разработки с целью выполнения различных требований.

А.7 Уровни полноты безопасности и стойкость к систематическим отказам программного обеспечения

Для достижения системами, связанными с безопасностью, необходимого снижения широкого диапазона риска важно иметь несколько доступных уровней полноты безопасности как способа удовлетворения требованиям полноты безопасности функций безопасности в системе, связанной с безопасностью. Стойкости к систематическим отказам программного обеспечения используются в качестве основы определения требований к полноте безопасности функций безопасности, частично реализованных программным обеспечением, связанным с безопасностью. Спецификация требований к полноте безопасности должна указывать уровни полноты безопасности для Э/Э/ПЭ систем, связанных с безопасностью.

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

Целевые 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 с низкой интенсивности запросов, другой – для систем, связанных с безопасностью, работающих в режиме с высокой интенсивностью запросов или в режиме с непрерывным запросом.

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 (см. МЭК 61508-4, пункты 3.5.12 и 3.5.13).

А.8 Распределение требований безопасности

Распределение требований безопасности (как требований к функциям безопасности, так и требований к полноте безопасности) по Э/Э/ПЭ системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и другим средствам снижения риска, показано на рисунке А.7, который идентичен рисунку 6 в МЭК 61508-1. Требования к стадии распределения требований безопасности приведены в МЭК 61508-1 (подраздел 7.6).

Методы, используемые для распределения требований полноты безопасности по Э/Э/ПЭ системам, связанным с безопасностью, системам, связанным с безопасностью, основанным на других технологиях, и другим средствам снижения риска, зависят, в первую очередь, от того, каким образом определена степень необходимого снижения риска – количественно или качественно. Такие подходы называют количественными и качественными соответственно (см. приложения C–G).

Примечания

1 Требования к полноте безопасности связываются с каждой функцией безопасности до распределения (см. МЭК 61508-1, подпункты 7.5.2.3 и 7.5.2.4).

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

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

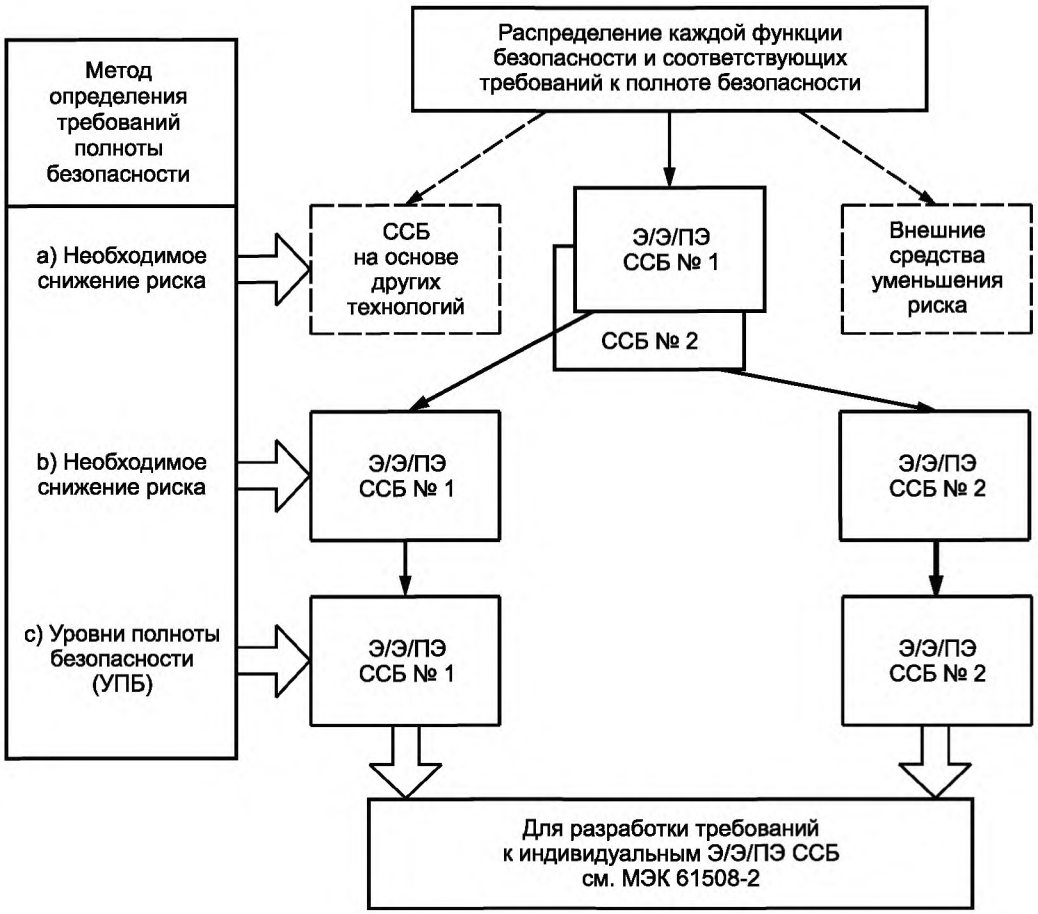


Рисунок А.7 – Распределение требований безопасности по Э/Э/ПЭ системам, связанным с безопасностью, и другим средствам снижения риска

А.9 Ослабляющие системы

Ослабляющие системы действуют в случае полного или частичного отказа других систем, связанных с безопасностью, таких как Э/Э/ПЭ системы безопасности. Задача – сократить последствия, связанные с опасным событием, а не его частоту. Примерами смягчающих систем являются системы противогазовой и противопожарной безопасности (обнаружение огня/газа и последующие действия по устранению пожара, например, потоком воды) и системы подушек безопасности в автомобиле.

При определении требований к полноте безопасности необходимо понимать, что при обосновании тяжести последствий должны учитываться только дополнительные последствия. То есть необходимо определить увеличение тяжести последствий только за счет того, что рассматриваемая функция перестает работать. Это можно сделать, оценив сначала последствия в случае сбоев в работе системы, а затем рассмотреть, как изменяются последствия, если будет корректно работать ослабляющая функция. Если в системе происходят сбои, то последствий будет несколько, причем все они будут иметь различную вероятность. В этом случае полезным может быть применение метода анализа дерева событий.

Примечание – Руководство по определению уровней полноты безопасности систем отключения при пожаре, утечке газа и чрезвычайных ситуациях включено в приложение В ИСО 10418 [9].

Приложение В
(справочное)

Выбор методов для определения требований к уровню полноты безопасности

В.1 Общие положения

В настоящем приложении рассматривается ряд методов, которые можно применить при определении уровней полноты безопасности. Ни один из методов не является универсальным; пользователям необходимо выбрать наиболее подходящий. При выборе наиболее подходящего метода следует рассмотреть следующие факторы:

1) критерии приемлемого риска, которые должны быть выполнены. Если требуется продемонстрировать, что риск был снижен настолько, насколько это практически достаточно, то некоторые методы не подойдут;

2) режим работы функции безопасности. Некоторые методы подходят только для режима с низкой интенсивностью запросов;

3) знания и опыт сотрудников, определяющих уровень полноты безопасности, а также владеющих традиционным подходом в данной области;

4) необходима уверенность в том, что полученный в результате остаточный риск удовлетворяет критериям, указанным организацией-потребителем. Некоторые методы могут давать количественную оценку, а некоторые являются только качественными;

5) можно применять несколько методов. Один метод можно использовать для предварительной оценки с последующим применением более строгого подхода, если предварительная оценка выявляет необходимость более высокого уровня полноты безопасности;

6) тяжесть последствий. Для последствий с многочисленными несчастными случаями с летальным исходом могут быть выбраны более строгие методы;

7) возникает ли для отказов общая причина между Э/Э/ПЭ системами, связанными с безопасностью, или между Э/Э/ПЭ системой, связанной с безопасностью, и причинами запросов.

Какой бы метод ни использовался, все предположения должны быть документально оформлены для дальнейшего управления безопасностью. Все решения должны быть документально оформлены, чтобы можно было подтвердить оценку уровня полноты безопасности; они также должны быть объектом независимой оценки функциональной безопасности.

