ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61511-3— 2018

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 3

Руководство по определению требуемых уровней полноты безопасности

(IEC 61511-3:2016, IDT)

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

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

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2018 г. № 467-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61511-3:2016 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности» (IEC 61511-3:2016 «Functional safety — Safety instrumented systems for the process industry sector — Part 3: Guidelines for the determination of the required safety integrity levels», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочного международного стандарта соответствующий ему национальный стандарт, сведения о котором приведены в дополнительном приложении ДА

5 ВЗАМЕН ГОСТ Р МЭК 61511-3—2011

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2018

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 2
3 Термины, определения и сокращения . . . 2
Приложение A (справочное) Риск и полнота безопасности. Общие требования . . . 3
Приложение B (справочное) Полуколичественный метод. Анализ дерева событий . . . 8
Приложение C (справочное) Метод матрицы слоев безопасности . . . 15
Приложение D (справочное) Полукачественный метод. Калиброванный граф риска . . . 19
Приложение E (справочное) Качественный метод. Граф риска . . . 26
Приложение F (справочное) Анализ слоев защиты . . . 29
Приложение G (справочное) Анализ слоев защиты, используя матрицу риска . . . 35
Приложение H (справочное) Качественный подход для оценки риска и назначение уровня полноты безопасности (УПБ) . . . 49
Приложение I (справочное) Создание и калибровка графа риска . . . 59
Приложение J (справочное) Многоконтурные системы безопасности . . . 63
Приложение K (справочное) Принцип снижения риска настолько, насколько это практически целесообразно (принцип ALARP), и концепция приемлемого риска . . . 73
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам . . . 75

Введение

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

Область применения комплекса стандартов МЭК 61511 — ПСБ, применяемые в промышленных процессах. Комплекс стандартов МЭК 61511 также рассматривает проведение анализа опасности и риска процесса для обеспечения формирования спецификации приборных систем безопасности. Вклад других систем безопасности учитывается только по отношению к требованиям к эффективности приборных систем безопасности. ПСБ включает все устройства, необходимые для выполнения каждой ФБ ПСБ, — от датчика(ов) до исполнительного(ых) элемента(ов).

В основе комплекса стандартов МЭК 61511 лежат две фундаментальные концепции, необходимые для ее применения: концепция жизненного цикла системы безопасности и концепция уровней полноты безопасности (УПБ).

Комплекс стандартов МЭК 61511 рассматривает ПСБ, использующие электрические/электронные/программируемые электронные технологии. Если для логических устройств используют другие принципы действия, то следует применять основные положения МЭК 61511, чтобы гарантировать выполнение требований к функциональной безопасности. Комплекс стандартов МЭК 61511 также рассматривает датчики и исполнительные элементы ПСБ независимо от принципа их действия. Комплекс стандартов МЭК 61511 является конкретизацией для промышленных процессов общего подхода к вопросам обеспечения безопасности, представленного в комплексе стандартов МЭК 61508:2010.

Комплекс стандартов МЭК 61511 устанавливает подход, минимизирующий стандартизацию деятельности для всех стадий жизненного цикла ПСБ. Этот подход был принят в целях реализации рациональной и последовательной технической политики.

В большинстве ситуаций безопасность лучше всего может быть достигнута с помощью проектирования безопасного в своей основе процесса. Но при необходимости процесс может быть дополнен системами защиты или системами, с помощью которых достигается любой установленный остаточный риск. Системы защиты основаны на применении различных технологий: химических, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных. Любая стратегия обеспечения безопасности должна рассматривать каждую конкретную ПСБ в контексте других систем защиты. Для облегчения применения такого подхода комплекс стандартов МЭК 61511:

- требует, чтобы выполнялась оценка опасностей и рисков для определения общих требований к безопасности;
- требует, чтобы выполнялось распределение требований к безопасности в (по) приборной(ым) системе(ам) безопасности;
- реализует подход, который применим ко всем приборным мерам обеспечения функциональной безопасности;
- подробно рассматривает применение определенных действий по управлению безопасностью, которые могут быть применены ко всем методам обеспечения функциональной безопасности;
- охватывает все стадии жизненного цикла системы безопасности — от разработки первоначальной концепции, проектирования, внедрения, эксплуатации и технического обслуживания вплоть до утилизации;
- дает возможность, чтобы существующие или новые стандарты в разных странах, регламентирующие конкретные промышленные процессы, были с ним гармонизированы.

Комплекс стандартов МЭК 61511 призван привести к высокому уровню согласованности (например, основных принципов, терминологии, информации) в рамках конкретных промышленных процессов. Это принесет преимущества как в плане безопасности, так и в плане экономики.

В пределах своей юрисдикции соответствующие регулирующие органы (например, национальные, федеральные, штата, провинции, округа, города) могут устанавливать такие правила к процессу проектирования системы безопасности, к процессу управления безопасностью или другие правила, которые должны превалировать над требованиями, определенными в МЭК 61511-1.

Настоящий стандарт содержит руководство по определению требуемых уровней полноты безопасности, используя анализ опасности и риска (АОР). Содержащаяся в настоящем стандарте информация предназначена для проведения глубокого анализа различных общих методов применения АОР. Для применения любого из этих методов представленной информации недостаточно.

Перед применением настоящего стандарта следует ознакомиться с концепцией и определением понятия «уровень полноты безопасности», приведенными в МЭК 61511-1:2016. Приложения к настоящему стандарту рассматривают следующие вопросы:

Приложение A содержит общую информацию для всех рассматриваемых ниже методов оценки различных опасностей и рисков.

Приложение B содержит обзор полуколичественного метода определения требуемого УПБ.

Приложение C содержит обзор метода матриц безопасности для определения требуемого УПБ.

Приложение D содержит обзор метода, использующего для определения требуемого УПБ полукачественный подход графа рисков.

Приложение E содержит обзор метода, использующего для определения требуемого УПБ качественный подход графа рисков.

Приложение F содержит обзор метода, использующего для выбора требуемого УПБ анализ слоев защиты (АСЗ).

Приложение G содержит анализ слоев защиты, использующий матрицу риска.

Приложение H содержит обзор качественного подхода для оценки риска и назначения УПБ.

Приложение I содержит обзор основных этапов проектирования и калибровки графа рисков.

Приложение J содержит обзор влияния многоконтурных систем безопасности на определение требуемого УПБ.

Приложение K содержит обзор основных положений метода приемлемого риска и метода ALARP.

На рисунке 1 представлена общая структура комплекса стандартов МЭК 61511 и показана роль, которую комплекс стандартов МЭК 61511 играет в достижении функциональной безопасности для ПСБ.