В.2 Метод ALARP

Принципы ALARP могут быть использованы самостоятельно или в совокупности с другими методами для определения требований уровня полноты безопасности для функции безопасности. Метод ALARP позволяет реализовать качественный и количественный подходы. При использовании качественного метода требования к уровню полноты безопасности для определенной функции безопасности увеличивают до тех пор, пока частота событий не уменьшится настолько, что будут выполнены условия, связанные с рисками класса II или класса III. При использовании количественного метода частоты и последствия событий заданы в числовых значениях и требования к уровню полноты безопасности увеличивают до тех пор, пока можно показать, что дополнительные и текущие расходы, связанные с реализацией более высокого уровня полноты безопасности, удовлетворят условиям риска класса II или класса III (см. рисунок С.1).

При использовании метода ALARP следует учитывать границу между недопустимым уровнем и ALARP.

В.3 Количественный метод определения уровня полноты безопасности

Количественный метод описан в приложении G. Он может быть использован в совокупности с методом ALARP, описанным в приложении С.

Количественный метод может быть использован как в простых, так и в сложных случаях. В сложных случаях можно построить дерево ошибок для отображения модели опасности. Конечным событием, как правило, является один или несколько случаев с летальным исходом, а логика отображает причины запросов и отказы Э/Э/ПЭ систем, связанных с безопасностью, которые приводят к конечному событию. Если для реализации функций управления и защиты используется один и тот же тип оборудования, то для моделирования отказов по общей причине применяются программные средства. В некоторых сложных случаях единичный отказ может произойти в более чем одном месте на дереве ошибок и это потребует проведения логического упрощения. Эти инструменты также содействуют анализу чувствительности, который выявляет главные факторы, влияющие на частоту конечного события. Уровень полноты безопасности может быть установлен путем определения требуемого снижения риска для достижения критерия допустимого риска.

Этот метод подходит для функций безопасности, работающих в режиме с непрерывным запросом/режиме с высокой частотой запросов и в режиме с низкой частотой запросов. Метод обычно дает низкие уровни полноты безопасности, так как модель риска специально разработана для каждого применения, а для представления каж-

дого фактора риска используются числовые значения, а не числовые диапазоны, используемые в калиброванных графах риска. Однако количественные методы требуют построения специальной модели для каждого опасного события. Моделирование требует навыков, инструментов и знаний в области применения, а также может занять значительное время на разработку и проверку модели.

Этот метод позволяет продемонстрировать, что риск был снижен до практически осуществимого низкого уровня. Это можно сделать, рассматривая возможности дальнейшего снижения риска, включая в модель дерева ошибок для каждой возможности дополнительные средства и затем, определив полученное сокращение риска, сравнить его со стоимостью каждой такой возможности.

В.4 Метод графа рисков

В приложении Е описан качественный метод графа рисков. Этот метод позволяет определить уровень полноты безопасности, основываясь на знании факторов риска, связанного с УО и системой управления УО. Вводятся несколько параметров, которые вместе описывают природу опасной ситуации при отказе систем, связанных с безопасностью, или при их недоступности. Из каждого из четырех наборов выбирается один параметр; выбранные параметры затем объединяются для принятия решения об уровне полноты безопасности, распределенном по функциям безопасности. Этот метод широко использовался в сфере машиностроения, см.

ИСО 14121-2 [10] и ИСО 13849-1, приложение А [11].

Этот метод может быть качественным; в таком случае выбор параметров субъективен и требует значительного обдумывания. Остаточный риск не может быть рассчитан из значений параметров. Он не применим, если организации требуется уверенность в том, что риск снижен до заданного числового значения.

Числовые значения параметров можно получить с помощью калибровки графа рисков по числовым критериям приемлемости риска. Зная числовые значения каждого параметра, можно получить остаточный риск. Метод можно применять, если организации требуется уверенность в том, что остаточный риск снижен до указанного числового значения. Опыт показал, что использование метода калиброванного графа рисков может дать высокие уровни полноты безопасности. Причиной является то, что калибровка обычно проводится с использованием наихудших значений по каждому параметру. Каждый параметр имеет диапазон в один десятичный порядок, поэтому в случаях, где все параметры – средние для диапазона, уровень полноты безопасности будет на единицу выше, чем необходимо для допустимого риска. Этот метод широко используется для процессов и в секторе морского судоходства.

Метод графа рисков не учитывает отказы по общей причине среди причин запросов и причину отказа Э/Э/ПЭ системы, связанной с безопасностью, или вопросы, связанные с общей причиной, для других слоев защиты.

В.5 Анализ слоя защиты (АСЗ)

Основной подход метода широко представлен в литературе и применяется в разнообразных модификациях. В приложении F описано применение этого метода для определения уровня полноты безопасности.

Этот метод является количественным, и пользователю необходимо определить допустимые частоты и тяжести последствий для каждого слоя. Слоям защиты, снижающим частоту причин отдельных запросов, задается числовое значение такого снижения. Не все слои защиты связаны со всеми причинам запросов, поэтому рассматриваемый метод может быть применен в более сложных случаях. Числовые значения, задаваемые слоям защиты, могут быть округлены в большую сторону до следующей значащей цифры или следующего значащего десятичного значения. Если числовые значения слоев защиты округлены до следующей значащей цифры, метод в среднем дает более низкие значения требований по снижению риска и более низкие значения уровня полноты безопасности, чем калиброванные графы рисков.

Так как задаваемым величинам тяжести последствий для слоев задаются числовые целевые значения, то пользователь может быть уверен, что остаточный риск удовлетворяет корпоративным критериям.

Описанный метод не применим для функций, работающих в режиме с непрерывным запросом, и не учитывает отказов по общей причине между причинами запросов и Э/Э/ПЭ системами, связанными с безопасностью. Однако этот метод можно скорректировать для таких случаев.

Б.6 Матрица тяжести опасных событий

Метод тяжести опасных событий описан в приложении G. Неотъемлемым допущением является то, что добавление слоя защиты должно обеспечить снижение значения риска на один порядок. Следующее допущение состоит в том, что слои защиты независимы от причины запросов и друг от друга. Описанный метод не применим для функций, работающих в режиме с непрерывным запросом. Метод может быть качественным; в этом случае выбор факторов риска субъективен и требует серьезного обоснования. Остаточный риск нельзя рассчитать, зная выбранные факторы риска. Метод не применим, если организации требуется уверенность, что остаточный риск снижен до указанного количественного значения.

Приложение С
(справочное)

ALARP и концепции допустимого риска

С.1 Общие положения

В настоящем приложении рассматривается один частный подход к достижению допустимого риска. В приложении нет подробного описания метода, даны только основные принципы. Этот подход включает процесс постоянного улучшения, где все возможности, которые могут сократить риски, впоследствии анализируются с точки зрения их преимуществ и затрат. Желающие использовать методы, указанные в этом приложении, должны обратиться к первоисточнику [4].

С.2 Модель ALARP

С.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 с 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 достаточно (последняя фраза на английском языке “as low as reasonably practicable” и образует аббревиатуру ALARP). Если риск находился между областью недопустимого риска и областью приемлемого риска и был использован принцип ALARP, то результирующий риск является допустимым риском для конкретного применения. Такой подход, использующий три области, показан на рисунке С.1.

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

Ниже этого уровня находится область допустимого риска, в которой деятельность может производиться при условии, что риски будут сделаны настолько малыми, насколько это практически достаточно. Допустимый риск отличается от приемлемого 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 на его снижение. На границе области допустимого 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 допустимого риска баланс между затратами и выгодами может оказаться удовлетворительным.

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

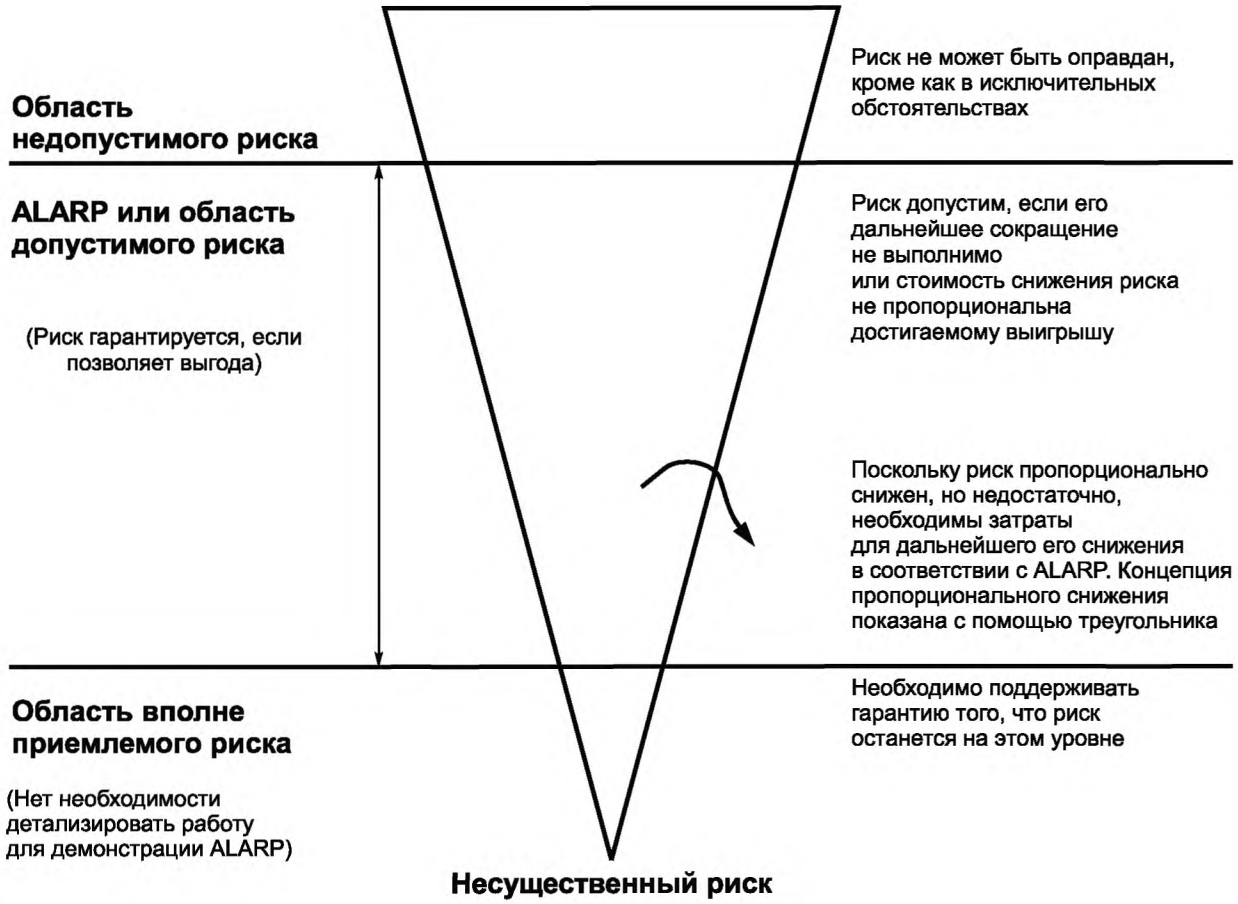


Рисунок С.1 – Допустимый риск и ALARP

Концепция ALARP может быть использована тогда, когда приняты качественные или количественные целевые значения риска. В С.2.2 описан метод количественной оценки риска. (В приложениях D и F описываются количественные методы, а в приложениях E и G – качественные методы определения требуемого снижения риска для конкретной опасности; указанные методы могут включать концепцию ALARP на стадии принятия решений).

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

С.2.2 Целевой допустимый риск

Один из путей получения целевого 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).

Чтобы использовать принцип ALARP, надо установить соответствие между последствиями риска и приемлемой частотой его возникновения, что может быть сделано, введением классов риска. В таблице С.1 в качестве примера приводятся три класса (I, II, III) для разных частот возникновения риска и разных вариантов его последствий. В таблице С.2 дается интерпретация каждого из классов риска на базе концепции ALARP. Описание каждого из классов риска выполняется на основе рисунка С.1. Подразумевается, что риски, определенные внутри каждого из классов, – это риски, по отношению к которым уже приняты меры по их снижению.

Согласно рисунку С.1 можно выделить следующие три класса рисков:

- 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 явно приемлемых рисков.

Для каждой конкретной ситуации или для сравнимых промышленных отраслей может быть разработана таблица, аналогичная таблице С.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 С.1 может обозначать событие, которое будет встречаться постоян-

но, 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 С.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
Неправдоподобные	IV	IV	IV	IV

Примечания

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

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

Таблица С.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 D
(справочное)

Определение уровней полноты безопасности. Количественный метод

D.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 С.1 и подобных ей таблицах. Количественный подход приобретает особое значение, когда:

- допустимый риск должен быть 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 (см. 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.

D.2 Общее описание метода

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

- установить допустимый риск при помощи таблицы, подобной таблице С.1;
- установить риск УО;
- установить необходимое снижение риска для достижения допустимого риска;
- распределить необходимое снижение риска между Э/Э/ПЭ системами, связанными с безопасностью, системами, связанными с безопасностью, основанными на других технологиях, и другими средствами снижения риска (см. МЭК 61508-1, подраздел 7.6).

Таблица С.1 содержит частоты возникновения риска и позволяет определить численное значение целевого допустимого риска (F_t).

Частота, связанная с риском, создаваемым УО, включая систему управления УО и вопросы, связанные с человеческим фактором (риск УО), но без учета каких-либо мер защиты, может быть определена с использованием количественных методов оценки риска. Частота возникновения опасного события в отсутствие средств защиты $F_{пр}$ представляет собой один из двух компонентов риска УО; другим компонентом является последствие опасного события. $F_{пр}$ 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 УО (см. МЭК 61508-1, подпункт 7.5.2.5). Если задано, что система управления УО имеет интенсивность отказов меньше минимальной, то система управления УО должна рассматриваться как система, связанная с безопасностью, и должна быть объектом всех требований к системам, связанным с безопасностью, содержащихся в настоящем стандарте.

D.3 Пример расчетов

На рисунке D.1 представлен пример расчета необходимой полноты безопасности для единичной системы защиты, связанной с безопасностью. Для этого примера

$$PFD_{avg} \le F_t / F_{пр},$$

где PFD_{avg} – средняя вероятность отказа по запросу системы защиты, связанной с безопасностью, которая является целевой мерой отказов для систем защиты, связанных с безопасностью и работающих в режиме низкой интенсивности запросов (см. МЭК 61508-1, таблица 2 и МЭК 61508-4, пункт 3.5.12);

F_t – частота для допустимого риска;

$F_{пр}$ – интенсивность запросов к системе защиты, связанной с безопасностью.

Также на рисунке D.1:

- C – это последствие опасного события;
- F_p – это частота, с которой данное место подвергается риску с учетом функций защиты.