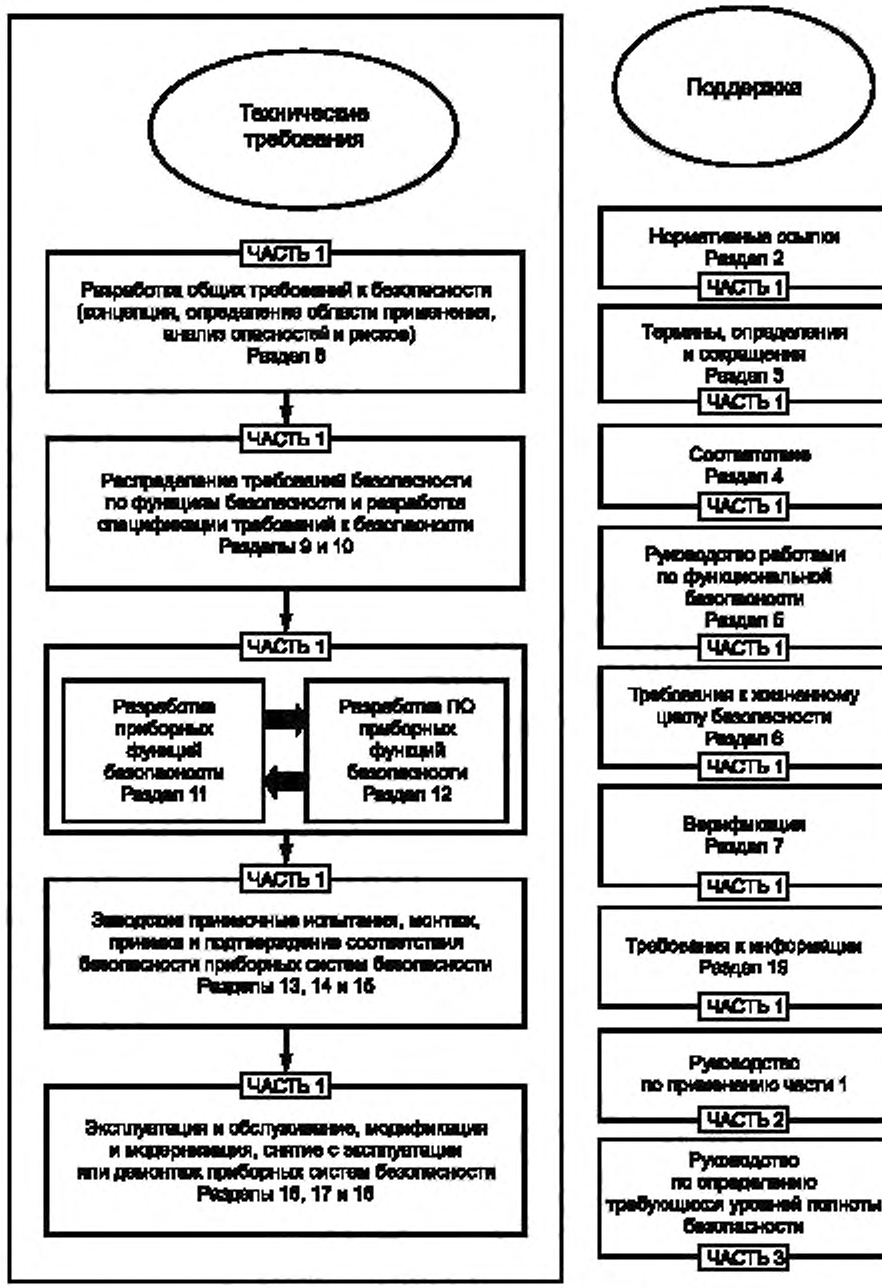


Рисунок 1 — Общая структура комплекса стандартов МЭК 61511

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

БЕЗОПАСНОСТЬ ФУНКЦИОНАЛЬНАЯ

Системы безопасности приборные для промышленных процессов

Часть 3

Руководство по определению требуемых уровней полноты безопасности

Functional safety. Safety instrumented systems for the process industry sector.
Part 3. Guidelines for the determination of the required safety integrity levels

Дата введения — 2019—07—01

1 Область применения

Настоящий стандарт содержит:

- основные положения концепции риска и описание отношения между риском и полнотой безопасности (см. А.4, приложение А);
- определение допустимого риска (см. приложение К);
- описание различных методов, позволяющих определить уровень полноты безопасности (УПБ) для функций безопасности ПСБ (см. приложения В—К);
- влияние многоконтурных систем безопасности на вычисления, определяющие способность достигнуть желаемого снижения риска (см. приложение J).

В частности, настоящий стандарт:

a) применяют в случаях, когда функциональная безопасность достигается путем использования одной или более функций безопасности ПСБ для защиты персонала, населения или окружающей среды;

b) может быть применен на объектах, не требующих обеспечения безопасности, например для защиты имущества;

c) иллюстрирует типичные методы оценки опасностей и рисков, которые могут быть выполнены для определения требований к функциональной безопасности, а также УПБ каждой из функций безопасности ПСБ;

d) иллюстрирует методы и/или средства, позволяющие определить требуемые УПБ;

e) содержит структуру работ по установлению УПБ, но не определяет УПБ для конкретных случаев применения;

f) не содержит примеров определения требований к иным методам снижения рисков.

Приложения В—К упрощенно иллюстрируют количественные и качественные подходы. Эти приложения были включены лишь для иллюстрации общих принципов, положенных в основу ряда используемых методов, и не могут служить руководством к их практическому применению.

Примечания

1 Тем, кто намеревается практически использовать методы, описанные в упомянутых приложениях, следует обратиться к ссылкам, имеющимся в каждом приложении.

2 Методы определения УПБ, включенные в настоящий стандарт, могут не подойти для всех применений. В частности, для режима с высокой частотой запросов или непрерывного режима работы могут потребоваться конкретные методы или дополнительные факторы, которые в настоящем стандарте не описаны.

Издание официальное

3 Представленные в настоящем стандарте методы могут привести к неконсервативным результатам, если они используются за пределами их областей применения и если должным образом не рассматривают такие факторы, как общая причина, отказоустойчивость, общесистемные свойства приложения, отсутствие опыта использования методов, независимость слоев защиты и т. д. См. приложение J.

На рисунке 2 показана совокупность типовых слоев защиты и методов снижения риска.

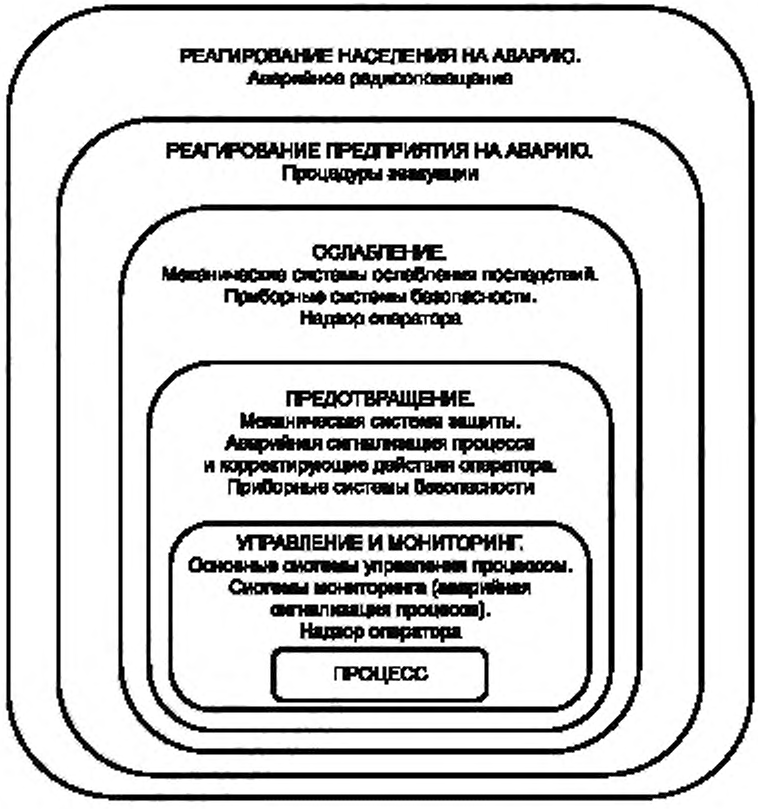


Рисунок 2 — Типовые слои защиты и средства снижения риска

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий международный стандарт (для датированной ссылки применяют только указанное издание ссылочного стандарта):

IEC 61511-1:2016, Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and application programming requirements («Безопасность функциональная. Приборные системы безопасности, для технологических процессов в промышленности. Часть 1. Термины, определения и технические требования»)

3 Термины, определения и сокращения

В настоящем стандарте применены термины, определения и сокращения, приведенные по МЭК 61511-1 (раздел 3).

Приложения настоящего стандарта являются справочными и не обязательными. Кроме того, применение любого конкретного метода, описанного в приложениях настоящего стандарта, не гарантирует соответствия требованиям МЭК 61511-1:2016.

Приложение А
(справочное)

Риск и полнота безопасности. Общие требования

А.1 Общие сведения

В данном разделе приведена информация об основополагающих концепциях риска и связи рисков с полнотой безопасности. Эта информация является общей для всех рассматриваемых ниже методов оценки различных опасностей и рисков.

А.2 Необходимая степень снижения риска

Необходимая степень снижения риска, которая может быть установлена либо качественно (см. примечание 1), либо количественно (см. примечание 2), — это такое снижение риска, которое должно быть обеспечено для достижения уровня риска (например, целевого уровня безопасности процесса), приемлемого в конкретной ситуации. Концепция необходимого снижения риска является фундаментально важной для формулирования спецификации требований безопасности для функций безопасности ПСБ (в частности, требований к полноте безопасности). Цель определения приемлемого риска (например, целевого уровня безопасности процесса) в случае конкретного опасного события состоит в установлении величины «разумного» риска, учитывающего как частоту возникновения опасных событий, так и их специфические последствия. Слои защиты (см. рисунок А.2) разрабатываются так, чтобы уменьшить частоту возникновения опасных ситуаций и/или их последствия.

Важными факторами для оценки величины приемлемого риска являются восприятие и точки зрения тех лиц, которые подвергаются опасности. При определении приемлемого риска для конкретного применения необходимо учитывать:

- указания соответствующих регулирующих органов;
- обсуждения и соглашения между различными сторонами, принимающими участие в данном применении;
- промышленные стандарты и руководства;
- промышленные, экспертные и научные советы;
- законодательные и регулирующие требования, как общие, так и относящиеся к конкретному применению.