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

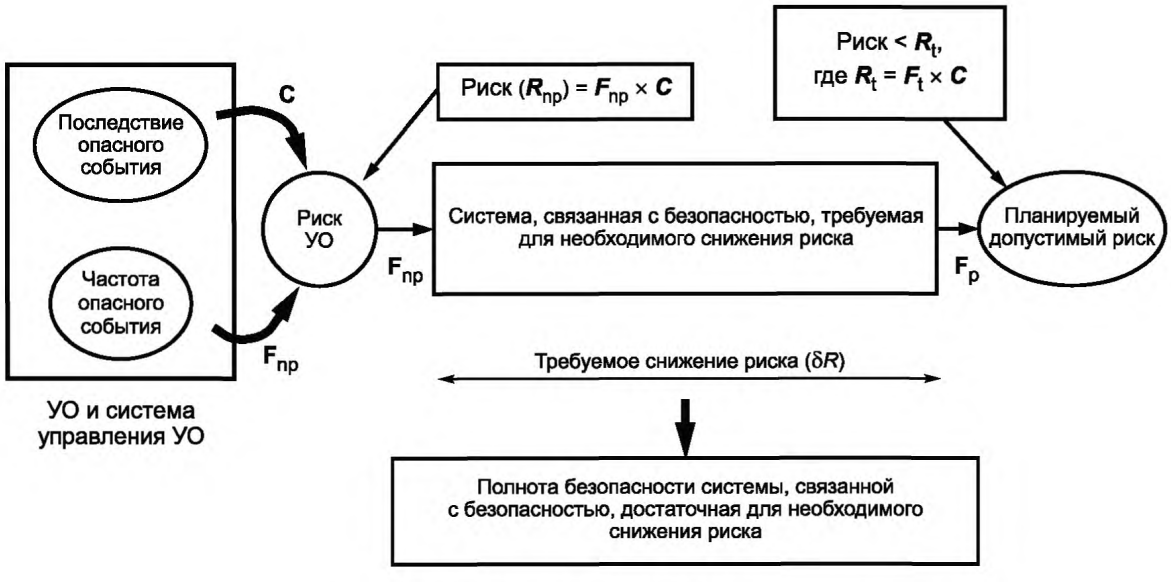
Шаги, которые должны быть выполнены при определении уровня полноты безопасности (когда последствие *C* остается неизменным), приведены ниже (они также показаны на рисунке D.1) для ситуации, при которой необходимое снижение риска целиком достигается за счет одной системы защиты, связанной с безопасностью, которая должна снизить интенсивность возникновения опасностей как минимум с F_{np} до F_t:

- определить частотную составляющую риска УО без учета каких-либо средств защиты (F_{np});
- определить последствие *C* без учета каких-либо средств защиты;
- определить, используя таблицу С.1, достигается ли для частоты F_{np} и последствия *C* допустимый уровень риска. Если при использовании таблицы С.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 С.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 ΔR. Для постоянного последствия в описанной конкретной ситуации $PFD_{avg} = (F_t / F_{np}) = \Delta R$;
- для $PFD_{avg} = (F_t / F_{np})$ 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_{np} до F_t.



C – последствие опасного события;
F_p – частота опасного события при установленных средствах защиты

Рисунок D.1 – Назначение полноты безопасности: пример для системы, связанной с безопасностью

Приложение Е
(справочное)

Определение уровней полноты безопасности. Методы, основанные на графе рисков

Е.1 Общие положения

Настоящее приложение описывает метод графа рисков, который позволяет определить уровень полноты безопасности системы, связанной с безопасностью, на основе знаний факторов риска, связанных с УО и системой управления УО. Он применим, в частности, когда модель риска соответствует той, которая показана на рисунках А.1 и А.2. Этот метод может быть использован как для получения качественного, так и количественного результата.

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 функциям безопасности. Эти параметры:

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

В настоящем приложении нет подробного описания метода, а дана иллюстрация его основных принципов.

Е.2 Построение графа риска

Упрощенная процедура, описываемая ниже, основывается на следующем уравнении:

$$R = (f) \text{ для заданного } C,$$

где R – риск при отсутствии системы, связанной с безопасностью;

f – частота опасного события без применения системы, связанной с безопасностью;

C – последствие опасного события (последствия должны быть связаны с ущербом, связанным со здоровьем и безопасностью или с ущербом от вреда 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:

- последствие опасного события (C);
- частота и время нахождения в опасной зоне(F);
- вероятность того, что опасности можно избежать (P);
- вероятность нежелательного события (W).

Параметры риска могут быть определены качественно, как описано в таблице Е.1, либо количественно, как описано в таблице Е.2. При определении числовых значений по каждому параметру в таблице Е.2 потребуется процесс калибровки.

Е.3 Калибровка

Задачи процесса калибровки следующие:

- описать все параметры таким образом, чтобы дать возможность команде, занимающейся оценкой уровня полноты безопасности, сделать объективное заключение, основанное на характеристиках применения;
- обеспечить соответствие выбранного для данного применения уровня полноты безопасности корпоративному критерию риска и обеспечить при определении уровня полноты безопасности учет возможного риска со стороны других источников;
- обеспечить проверку процесса выбора параметров.

Калибровка графа риска – это процесс присвоения числовых значений параметрам графа риска. При этом формируется основа для оценки риска существующего процесса и оказывается возможным определить требуемую полноту безопасности рассматриваемой функции безопасности приборной системы безопасности. Каждому параметру присваивается диапазон значений, которые, будучи применены в комбинации, позволяют получить количественную оценку риска, существующего в отсутствии данной функции безопасности. Так устанавливается мера степени доверия функции безопасности. Граф риска связывает определенные комбинации параметров риска с уровнем полноты безопасности. Связь между комбинациями параметров риска и уровнем полноты безопасности устанавливается путем рассмотрения величины допустимого риска, связанного с конкретной опасностью.

Рассматривая калибровку графа риска, важно принять во внимание требования к риску, возникающие как со стороны собственников, так и со стороны регламентирующих органов. Риски для жизни могут быть проанализированы многими способами, как описано в А.2 и приложении С.

Если необходимо снизить частоту отдельных несчастных случаев с летальным исходом до определенного максимально допустимого уровня, то нельзя полагать, что такое снижение риска может быть достигнуто применением какой-либо одной Э/Э/ПЭ системы, связанной с безопасностью. Лицо, подвергаемое риску, может находиться под воздействием многих его источников (например риски падения, пожара, взрыва). При калибровке необходимо учитывать количество видов опасности, которым подвергаются люди, а также общее время, проведенное в зоне риска.

При рассмотрении требуемой степени снижения риска организация может исходить из критериев, связанных с приращением стоимости устранения фатального исхода. Эту величину можно подсчитать, разделив суммированные за год расходы на дополнительное оборудование и технику, обеспечивающие увеличение полноты безопасности, на приращение сокращения риска. Дополнительный уровень полноты безопасности считается оправданным, если приращение затрат на устранение фатального исхода оказывается меньше предусмотренного ранее значения.

Все эти соображения следует принять во внимание перед тем, как установить значения каждого из параметров. Большинству параметров присваивается определенный диапазон (например, если ожидаемая частота запроса оказывается в пределах определенного уровня значений запросов в год, то можно использовать параметр W_3). Аналогично, в случае запросов, имеющих частоту ниже на порядок, применяется параметр W_2, а на следующем, еще более низком уровне, – параметр W_1. Присвоение каждому параметру определенного уровня помогает команде специалистов принять решение о том, какое значение параметра выбрать для конкретного объекта. Для калибровки графа риска каждому параметру присваивается или численное значение, или определенный диапазон. Затем риск, связанный с каждой комбинацией параметров, оценивается по заданным критериям риска. Описания параметра далее модифицируются, чтобы заданные критерии риска были достигнуты для всех комбинаций всех значений параметров. В примере калибровки, показанном в таблице Е.2, вводится фактор «*D*» для того, чтобы диапазон запросов, связанных с каждым фактором *W*, мог быть модифицирован для достижения допустимого риска. В некоторых случаях необходимо модифицировать диапазоны, связанные с другими факторами риска, для отражения значений параметров, встречающихся в рассматриваемых применениях. Калибровка – это итеративный процесс; он продолжается, пока критерии приемлемости указанного риска не будут выполнены для всех комбинаций значений параметров.

Работу по калибровке не нужно проводить каждый раз, когда необходимо определить уровень полноты безопасности для конкретного применения. Обычно организациям необходимо сделать это только один раз для похожих опасностей. Для конкретных проектов может понадобиться корректировка, если первоначальные предположения, сделанные во время калибровки, признаны неподходящими для этих конкретных проектов.

Если оценки параметров выполнены, то необходимо располагать информацией о том, как эти оценки были получены.

Важно, чтобы этот процесс калибровки был согласован в организации с сотрудником на уровне руководства, отвечающим за безопасность. Принятые решения определяют общий достигнутый уровень безопасности.