Примечания

1 При определении необходимой степени снижения риска следует предварительно установить приемлемый риск. В МЭК 61508–5:2010, приложения D и E, рассмотрены качественные и полуколичественные методы, хотя в рассмотренных там примерах необходимое снижение риска представлено, скорее, в неявном виде и не установлено точно.

2 Например, опасное событие, приводящее к определенным последствиям, как правило, характеризуется максимальной частотой повторений в год.

А.3 Роль приборных систем безопасности

ПСБ реализует функции безопасности, необходимые для достижения или для поддержания безопасного состояния процесса, и, следовательно, вносит вклад в решение задачи необходимого снижения риска для достижения приемлемого риска. Например, в спецификации требований к функциям безопасности может быть указано, что если температура достигает значение *x*, то клапан *y* открывается, обеспечивая поступление воды в емкость.

Необходимое снижение риска может достигаться с помощью одной или комбинации нескольких ПСБ либо с помощью других слоев защиты.

В выполнении функции безопасности может участвовать человек. Например, оператор может получать информацию о состоянии процесса и выполнять основанные на этой информации некоторые действия в системе безопасности. Если человек является частью функции безопасности, то должны быть учтены все человеческие факторы.

ПСБ может действовать по запросу или в непрерывном режиме.

Считается, что полнота безопасности состоит из двух частей:

a) **полнота безопасности аппаратных средств** — это часть полноты безопасности, связанная со случайными отказами аппаратных средств, причем относящимися к опасным отказам. Факт достижения установленного уровня полноты безопасности аппаратных средств можно оценить с разумным уровнем точности. Поэтому требования могут быть распределены между подсистемами, используя известные правила комбинации вероятностей с учетом отказов по общей причине. Для достижения требуемой полноты безопасности аппаратных средств может оказаться необходимым применение структур с резервированием;

b) **систематическая полнота безопасности** — эта часть полноты безопасности связана с систематическими отказами, относящимися к опасным отказам. 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 отказов ПСБ). Следовательно, необходимо обосновать, какие способы минимизации этой неопределенности окажутся наиболее эффективными. Нужно

отметить, 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 систематических отказов.

Общее снижение риска, достигаемое функциями безопасности ПСБ вместе со средствами других слоев защиты, должно быть таким, чтобы обеспечить:

- частоту отказов функций безопасности, достаточно низкую для того, чтобы частота опасных событий не превышала бы значения, соответствующего приемлемому риску, и/или
- возможность того, что функции безопасности так изменяют последствия отказов, чтобы риск не превышал значение приемлемого риска.

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

- имеется процесс и связанная с ним основная система управления процессом (ОСУП);
- существует связанный с процессом человеческий фактор;
- слои защиты безопасности включают в свой состав:
  - механическую систему защиты,
  - приборные системы безопасности,
  - неприборные системы,
  - механическую систему ослабления последствий.

Примечание — На рисунке А.1 представлена обобщенная модель риска, иллюстрирующая общие принципы. Модель риска для конкретного случая должна составляться с учетом конкретных приемов, с помощью которых на базе ПСБ и других слоев защиты фактически достигается необходимое снижение риска. Результирующая модель риска в конкретном случае может отличаться от представленной на рисунке А.1.

На рисунках А.1 и А.2 показаны следующие риски:

- риск процесса. Это риск наличия конкретных опасных событий для процесса. При этом учитывается наличие основной системы управления процессом и человеческого фактора. При определении этого риска не рассматриваются какие бы то ни было специальные средства защиты безопасности;
- приемлемый риск (заданный уровень безопасности процесса). Риск, который считается приемлемым в данном контексте на основе принятой в обществе системы ценностей;
- остаточный риск. В контексте настоящего стандарта это риск возникновения опасных событий при условии применения всей совокупности слоев защиты.

Риск процесса является функцией от риска, связанного с самим процессом, но учитывающего также снижение риска, достигнутое благодаря применению системы управления процессом. Для того чтобы избежать неразумных требований к полноте безопасности ОСУП, настоящий стандарт устанавливает ограничения на возможные требования.

Необходимое снижение риска — это уменьшение уровня риска до такого минимального значения, который необходим для обеспечения приемлемого риска. Оно может достигаться с помощью как одного способа, так и комбинацией способов снижения риска. Процесс необходимого снижения риска, обеспечивающий достижение конкретного приемлемого риска от начального значения риска процесса, показан на рисунке А.1.

Примечание — В некоторых применениях для достижения целевого риска параметры риска (например, частота и вероятность отказа по запросу) не могут быть просто объединены, как представлено в рисунке А.1, без учета факторов, отмеченных в приложении J. Это может произойти из-за влияния отказов по общей причине и общих зависимостей между различными слоями защиты.

А.4 Риск и полнота безопасности

Очень важно полностью осознать разницу между риском и полнотой безопасности. Риск — это мера частоты появления и последствий конкретного опасного события. Его можно оценить для различных ситуаций (риск процесса, приемлемый риск, остаточный риск и т. д., см. рисунок А.1). При определении приемлемого риска учитывают социальные и политические факторы. Полнота безопасности — это мера вероятности того, что функция безопасности ПСБ и другие слои защиты обеспечат установленную безопасность. Только после того как приемлемый риск установлен и получена оценка величины необходимого снижения риска, можно определить требования к полноте безопасности ПСБ.

Примечание — Такая процедура может носить итеративный характер, что позволит осуществить оптимизацию разработки в целях выполнения различных требований. Роль, которую играют функции безопасности при достижении необходимого снижения риска, показаны на рисунках А.1 и А.2.

А.5 Распределение требований к безопасности

На рисунке А.4 показано распределение требований к безопасности (требований как к функциям безопасности, так и к полноте безопасности) по различным ПСБ и другим слоям защиты. Требования к процессу распределения даны в МЭК 61511-1, раздел 9.

Применение тех или иных методов для распределения требований полноты безопасности по ПСБ, другим связанным с безопасностью технологическим системам, а также по внешним средствам снижения риска зависит прежде всего от того, каким образом определена степень необходимого снижения риска — количественно или качественно. Эти подходы называют полуколичественными, полукачественными и качественными соответственно (см. приложения B—F).

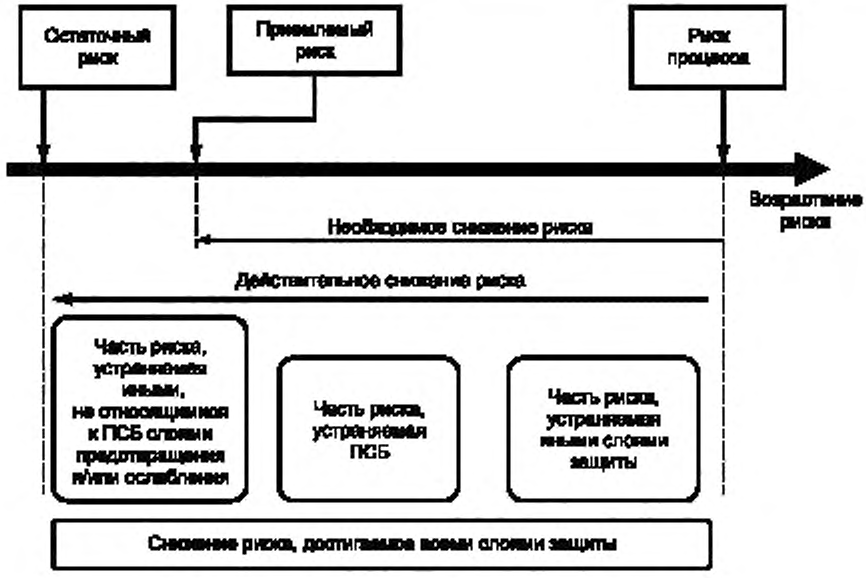


Рисунок А.1 — Общая концепция снижения риска



Рисунок А.2 — Концепции риска и полноты безопасности

А.6 Опасное событие, опасная ситуация и вредоносное событие

Термины «опасное событие» и «опасная ситуация» часто используются в последующих приложениях. На рисунке А.3 продемонстрировано различие между терминами и показано развитие от опасного события до опасной ситуации из-за потери управления, приводящее к возникновению вредоносного события.

Рисунок А.3 демонстрирует, как вред наносится людям, но его также можно применить и к нанесению вреда окружающей среде или ущерба имуществу.