В общем случае с помощью графа риска сложно определить возможность существования зависимого отказа между источниками запроса и оборудованием, используемым в Э/Э/ПЭ системе, связанной с безопасностью. При этом может потребоваться провести переоценку эффективности Э/Э/ПЭ системы, связанной с безопасностью. Если графы рисков калиброваны и для значений интенсивностей запросов больше, чем один раз в год, то требования уровней полноты безопасности, полученные в результате применения такого графа рисков, могут быть выше, чем необходимо. В таких случаях рекомендуется использовать другие методы.

Е.4 Другие возможные параметры риска

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

Е.5 Построение графа риска: общая схема

Объединение параметров риска, описанных выше, позволяет построить граф риска, подобный тому, который показан на рисунке Е.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 области применения, для которой строится граф риска). На рисунке Е.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 Э/Э/ПЭ системой, связанной с безопасностью. На практике могут встречаться ситуации, когда одна Э/Э/ПЭ система, связанная с безопасностью, не может обеспечить требуемого уменьшения риска.

- Отображение на W_1, W_2 или W_3 позволяет учесть вклад других средств снижения риска. Смещение шкал W_1, W_2 и W_3 позволяет учесть три различных уровня уменьшения риска, обеспечиваемого другими средствами. Так, шкала W_3 дает минимальное уменьшение риска за счет других средств (т. е. наибольшую вероятность того, что произойдет нежелательное событие); шкала W_2 соответствует промежуточному по величине вкладу других средств, 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 Э/Э/ПЭ систем, связанных с безопасностью, (т. е. 1, 2, 3 или 4). Они представляют собой оценку требуемого снижения риска для данной системы. Это снижение риска вместе со снижением риска, достигаемым другими средствами (например, с помощью систем, связанных с безопасностью, основанных на других технологиях и других средств снижения риска) и учитываемым с помощью механизма шкалы W, дает требуемое снижение риска для конкретной ситуации.

Параметры, указанные на рисунке Е.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 областей применения.

Е.6 Пример графа рисков

Пример графа рисков, основанный на данных, приведенных в таблице Е.1, показан на рисунке Е.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.

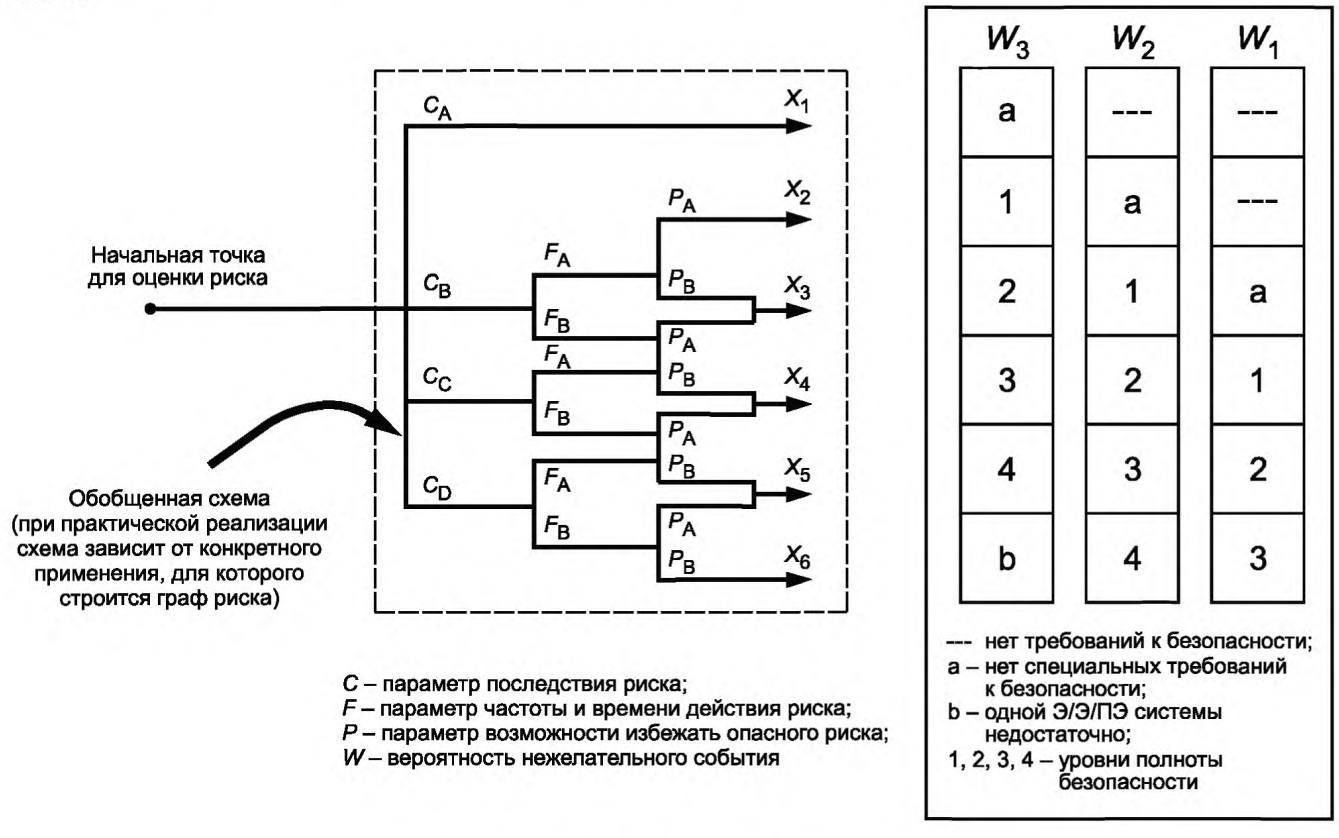
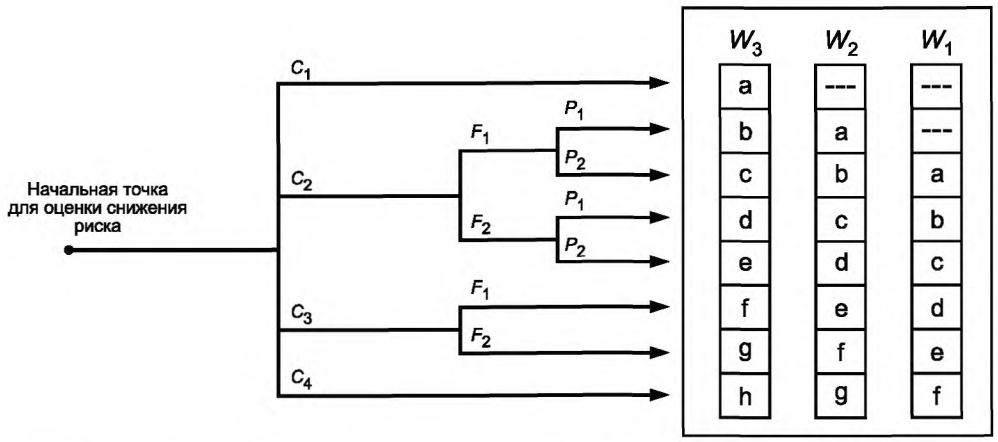


Рисунок Е.1 – Граф риска: общая схема



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 последствия 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 снижения риска для Э/Э/ПЭ 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	Э/Э/ПЭ системы, связанной с безопасностью, недостаточно

Рисунок Е.2 – Граф риска: пример (показывает только общие принципы)

Таблица Е.1 – Данные для графа рисков (рисунок Е.2)