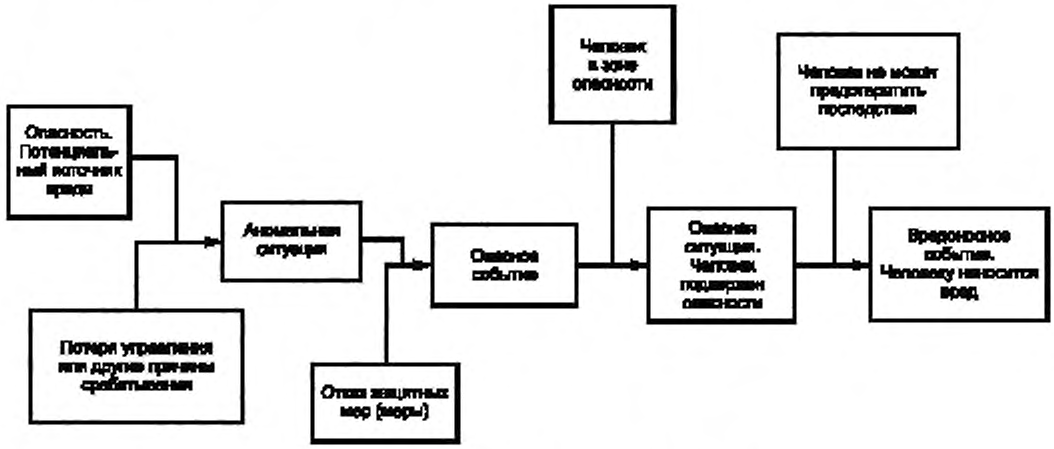


Рисунок А.3 — Развитие вредоносного события

Рисунок А.3 показывает, как потеря управления или инициирование любой другой причины приводит к аварийной ситуации и формирует запрос к мерам защиты, таким как предупредительные тревожные сигнализации, ПСБ, предохранительная арматура и т. д. Опасное событие возникает, если выполняется запрос, а соответствующие меры защиты находятся в состоянии отказа и не функционируют, как положено. Опасное событие само по себе не обязательно наносит ущерб, но если человек (люди) находился в зоне (или области) его воздействия, и таким образом подвергался воздействию опасного события, то это приводит к опасной ситуации. Если человек не способен избежать пагубных последствий воздействия, то оно характеризуется как вредоносное воздействие из-за нанесения вреда здоровью.

А.7 Уровни полноты безопасности

В настоящем стандарте определены четыре уровня полноты безопасности, причем уровень полноты безопасности 4 — наивысший, уровень полноты безопасности 1 — низший.

Целевые меры отказов для задания всех четырех уровней полноты безопасности определены в МЭК 61511-1, таблицы 3 и 4. Установлены два таких параметра: один для ПСБ, действующих в режиме низкой интенсивности запросов, и другой для ПСБ, работающих в режиме с непрерывным запросом или в режиме высокой интенсивности запросов.

Примечание — В случае ПСБ, работающей в режиме низкой интенсивности запросов, целевой мерой отказов является средняя вероятность опасного отказа функции безопасности по запросу. В случае если ПСБ работает в режиме с непрерывным запросом или в режиме высокой интенсивности запросов, то целевой мерой отказов является средняя частота опасных отказов функции безопасности (см. МЭК 61511-1, 3.2.83 и таблицу 5).

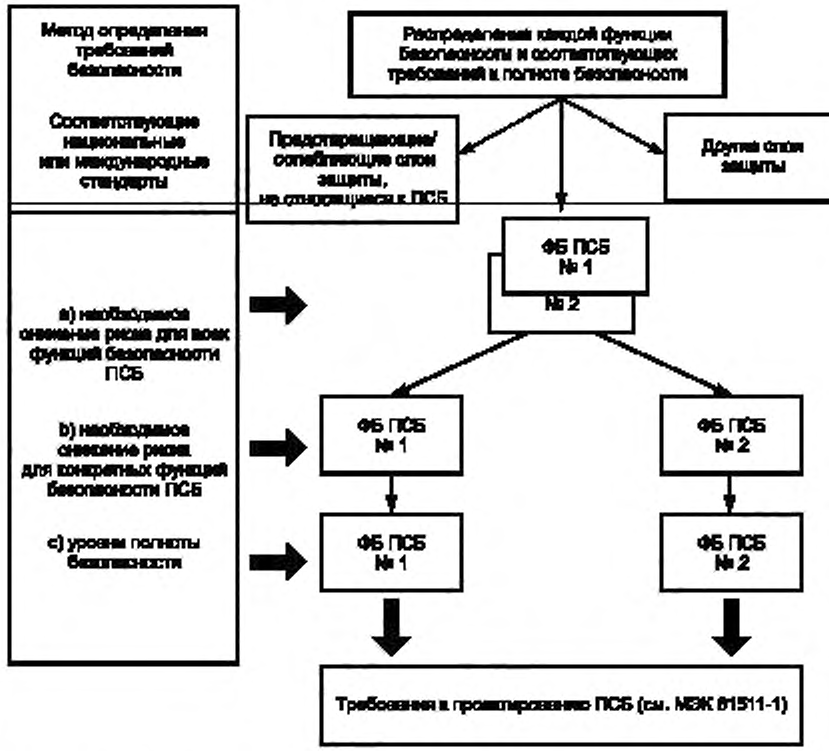
А.8 Выбор метода для определения требуемого уровня полноты безопасности

Имеются различные пути установления требуемого УПБ для конкретного случая. В приложениях В—I представлена информация о ряде используемых методов. Выбор метода для конкретного применения зависит от многих факторов, в том числе:

- от сложности задачи;
- указаний регулирующих органов;
- природы риска и требуемой величины его снижения;
- опыта и квалификации персонала, выполняющего эту работу;
- доступной информации о параметрах риска (см. рисунок А.4);
- доступной информации о ПСБ, использующейся в настоящее время в конкретных применениях, описанных в отраслевых стандартах и промышленной практике.

В некоторых случаях можно использовать не один, а несколько методов. Так, при определении требуемого УПБ для всех рассматриваемых функций безопасности ПСБ в качестве первого шага можно использовать качественные методы. Те функции, которым с помощью этого метода был присвоен уровень 3 или 4, следует затем проанализировать более детально с использованием количественных методов для получения более точной оценки требуемой их полноты безопасности.

Важно то, что какой бы ни был выбран метод (методы) для конкретного применения, для его оценки должны использоваться определенные критерии риска.



Примечание — Требования к полноте безопасности устанавливаются для каждой функции безопасности ПСБ до распределения [см. МЭК 61511-1 (раздел 9)].

Рисунок А.4 — Распределение требований безопасности по слоям защиты, не относящимся к ПСБ, и другим слоям защиты

Приложение В
(справочное)

Полуколичественный метод. Анализ дерева событий

В.1 Общие сведения

В данном приложении рассмотрен вопрос о том, как с помощью полуколичественного подхода можно определять целевые уровни полноты безопасности. Полуколичественный подход использует как качественные, так и количественные методы и наиболее целесообразен в случаях, когда приемлемый риск определяется численно (например, определенные последствия не должны возникать чаще чем один раз в сто лет).

Данное приложение не предназначено для использования в качестве руководства по применению конкретного метода, а имеет своей целью проиллюстрировать его общие принципы. Приложение основано на методе, детально описанном в CCPS/AIChE, Guidelines for Hazard Evaluation Procedures, Third Edition, Wiley-Interscience, New York (2008).

В.2 Соответствие МЭК 61511-1

Основная цель данного приложения — проследить процедуру выбора необходимых функций безопасности ПСБ и установления их УПБ. Для решения этой задачи необходимо выполнить следующие основные шаги:

a) установить целевую (заданную) безопасность процесса (приемлемый риск);

b) провести анализ опасности и риска, чтобы оценить существующий риск для каждого конкретного опасного события;

c) определить функцию (функции) безопасности, требуемую для каждого конкретного опасного события;

d) распределить функции безопасности по слоям защиты.

Примечание — Предполагается, что слои защиты не зависят один от другого. Процесс распределения может гарантировать, что вероятность отказов по общей причине, отказов общего вида и систематических отказов достаточно мала по сравнению с общими требованиями снижения риска;

e) определить, требуются ли функции безопасности ПСБ;

f) определить УПБ функций безопасности ПСБ.