Параметр риска		Классификация	Комментарии
Последствие *C*	C_1 C_2 C_3 C_4	Небольшая травма. Серьезная постоянная травма у одного или нескольких человек. Смерть нескольких человек. Смерть очень многих людей	1 Данная система классификации основана на травмах и смерти людей. В случае ущерба окружающей среде или материального ущерба может потребоваться разработка других схем классификации. 2 Для интерпретации параметров C_1, C_2, C_3 и C_4 необходимо учитывать последствия несчастных случаев и потребность в лечении
Частота и продолжительность пребывания в опасной зоне *F*	F_1 F_2	От редкого до частого пребывания в опасной зоне. От частого до постоянного пребывания в опасной зоне	3 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 P_2	Возможно при определенных обстоятельствах. Почти невозможно	4 Данный параметр учитывает: - тип операций процесса [контролируемых (т. е. управляемых подготовленным или неподготовленным персоналом) или неконтролируемых]; - скорость развития опасного события (например: внезапное, быстрое или медленное); - легкость распознавания опасности (например: видна сразу, обнаруживается техническими средствами или обнаруживается без использования технических средств); - возможность избежать опасного события (например: возможно отступление, отступление невозможно либо отступление возможно при определенных обстоятельствах); - реальный опыт в области техники безопасности (такой опыт может быть для идентичного УО, для сходного УО либо отсутствовать)

Окончание таблицы Е.1

Параметр риска		Классификация	Комментарии
Вероятность нежелательного события W	W_1	Весьма незначительная вероятность нежелательного события, возможно только небольшое число таких событий.	5 Назначение параметра W состоит в том, чтобы оценить частоту нежелательных событий в условиях отсутствия каких либо систем, связанных с безопасностью (Э/Э/ПЭ систем или систем, основанных на других технологиях), но с учетом внешних средств снижения риска.
	W_2	Небольшая вероятность нежелательного события, возможно небольшое число таких событий.	6 При отсутствии или незначительности опыта использования УО или систем управления УО оценка параметра W может быть проведена с помощью расчетов, которые в таком случае должны представлять собой прогноз для наихудшего случая
	W_3	Относительно высокая вероятность наступления нежелательного события, вероятны частые повторения нежелательного события	

Т а б л и ц а Е.2 – Пример калибровки графа рисков общего назначения

Параметр риска		Классификация	Комментарии
Последствия (C) Число фатальных исходов. Подсчитывается умножением числа людей, находящихся в опасной области, на уязвимость к определенной опасности. Уязвимость определяется природой опасности, от которой осуществляется защита. Могут использоваться следующие факторы: V=0,01 Небольшой выброс воспламеняющихся или токсичных материалов. V=0,1 Большой выброс воспламеняющихся или токсичных материалов. V=0,5 То же, что и выше, но велика вероятность возгорания, либо отравление высокотоксичными материалами. V=1 Разрушение или взрыв	C_A C_B C_C C_D	Незначительные травмы Диапазон 0, 01 до 0, 1 Диапазон >0, 1 до 1,0 Диапазон > 1,0	1 Система классификации отно-сится к случаям фатального исхода или травм для людей. 2 При интерпретации параметров C_A, C_B, C_C и C_D, следует учитывать последствия несчастного случая и квалифицированное его устранение
Пребывание (нахождение) (F) Определяется как доля времени пребывания людей в месте, подвергающемуся опасности, по отношению к величине рабочего времени. Примечания 1 Если время пребывания в опасной области различно для различных смен, то следует выбирать наибольшее время. 2 Величину F_A следует применять только в тех случаях, когда частота запроса случайна и не зависит от того, превышает ли нахождение обычное значение. Последнее характерно для случаев, когда запросы возникают при пуске оборудования или во время изучения ненормальных ситуаций	F_A F_B	От редкого до более частого нахождения в опасной области. Обитаемость меньше, чем 0,1. От частого до постоянного пребывания в опасной области	3 См. комментарий 1 выше
Вероятность избежать опасного события (P), если отказывает система защиты	P_A P_B	Принимается, если выполняются условия в комментарии 4. Принимается, если условия не выполняются	4 P_A следует выбирать, только если справедливы следующие условия: - предусмотрены средства оповещения оператора об отказе приборной системы безопасности; - предусмотрены независимые средства останова процесса, так чтобы избежать опасности или позволить персоналу эвакуироваться в безопасную зону; - время между оповещением оператора и опасным событием превышает 1 час или вполне достаточное для выполнения необходимых действий

Окончание таблицы Е.2

Параметр риска		Классификация	Комментарии
Интенсивность запросов (W) Количество случаев в год, когда опасное событие возникает при отсутствии Э/Э/ПЭ системы, связанной с безопасностью. Чтобы определить частоту запроса, необходимо рассмотреть все причины отказа, которые могут привести к возникновению одного и того же опасного события. При определении интенсивности запросов роль системы управления и ее вмешательство в ход процесса следует учитывать в минимальной степени. Если система спроектирована и эксплуатируется не в соответствии с МЭК 61508, то ее функционирование ограничено уровнем безопасности ниже, чем УПБ1	W_1 W_2 W_3	Частота запросов меньше, чем 0,1 D в год Частота запросов лежит в диапазоне 0,1 D и D в год Частота запросов лежит в диапазоне D и 10 D в год При частотах запросов, больших, чем 10 D, потребуется более высокий уровень полноты безопасности	5 Цель введения фактора W – оценить частоту возникновения опасности без применения Э/Э/ПЭ систем, связанных с безопасностью. Если частота запроса очень велика, то уровень полноты безопасности следует определять либо другим методом, либо путем перекалибровки графа риска. Следует отметить, что методы графа риска могут оказаться не лучшим решением задачи, если объект работает в непрерывном режиме (см. МЭК 61508-4, пункт 3.5.16). 6 Значение D следует определять исходя из корпоративного критерия допустимого риска с учетом других источников риска для людей, ему подвергающихся
Примечание – Этот пример предназначен для иллюстрации принципов построения графов риска. Граф риска для конкретного применения и конкретных опасных ситуаций должен быть согласован с условиями, учитываемыми при определении допустимого риска (см. Е.1 – Е.6).			

Приложение F
(справочное)

Полуколичественный метод, использующий анализ слоя защиты

F.1 Общая информация

F.1.1 Описание

Настоящее приложение описывает метод под названием анализ слоя защиты (АСЗ). Настоящее приложение не призвано дать определение метода, а предназначено для иллюстрации его основных принципов.

F.1.2 Ссылка приложения

Настоящее приложение основано на методе, описанном более подробно в публикации Американского института инженеров-химиков [5]. В этой публикации содержится множество способов использования методик АСЗ.

В одном подходе все соответствующие параметры округляются до большего десятичного значения (например, вероятность 5×10^{-2} округляется до 10^{-1}). Это очень консервативный подход, он может привести к значительно более высоким уровням полноты безопасности. Однако необходимо учитывать неточности в данных, округляя значения параметров в большую сторону до следующей значимой цифры (например, $5{,}4\times10^{-2}$ должно быть округлено до 6×10^{-2}).

F.1.3 Описание метода

Метод АСЗ используется при проведении анализа опасностей для выяснения того, необходимы ли функции безопасности, и если они необходимы, то определяется требуемый уровень полноты безопасности для каждой функции безопасности. Метод АСЗ необходимо адаптировать к применяемым критериям приемлемого риска. Метод начинает работу с идентификации опасностей. Каждая идентифицированная опасность учитывается документальным оформлением инициирующих ее причин и слоев защиты, которые предотвращают или ослабляют опасность. Затем может быть определено значение общего снижения риска, а также проанализирована необходимость дальнейшего снижения риска. Если потребуется дополнительное снижение риска, и оно будет осуществляться с помощью Э/Э/ПЭ системы, связанной с безопасностью, то методология АСЗ позволит определить подходящий уровень полноты безопасности. Для каждой опасности для снижения рисков до допустимого уровня определяется подходящий уровень полноты безопасности. Таблица F.1 представляет типичную форму для АСЗ.

F.2 Влияющее событие

Описание (последствие) каждого влияющего события, полученное в результате идентификации опасности, заносится в колонку 1 таблицы F.1.

F.3 Уровень тяжести

Значение уровня тяжести события заносится в *колонку* 2 таблицы F.1. Уровень тяжести формируется из таблицы с общими описаниями уровней последствий, например, незначительное, тяжелое, катастрофичное, с указанием диапазонов последствий и максимальной частотой для каждого уровня тяжести. В сущности, эта таблица устанавливает критерии допустимости пользователя. Эта информация понадобится для определения уровней тяжести и максимальных частот для событий, ведущих к последствиям в области безопасности и сохранения окружающей среды.

F.4 Исходные причины

Все причины, инициирующие возникновение опасного события, записываются в колонку 3 таблицы F.1. Опасное событие может иметь много исходных причин, и важно перечислить их все.

F.5 Вероятность возникновения исходных причин

Численное значение вероятности возникновения каждой из исходных причин, перечисленных в колонке 3, измеряемое количеством событий за один год, заносится в колонку 4 таблицы F.1.

Вероятность возникновения может быть рассчитана из общих данных по интенсивностям отказов оборудования и знания интервалов между контрольными проверками, либо из записей по оборудованию. Низкое значение вероятности должно использоваться только в случаях, если существует достаточная статистическая база для таких данных.

Таблица F.1 – Отчет АСЗ

а)	1	2	3	4	5 Слои защиты (СЗ)			6	7	8	9	10	11
	Описание опасного события F.2	Уровень тяжести F.3	Исходная причина F.4	Вероятность появления исходной причины F.5	Общее проектирование F.6.1	Система управления F.6.2	Аварийные сигналы и т.д. F.6.3	Дополнительное смягчение, ограниченный доступ F.7	Дополнительное смягчение F.8	Вероятность промежуточного события F.9	PFD_{avg} требуемый для Э/Э/ПЭ системы (и УПБ) F.10	Допустимая вероятность смягченного события F.11	Примечания
1	Превышение скорости ротора, ведущее к трещине в корпусе	Утрата жизни людей, находящихся поблизости с корпусом, летальные случаи не превышают 2	Отказ системы управления скорости	0,1	1	1	1	0,1	0,1	10^{-3}	$5 \cdot 10^{-3}$ (УПБ. 2 с минимальным PFD_{avg}, равным $5 \cdot 10^{-3}$)	10^{-5}	
			Недозагрузка	1	1	0,1	1	0,1	0,1	10^{-3}			
			Отказ муфты	0,1	1	0,1	1	0,1	0,1	10^{-4}			
						0,1 доверие системе управления		Пребывание людей ограничено, люди отсутствуют 90 % времени	Летальный случай произойдет, если фрагменты будут в зоне досягаемости человека	Всего $2,1 \cdot 10^{-3}$		Допустимая частота, если летальные исходы не превышают 5	
2	Повторить приведенный выше случай для анализа риска окружающей среды												
3				Продолжение при необходимости									
.													
.													
N													

[a] Даны номера колонок и строк, так как их дальнейшие описания включены в приложение F.

Примечания

1 Уровни тяжести события могут быть: C (катастрофический), E (высокий), S (серьезный), M (незначительный). Вероятность допустимого смягченного события зависит от уровня тяжести.

2 Величины в колонках 4, 8 и 10 характеризуются числом событий в год.

3 Величины в колонках 5 - 7 и 9 безразмерные. Числа между 0 и 1 – это факторы, на которые будет умножаться вероятность события для вычисления смягчающего эффекта соответствующего слоя защиты. Таким образом, 1 значит, что смягчающего эффекта нет, а 0.1 обозначает фактор смягчения риска в 10 раз.

F.6 Слои защиты

F.6.1 Общая информация

Каждый слой защиты (СЗ) представляет собой совокупность технических средств и/или организационных мер, которые функционируют независимо от других слоев.

Конструктивные особенности, снижающие вероятность опасного события при возникновении исходной причины, перечислены в колонке 5 таблицы F.1.

СЗ должен обладать следующими важными характеристиками:

- Специфичность: СЗ проектируется специально для того, чтобы предотвратить или ослабить последствия конкретной потенциально опасной ситуации (например, неуправляемая реакция, выброс токсичного материала, разгерметизация аппарата, пожар). Причин возникновения этой опасной ситуации может быть много и, следовательно, действие СЗ может происходить по многим сценариям, вызванным многочисленными исходными событиями.

- Эффективность: СЗ должен самостоятельно предотвращать последствия проблемы, когда все остальные меры оказались совершенно несостоятельными.

- Независимость: СЗ не зависит от других слоев защиты, связанных с тем же выявленным опасным событием.

- Надежность: Можно рассчитывать, что СЗ будет выполнять предназначенные для него функции, если при его проектировании учитываются как случайные, так и систематические отказы.

- Проверяемость: СЗ должен облегчать проведение регулярного подтверждения соответствия функций защиты. При этом необходимы контрольные проверки и техническое обслуживание системы безопасности.

F.6.2 Основнаая система управления

Следующий пункт в колонке 5 таблицы F.1 – это система управления УО. Если функция управления предотвращает влияние опасного события при возникновении исходной причины, то ее влияние характеризуют сокращением средней частоты отказов при наличии запроса (PFD_{avg}). Функцию управления не характеризуют таким сокращением, если отказ этой функции вызывает запрос к Э/Э/ПЭ системе, связанной с безопасностью. Необходимо также иметь в виду, что PFD_{avg}, требуемый от функции управления, должен быть ограничен минимальным значением, равным 0.1, в случае если функция управления не разрабатывалась и не эксплуатируется как система безопасности.

F.6.3 Аварийные сигналы

В последнем столбце колонки 5 таблицы F.1 указывается влияние аварийной сигнализации, которая привлекает внимание оператора и стимулирует его вмешательство в процесс. Требовать доверия к аварийной сигнализации можно только при следующих обстоятельствах:

- Применяемые технические средства и программное обеспечение отделены и независимы от используемых в системе управления (например, входные платы и процессоры не должны быть общими);

- Аварийный сигнал отображается с высокой приоритетностью в месте, где постоянно находятся люди. Требуемое доверие к аварийной сигнализации должно учитывать следующее:

- эффективность аварийных сигналов зависит от сложности задачи, которую необходимо выполнить в случае возникновения аварийного события, а также от других задач, которые необходимо выполнить в это же время;

- доверие к аварийной сигнализации должно быть ограничено минимальным значением величины PFD_{avg}, равным 0.1;

- оператор должен обладать достаточным временем и независимыми средствами для того, чтобы ограничить опасность. Обычно доверие к аварийной сигнализации не требуется, если время доступа к источнику опасности после аварийного сигнала не превышает 20 мин.

F.7 и F.8 Дополнительное смягчение

Смягчающие слои относятся к одной из трех категорий – механические, структурные и процедурные. Примерами могут служить:

- ограниченный доступ;

- снижение вероятности воспламенения;

- любые другие факторы, которые сокращают уязвимость людей, подверженных опасности.

Смягчающие слои могут уменьшить тяжесть последствий нежелательного события, но не предотвращают его возникновение. Примерами могут служить:

- системы пожаротушения водой в случае пожара;

- сигнализация утечки газа;

- процедуры эвакуации персонала, которые могут снизить вероятность нахождения людей в зоне действия развивающегося события.

При смягчении последствий можно учесть процент времени нахождения в опасной зоне наиболее подверженного опасности человека. Этот процент должен быть определен установлением количества часов нахождения в опасной зоне в год, поделенного на 8760 часов в год.

Подходящий PFD_{avg} или эквивалент для всех слоев ослабления должен быть определен и занесен в графы 6 и 7 таблицы F.1.

F.9 Вероятность промежуточного события

Вероятность промежуточного события в каждом случае рассчитывается перемножением перечисленных ниже факторов; результирующая частота за год заносится в графу 8 таблицы F.1:

- уязвимость самого подверженного опасности человека;
- вероятность исходной причины (*графа* 4);
- PFD_{avg} слоев защиты и смягчения (*графы* 5, 6 и 7).

Общая частота промежуточного события вычисляется посредством добавления частот промежуточных событий для каждого случая.

Общая частота промежуточного события должна сравниваться с допустимым риском для соответствующего уровня тяжести последствий. Если общая частота промежуточного события превышает допустимую частоту, то потребуется снижение риска. Перед тем, как применить в качестве дополнительного СЗ Э/Э/ПЭ систему, связанную с безопасностью, необходимо рассмотреть другие, по своей сути более безопасные методы и решения.