Шаг a) определяет целевую безопасность процесса. На шаге b) выполняется анализ риска процесса, а шаг c) позволяет на основании анализа риска определить, какие требуются функции безопасности и каким должно быть снижение риска, чтобы была достигнута целевая безопасность. После распределения на шаге d) этих функций безопасности по слоям защиты становится ясным, требуется ли функция (функции) безопасности ПСБ [шаг e)] и каким должен быть ее (их) УПБ [шаг f)].

В данном приложении при оценивании риска для достижения целей стандартов МЭК 61511 предлагается использовать полуколичественные методы. Этот подход продемонстрирован на простом примере.

В.3 Пример

В.3.1 Общее описание

Рассмотрим процесс, включающий емкость под давлением с насосом и двумя выходами (жидкости и газа), содержащую смесь газа и летучей воспламеняющейся жидкости, а также необходимое оборудование (см. рисунок В.1). Управление процессом осуществляется основной системой управления процессом (ОСУП), которая контролирует сигнал датчика расхода и управляет перемещением клапана. Имеются следующие технические системы, реализующие процесс: a) независимый датчик давления, который в случае недопустимого повышения давления выдает предупредительный сигнал, побуждающий оператора к принятию соответствующих мер по прекращению подачи жидкости в емкость, и б) если реакции оператора на аварийный сигнал не последует, то включается дополнительный, неприборный слой защиты, который является регулятором давления, чтобы предотвратить опасности, связанные с высоким давлением в емкости. Сбросы из регулятора давления отводятся по трубам в сепараторную емкость, которая соединена с системой сброса газа. В этом примере принимается, что система сброса газа спроектирована, смонтирована и действует нормально и имеет разрешение на применение. Таким образом, потенциально возможные отказы системы сброса газа в этом примере не рассматриваются.

Примечание — Понятие «технические системы» относится здесь ко всем системам, работающим с процессом. Они включают и иные автоматические средства защиты, а также оператора (операторов).

В.3.2 Целевой уровень безопасности процесса

Фундаментальным условием успешного управления промышленным риском является четкое и ясное определение целевого уровня безопасности процесса (приемлемого риска). Он может быть установлен на базе национальных и международных стандартов и правил, корпоративной политики, а также под влиянием заинтересованных сторон, таких как сообщества и/или местные органы и страховые компании с хорошей технической подготовкой.

Целевой уровень безопасности процесса специфичен для конкретного процесса, корпорации или отрасли. Таким образом, обобщения невозможны, за исключением ситуаций, когда существующие правила и стандарты обеспечивают поддержку таким обобщениям. В качестве примера примем, что для целевого уровня безопасности процесса установлено, что средняя частота сброса не должна превышать 10^{-4} в год, что объясняется ожидаемыми последствиями сброса для окружающей среды.

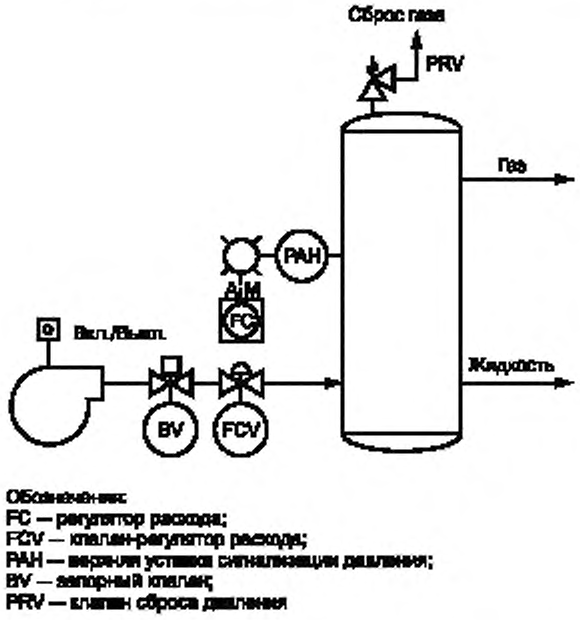


Рисунок В.1 — Емкость под давлением с существующими системами безопасности

В.3.3 Анализ опасности

Для того чтобы выявить опасности, возможные отклонения процесса и их причины, исходные события и потенциально опасные события (инциденты) в используемых технических системах, следует провести анализ опасностей процесса. Для этого могут быть использованы следующие методы качественного анализа:

- анализ безопасности;
- контрольные листы;
- анализ гипотез («что произойдет, если»);
- метод HAZOP;
- анализ видов и последствий отказов;
- анализ причин и последствий.

Одним из таких методов, получивших широкое применение, является метод анализа опасности и работоспособности (Hazard and Operability, HAZOP). Анализ (или изучение) опасности и работоспособности выявляет и оценивает опасности для технологической установки, а также другие неопасные проблемы, связанные с работоспособностью, которые могут повлиять на возможность достижения проектной производительности установки.

На втором шаге для примера, приведенного на рисунке В.1, проводится анализ HAZOP. Целью применения этого метода анализа является оценка потенциально опасных событий, связанных с выбросами в окружающую среду. Краткий перечень результатов применения метода приведен в таблице В.1.

В результате применения HAZOP установлено, что значительное превышение давления может привести к выбросам горючего материала в окружающую среду. Это является исходным событием, которое может перерасти в опасное событие по сценарию, зависящему от реакции имеющихся технических систем. Если бы метод HAZOP был применен к анализу объекта в полной мере, то в рассмотрении могли бы появиться иные исходные события, приводящие к выбросам, включая утечку из технологического оборудования, полный разрыв трубопровода и такие внешние события, как пожар. В данном иллюстративном примере рассмотрены только условия возникновения высокого давления.

Примечание — В данном примере предполагается, что емкость может оказаться под высоким давлением из-за неспособности оборудования, расположенного ниже по технологической цепочке, обслуживать полный поток газа из емкости, когда поток подачи слишком высок.

Таблица В.1 — Результаты анализа методом HAZOP

Объект	Отклонение	Причина	Последствие	Мера защиты	Действие
Емкость	Интенсивный поток	Отказ контура управления потоком	Интенсивный поток приводит к высокому давлению (см. примечание)		
	Высокое давление	1 Отказ контура управления потоком. 2 Внешнее возгорание	Повреждение емкости и выброс в окружающую среду	1) Аварийный сигнал высокого давления. 2) Система пожаротушения (потоком воды). 3) Клапан сброса давления	Оценка проектных условий сброса давления в окружающую среду
	Малый поток / отсутствие потока	Отказ контура управления потоком	Нет последствий, представляющих интерес		
	Обратный поток		Нет последствий, представляющих интерес		

В.3.4 Полуколичественный метод анализа риска

Оценку рисков процесса выполняют с помощью полуколичественного метода анализа, который позволяет определить и количественно оценить риски, связанные с возможными ошибками или опасными событиями в технологическом процессе. Результаты анализа могут быть использованы для выбора необходимых функций безопасности и их УПБ, дающих возможность снизить риск процесса до приемлемого уровня. Оценка риска процесса с помощью полуколичественного метода может быть выполнена в виде приведенной ниже последовательности шагов, причем первые четыре шага могут быть реализованы в процессе применения метода HAZOP:

a) определить опасности для процесса;

b) определить исходные события;

c) построить сценарии опасного развития событий применительно к каждому исходному событию;

d) определить состав слоев защиты.

Примечания

1 Чтобы обеспечить процесс защитой, функции безопасности распределены по слоям защиты, которые включают ПСБ и другие средства снижения риска (см. рисунок В.2).

2 Шаг d) применяется к рассматриваемому примеру, так как он связывает существующий процесс с существующими слоями защиты;

e) с помощью архивных данных или используя методы моделирования (анализ дерева событий, анализ видов и последствий отказов, анализ дерева ошибок) уточнить частоту появления исходных событий и надежность существующих систем безопасности;

f) оценить количественно частоту возникновения всех существенно опасных событий;

g) оценить последствия всех существенно опасных событий;

h) просуммировать результаты (последствия и частоту инцидентов) оценки риска, связанного с каждым опасным событием.

Существенные результаты такого анализа, представляющие интерес:

- лучшее и более детальное понимание опасностей и рисков, связанных с процессом;
- знание риска процесса;
- понимание вклада существующей функции безопасности в общее снижение риска;
- определение каждой функции безопасности, требующейся для снижения риска процесса до приемлемого уровня;
- сравнение полученной оценки риска процесса с целевым значением.

Метод полуколичественного анализа требует значительных ресурсов, но имеет достоинства, которые не обеспечивают качественные подходы. При определении опасностей этот метод базируется в большой степени на экспертных оценках команды специалистов, обеспечивает ясный способ управления существующими системами безопасности, основанными на других технологиях, использует средства документирования всех мероприятий, которые привели к полученным результатам, и обеспечивает поддержку жизненного цикла.