Если значение вероятности возникновения промежуточного события не удается сделать меньшим, чем критерий максимальной частоты, то требуется применить Э/Э/ПЭ систему, связанную с безопасностью.

F.10 Уровни полноты безопасности

Если необходима функция безопасности, то требуемые уровни полноты безопасности могут быть определены следующим образом:

- Разделить максимальную частоту для соответствующего уровня тяжести на вероятность общего промежуточного события для определения требуемого PFD_{avg}.
- Затем целевое значение PFD_{avg} может быть использовано в спецификации требований к безопасности вместе с соответствующим уровнем полноты безопасности. Соответствующий уровень полноты безопасности можно взять из МЭК 61508-1, таблица 2.
- Если числовое значение PFD_{avg} отсутствует в спецификации требований к процессу, а указан лишь требуемый уровень полноты безопасности, то уровень полноты безопасности должен быть на один уровень выше, чтобы соответствующее снижение риска было достигнуто по всем значениям PFD_{avg}, связанным с заданным уровнем полноты безопасности.

Если требуемый PFD_{avg} для допустимого риска больше либо равен 0,1, функции присваивается статус «Никаких особых требований к полноте безопасности».

F.11 Допустимая вероятность смягченного события

Допустимая вероятность смягченного события будет зависеть от уровня тяжести последствий. Это будет зависеть от принятых критериев допустимого риска (см. А.2 – критерии допустимых рисков).

Приложение G
(справочное)

Определение уровней полноты безопасности. Количественный метод. Матрица тяжести опасных событий

G.1 Общие положения

Количественный метод, описанный в приложении D, 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 Э/Э/ПЭ системы, связанной с безопасностью, на базе знаний факторов риска, связанных с УО и системой управления УО. Он применим, в частности, для модели риска, показанной на рисунках А.1 и А.2.

В схеме, описываемой в настоящем приложении, предполагается, что каждая система, связанная с безопасностью, и каждое внешнее средство снижения 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 первоисточникам, перечисленным в библиографии.

Примечание – Более подробная информация о матрице опасных событий содержится в [12].

G.2 Матрица тяжести опасных событий

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

a) Э/Э/ПЭ системы, связанные с безопасностью, и другие средства снижения риска являются независимыми;

b) каждая система, связанная с безопасностью (Э/Э/ПЭ и основанная на другой технологии), и другое средство снижения риска рассматривается как отдельный уровень защиты, обеспечивающий своими собственными средствами частичное снижение риска, как показано на рисунке А.1.

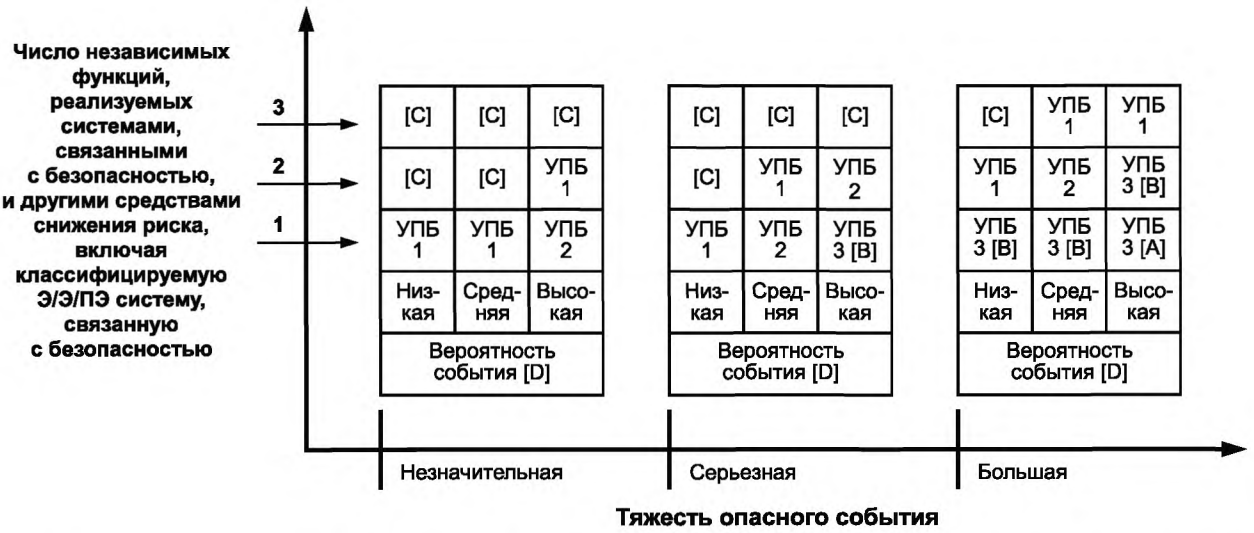
Примечание – Это предположение является справедливым только при условии выполнения систематических контрольных проверок уровней защиты;

c) 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 другие средства снижения риска являются в достаточной степени независимыми;

d) используется только одна Э/Э/ПЭ система, связанная с безопасностью (однако она может применяться в сочетании с системами, связанными с безопасностью, основанными на других технологиях, и/или другими средствами снижения риска), для которой данный метод устанавливает необходимый уровень полноты безопасности;

e) приведенный выше анализ приводит к матрице тяжести опасных событий, показанной на рисунке G.1. Необходимо отметить, что данные, содержащиеся в матрице, представляют собой только пример, иллюстрирующий основные принципы. Для каждой конкретной ситуации или для близких промышленных применений должна быть разработана своя матрица, аналогичная той, которая приведена на рисунке G.1 и прокалибрована в соответствии с критериями допустимого риска для этой ситуации.



A - одна Э/Э/ПЭ система, реализующая функцию безопасности, с УПБ = 3 не обеспечивает достаточного снижения риска для данного уровня риска. Требуются дополнительные меры по снижению риска.

B - одна Э/Э/ПЭ система, реализующая функцию безопасности, с УПБ = 3 может не обеспечить достаточного снижения риска для данного уровня риска. Требуется провести анализ опасностей и рисков для того, чтобы определить, нужны ли дополнительные меры по снижению риска.

C - независимая Э/Э/ПЭ система, реализующая функцию безопасности, по-видимому, не требуется.

D - вероятность события представляет собой вероятность того, что опасное событие произойдет в условиях отсутствия каких-либо систем, реализующих функцию безопасности, и других средств снижения риска.

E - Вероятность события и общее число независимых уровней защиты определяется в зависимости от конкретного применения.

Рисунок G.1 – Пример матрицы тяжести опасных событий (иллюстрирует только основные принципы)

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»
МЭК Руководство 104:1997	–	*
МЭК 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
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 61508-4:2010	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] Health and Safety Executive (UK) publication, ISBN 011 886368 1, Tolerability of risk from nuclear power stations, <gost.e-ecolog.ru >

[5] CCPS ISBN 0-8169-0811-7, Layer of Protection Analysis – Simplified Process Risk Assessment

[6] The Motor Industry Research Association, 1994, ISBN 09524156 0 7, Development guidelines for vehicle based software

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

[8] ISO/IEC 31010:2009, Risk management – Risk assessment techniques

[9] ISO 10418:2003, Petroleum and natural gas industries – Offshore production installations – Basic surface process safety systems

[10] ISO/TR 14121-2, Safety of machinery – Risk assessment – Part 2: Practical guidance and examples of methods

[11] ISO 13849-1:2006, Safety of machinery – Safety-related parts of control systems Part 1: General principles for design

[12] ANSI/ISA S84:1996, Application of safety Instrumented Systems for the Process Industries

УДК 62-783:614.8:331.454:006.354 ОКС 25.040.40 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 *Л.И. Нахимова*
Технический редактор *А.Б. Заварзина*
Корректор *В.Г. Смолин*
Компьютерная верстка *Д.Е. Першин*

Сдано в набор 20.12.2013. Подписано в печать 02.08.2014. Формат 60х841/8. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 3,72. Тираж 71 экз. Зак. 3078.

Набрано в ООО «Академиздат».
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