Для представленного примера с помощью HAZOP-анализа было идентифицировано одно исходное событие (возникновение избыточного давления), которое повлекло возникновение возможности выброса вещества в окружающую среду. Необходимо отметить, что используемый в данном пункте подход является комбинацией количественной оценки частоты возникновения опасного события и качественной оценки его последствий. Данный подход применяют для иллюстрации систематической процедуры, которой рекомендуется следовать для определения опасных событий и функций безопасности ПСБ.

B.3.5 Анализ рисков существующих процессов

Следующий шаг состоит в установлении факторов, которые могут способствовать возникновению исходного события. На рисунке В.2 показано простое дерево ошибок, на котором представлен ряд причин возникновения чрезвычайно высокого давления в емкости. Событие верхнего уровня — чрезмерное повышение давления в емкости — может быть вызвано отказом основной системы управления процессом (например, контура управления потоком) или внешним фактором — пожаром (см. таблицу В.1).

Дерево ошибок наглядно представляет воздействие отказа ОСУП на процесс, а частоту наружного пожара полагают незначительной. Сама ОСУП не выполняет каких-либо функций защиты. Ее отказ, однако, приводит к росту числа запросов к ПСБ. Таким образом, при наличии надежной ОСУП запросов к ПСБ будет меньше.

Дереву ошибок можно поставить в соответствие количественные оценки. В настоящем примере предполагается, что частота появления условий чрезвычайно высокого давления будет порядка 10^{-1} в год. Необходимо учесть, что каждая причина, показанная на рисунке В.2, предполагается независимой (т. е. отсутствуют взаимовлияния) от других причин, с интенсивностью отказов, выраженной как события в год.

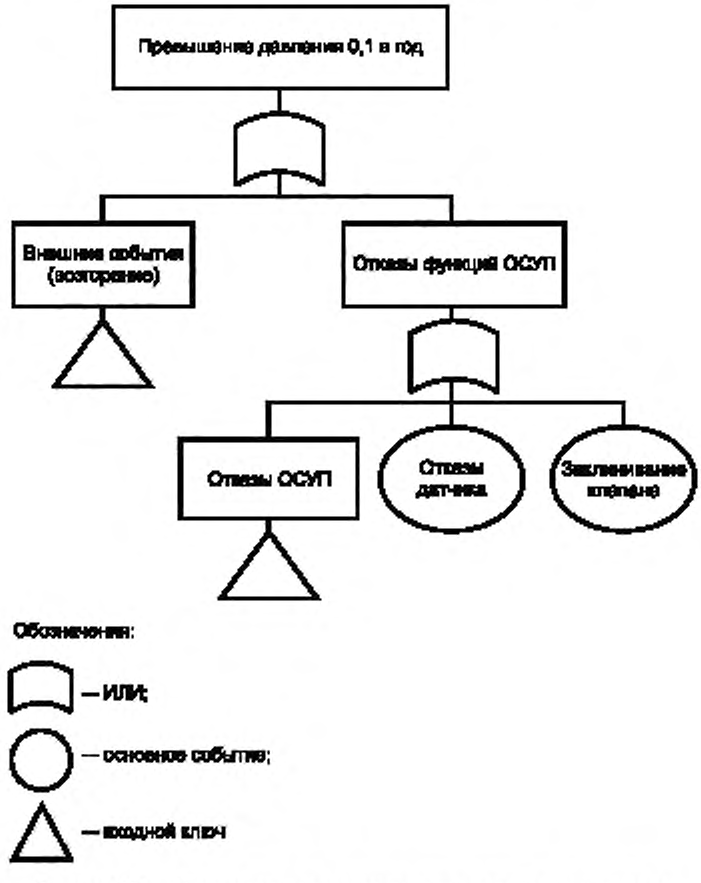


Рисунок В.2 — Дерево ошибок при превышении давления в емкости

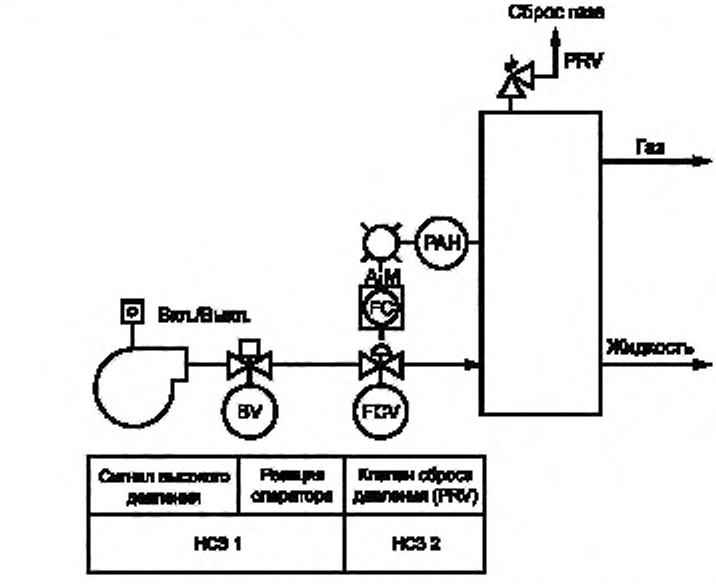
Примечание — На рисунке В.2 представлено дерево ошибок без учета мер защиты.

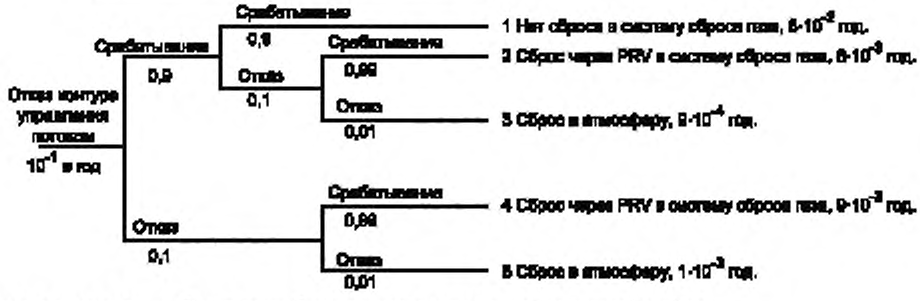
После установления частоты появления исходного события, используя средства анализа дерева событий, проводят моделирование реакции систем безопасности (успешная работа или отказ) на аномальные условия. Данные по надежности систем безопасности могут быть взяты из эксплуатационных данных, опубликованных баз данных или получены по результатам прогноза, полученным методом моделирования надежности.

Для рассматриваемого примера использованы реальные данные по надежности, а не данные, взятые из литературы или полученные в результате прогнозирования работы системы. На рисунке В.3 показаны возможные сценарии потенциального выброса, которые могут произойти в условиях повышения давления. В результате моделирования таких случаев были получены: a) частота возникновения каждой из приводящих к аварии последовательностей событий и b) качественная оценка последствий в виде выброса воспламеняющихся материалов.

На рисунке В.3 показаны пять вариантов развития опасных событий, причем для каждого приведены частота появления и последствия возможного выброса. Реализация сценария 1 включает реакцию оператора на аварийную сигнализацию о высоком давлении, что происходит с частотой $8 \cdot 10^{-2}$ в год, и эти действия оператора приводят к уменьшению выпуска продукции без выброса. Такая авария соответствует исходным условиям, принятым при проектировании процесса, а оператор обучен и протестирован для выполнения соответствующих действий, обеспечивающих достижение снижения риска.

Более того, условиям проектирования соответствуют также сценарии 2 и 4, при которых происходит выброс воспламеняющихся материалов с общей частотой $1{,}9 \cdot 10^{-2}$ в год ($9 \cdot 10^{-3} + 1 \cdot 10^{-2}$). Общая частота возникновения аварий для сценариев 3 и 5, для которых характерны повреждение емкости и выброс материала в окружающую среду, равна $1{,}9 \cdot 10^{-4}$ в год ($9 \cdot 10^{-5} + 1 \cdot 10^{-4}$).





Примечание — Результаты были округлены до первой значащей цифры.

Рисунок В.3 — Опасные события при существующих системах безопасности

Примечание — В некоторых применениях частота и вероятность отказов по запросу не могут быть получены умножением, как показано в рисунке В.3. Это может произойти из-за влияния отказов по общей причине и общих зависимостей между различными слоями защиты (см. Приложение J).

Следует отметить, что при анализе не принималась во внимание возможность отказа по общей причине сигнализатора высокого давления и отказа датчика уровня в составе ОСУП. Такого рода отказы по общей причине могут привести к существенному увеличению частоты аварий по сценарию 3 и, следовательно, к увеличению риска.

Примечание — Предполагается, что события, изображенные на рисунке В.3, независимы. Более того, указанные данные являются приближенными, поэтому сумма частот всех возникающих аварий приближается к частоте исходного события (0,1 в год).

В.3.6 События, не отвечающие целевому уровню безопасности процесса

Как отмечалось ранее, в соответствии с конкретными руководящими указаниями для технологического объекта устанавливается целевой уровень безопасности процесса: выброс материала в окружающую среду должен происходить с частотой, не превышающей 10^{-4} раз в год. Общая частота выбросов в окружающую среду составляет $1{,}9 \cdot 10^{-5}$ (сценарий 3) + $1{,}9 \cdot 10^{-4}$ (сценарий 5) = $1{,}92 \cdot 10^{-4}$ в год, что больше, чем целевой уровень безопасности процесса. Учитывая данные о частоте возникновения опасных событий и данные о последствиях, представленные на рисунке В.3, для сценариев выброса 2, 3 и 5 необходимо дополнительное снижение риска, чтобы частота выбросов была ниже целевого уровня безопасности процесса.

В.3.7 Снижение риска путем использования других слоев защиты

Прежде чем установить необходимость функции безопасности ПСБ, следует рассмотреть слои защиты, использующие другие технологии. Система пожаротушения (потоком воды) перечислена в качестве меры защиты в таблице В.1, но она не предотвращает повреждение сосуда или выброс в окружающую среду.

Учитывая, что цель анализа состоит в том, чтобы минимизировать риск, связанный с выбросами материала в окружающую среду, можно заключить, что система пожаротушения (потоком воды) не является приемлемой схемой снижения риска повреждения сосуда или выброса в окружающую среду. Система пожаротушения (потоком воды) действительно снижает риск для персонала и эскалации событий, что в данном примере не оценивается.

В.3.8 Снижение риска путем использования функции безопасности ПСБ

Целевой уровень безопасности процесса не может быть достигнут применением слоев защиты, использующих другие технологии. Для уменьшения общей частоты выбросов в атмосферу требуется новая ПСБ, реализующая функцию безопасности с УПБ 2, чтобы обеспечить достижение целевого уровня безопасности процесса. Такая новая ПСБ показана в рисунке В.4.

Нет необходимости в данном пункте выполнять детальный проект функции безопасности ПСБ. Вполне достаточна общая концепция ее проекта. Цель на данном шаге состоит в том, чтобы определить, обеспечит ли новая ПСБ, реализующая функцию безопасности с УПБ 2, необходимое снижение риска и достижение целевого уровня безопасности процесса. Детальное проектирование функции безопасности ПСБ необходимо выполнять только после того, как для нее будет определен целевой уровень безопасности процесса. Для данного примера новая функция безопасности ПСБ использует сдвоенный специально предназначенный для безопасности датчик давления (на рисунке В.4 не показан), включенный по схеме 1oo2 и связанный с логическим решающим устройством, которое также управляет дополнительным отсечным клапаном и насосом.

Примечание — Обозначение 1oo2 означает «один из двух», т. е. любой из сдвоенных датчиков может послать сигнал, останавливающий процесс.

Новая функция безопасности ПСБ с УПБ 2 предназначена для уменьшения частоты выбросов из сосуда, находящегося под высоким давлением. На рисунке В.4 изображен новый слой защиты и представлены все потенциально опасные сценарии. Как можно видеть на этом рисунке, частота выбросов из такой емкости может быть снижена до значения 10^{-4} в год и ниже, и целевой уровень безопасности процесса может быть достигнут при условии, что полученная в результате функция безопасности ПСБ отвечает требованиям УПБ 2.

На рисунке В.4 определены семь возможных сценариев, для каждого из которых даны частота возникновения и качественное описание последствия. Частота сценария 1 совпадает с ранее рассмотренной. Реакция оператора происходит с частотой $8 \cdot 10^{-2}$ в год и приводит к уменьшению выпуска продукции.

В этом проекте успешная работа ПСБ приводит к остановке процесса с частотой $1{,}9 \cdot 10^{-2}$ в год. ПСБ уменьшает интенсивность запроса процесса к клапану сброса давления (PRV). Частота реализации сценария 3, включающая сброс из PRV в систему сброса газа, снижена на два порядка величины по сравнению с предыдущим случаем до $9 \cdot 10^{-5}$ в год. В сценарии 4 опасное событие с выбросом материала в окружающую среду происходит с частотой $9 \cdot 10^{-7}$ в год.

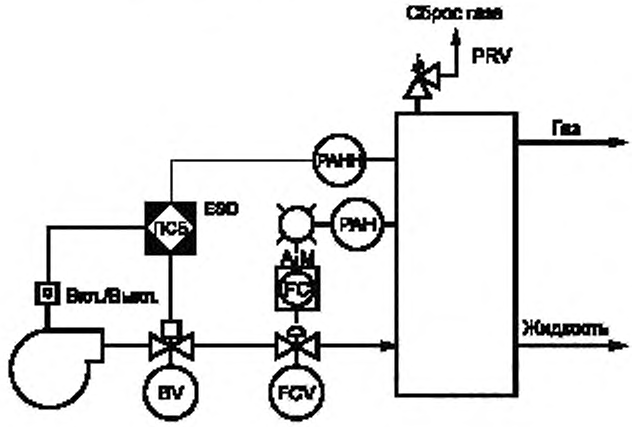
В сценарии 5 сброс в систему сброса не происходит в результате остановки процесса с помощью ПСБ с частотой $1 \cdot 10^{-2}$ в год. Если ПСБ не действует, то PRV обеспечивает следующую функцию безопасности, как показано в сценарии 6, и открывает систему сброса. Открытие PRV происходит с частотой $1 \cdot 10^{-4}$ в год. Общая частота сброса в систему сброса, определяется сценариями 3 и 6, которая вычисляется как сумма их полных

частот $9 \cdot 10^{-5} + 1 \cdot 10^{-4} = 1{,}9 \cdot 10^{-4}$. Сбросы из системы сброса являются приемлемым условием при проектировании процесса. Сценарий 7 связан с отказом всех функций безопасности и реализуется с частотой $1 \cdot 10^{-6}$ в год.

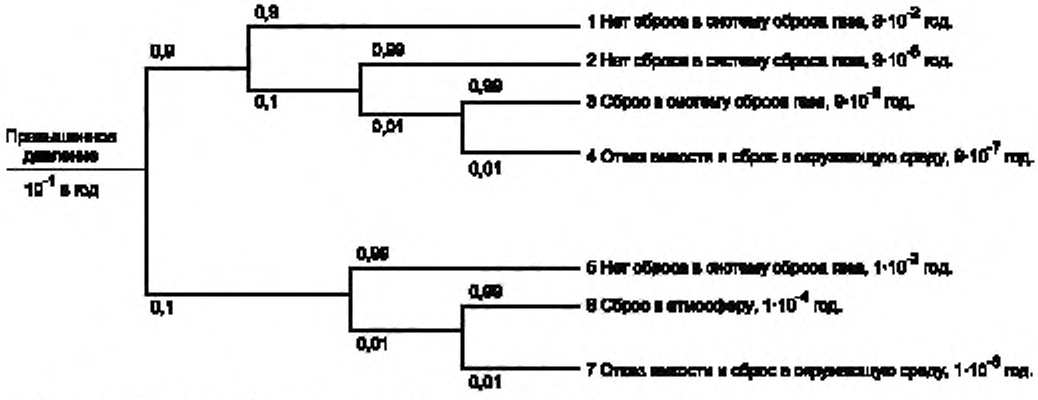
Общая частота выбросов в окружающую среду (сумма частот сценариев 4 и 7) снижена до $1{,}9 \cdot 10^{-5}$ в год, ниже целевого уровня безопасности процесса, равного 10^{-4} в год.

Следует отметить, что анализ с использованием дерева событий не учитывает возможность отказа по общей причине и общие зависимости между системой аварийной сигнализации высокого давления и функцией безопасности ПСБ с УПБ 2. Возможны также отказ по общей причине и общие зависимости между функциями безопасности и датчиком уровня в составе ОСУП.

Такие отказы по общей причине приводят к существенному увеличению вероятности отказа функций защиты при наличии запроса и, следовательно, к значительному увеличению общего риска.



Сигнал высокого давления	Реакция оператора	ПСБ УПБ 2	Клапан сброса давления (PRV)
HCS 1		HCS 2	HCS 3



Примечание — Результаты были округлены до первой значащей цифры.

Рисунок В.4 — Опасные события для функции безопасности ПСБ с УПБ 2

Приложение С
(справочное)

Метод матрицы слоев безопасности

С.1 Введение

Для каждого технологического процесса снижение риска должно начинаться уже на стадии проектирования процесса при выборе наиболее важных решений: при выборе собственно процесса и его местоположения, при принятии решения о запасах опасных реагентов и их размещении. Минимизация запасов опасных химических компонентов, применение таких трубопроводных и теплообменных систем, которые физически исключают нежелательное смешивание активных химических веществ, выбор толстостенных сосудов, способных противостоять максимально возможным давлениям в процессе, выбор теплоносителя, максимальная температура которого ниже температуры разложения реагентов, — все эти проектные решения по процессу снижают эксплуатационные риски. Такое внимание к снижению риска путем тщательного выбора конструктивных и технологических параметров процесса — это ключ к созданию безопасного процесса. Рекомендуется и в дальнейшем продолжать поиски путей снижения опасности и применения заведомо безопасных проектных решений. К сожалению, даже используя в максимальной степени эту философию проектирования, не удается полностью исключить потенциальную опасность и приходится применять дополнительные защитные меры.

В промышленных технологических процессах для их защиты применяют многочисленные слои защиты, как это показано на рисунке С.1. Каждый слой защиты, показанный на этом рисунке, состоит из специального оборудования и/или элементов административного управления, которые, действуя совместно с другими слоями защиты, уменьшают риск процесса и/или управляют им.

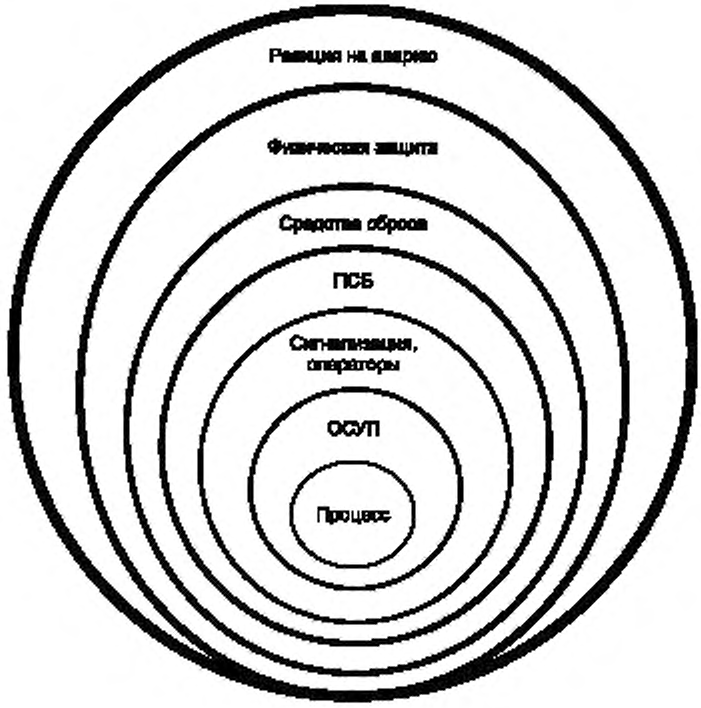


Рисунок С.1 — Слои защиты

Концепция слоев защиты (СЗ) базируется на трех основных принципах:

a) слой защиты представляет собой совокупность технических средств и/или организационных мер, которые функционируют в согласии с другими слоями защиты, обеспечивая снижение риска процесса или управление им;

b) слой защиты должен удовлетворять следующим критериям:

- снижать определенный риск по меньшей мере в 10 раз,

- обладать такими важными характеристиками, как:
  - специфичность. СЗ проектируется для того, чтобы предотвратить или ослабить последствия одного потенциально опасного события. Причин возникновения этого опасного события может быть много, и, следовательно, действие СЗ может быть вызвано многими исходными событиями,
  - независимость. СЗ считается независимым от других слоев защиты, если можно показать, что потенциально возможные совместные отказы по общей причине или общего типа отсутствуют;
  - надежность. Можно рассчитывать, что СЗ будет выполнять предназначенные для него функции, если при его проектировании учитываются как случайные, так и систематические отказы;
  - проверяемость. СЗ проектируется для того, чтобы облегчить регулярное подтверждение соответствия функций защиты;

с) слой защиты, обеспечиваемый функцией безопасности ПСБ, — это такой слой защиты, реализация которого удовлетворяет определению ПСБ, принятому в МЭК 61511-1:2016, 3.2.69 (термин «ПСБ» был использован при разработке матрицы слоев защиты).

Литература:

Guidelines for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, CCPS, 345 East 47th Street, New York, NY 10017, 1993, ISBN 0-8169-0554-1

Layer of Protection Analysis-Simplified — Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7

CCPS/AIChE, Guidelines for Safe and Reliable Instrumented Protective Systems, Wiley-Interscience, New York (2007)

ISA 84.91.01: Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industries, The Instrumentation, Society of Automation, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA

Safety Shutdown Systems: Design, Analysis and Justification, Gruhn and Cheddie, 1998, The Instrumentation, Systems, and Automation Society, 67 Alexander Drive, PO Box 12277, Research Triangle Park, NC 27709, USA, ISBN 1-55617-665-1

FM Global Property Loss Prevention Data Sheet 7-45, «Instrumentation and Control in Safety Applications», 1998, FM Global, Johnston, RI, USA

С.2 Целевой уровень безопасности процесса

Фундаментальным условием успешного управления промышленным риском является четкое и ясное определение задаваемого уровня безопасности процесса (приемлемого риска). Он может быть установлен на базе национальных и международных стандартов и правил, корпоративной политики, а также под влиянием заинтересованных сторон, таких как сообщества и/или местные органы и страховые компании с хорошей технической подготовкой. Заданный уровень безопасности процесса специфичен для конкретного процесса, корпорации или отрасли. Таким образом, обобщения невозможны, за исключением ситуаций, когда существующие правила и стандарты обеспечивают поддержку таким обобщениям.

С.3 Анализ опасности

Для того чтобы выявить опасности, возможные отклонения процесса и их причины, исходные события и потенциально опасные события (инциденты) в используемых технических системах, следует провести анализ опасностей процесса. Для этого могут быть использованы следующие методы качественного анализа:

- анализ безопасности;
- контрольные листы;
- анализ гипотез («что произойдет, если»);
- метод HAZOP;
- анализ видов и последствий отказов;
- анализ причин и последствий.

Одним из таких методов, получивших широкое применение, является метод анализа опасности и работоспособности (Hazadr and Operability, HAZOP). Анализ (или изучение) опасности и работоспособности выявляет и оценивает опасности для технологической установки, а также другие неопасные проблемы, связанные с работоспособностью, которые ставят под сомнение возможность достижения проектной производительности установки.

Метод HAZOP подробно рассмотрен в МЭК 61882:2001. Применение этого метода требует детальных знаний и понимания вопросов проектирования объекта, его функционирования и обслуживания. Обычно опытный руководитель осуществляющей анализ группы специалистов, выполняя процесс разработки, постоянно «ведет» свою команду, используя при этом соответствующий набор подсказок. Такие подсказки применяются в особые или ключевые моменты исследования объекта с учетом соответствующих параметров процесса. Все это позволяет обнаружить возможные отклонения от нормального функционирования процесса. Контрольные листы или опыт выполнения процесса также помогают группе исследователей составить необходимый перечень возможных отклонений, который подлежит рассмотрению в процессе анализа. В результате анализа группа составляет перечни возможных причин отклонений в процессе, последствий таких отклонений, а также необходимых организационных

и технических систем. Если причины и последствия отклонений в процессе существенны, а имеющиеся меры защиты недостаточны, то группа может представить на рассмотрение руководства предложения по дополнительным мерам безопасности или по перечню последующих действий.

Часто оказывается возможным обобщить приобретенный на конкретном объекте опыт и результаты его исследования методом HAZOP и распространить все это на имеющиеся в компании аналогичные процессы. Если такое обобщение возможно, то применение метода матрицы слоев безопасности оказывается целесообразным и при ограниченных ресурсах.

С.4 Метод анализа риска

После того как анализ по методу HAZOP проведен, связанный с процессом риск можно оценить, используя как количественные, так и качественные методы. В основе этих методов лежат экспертные оценки, сделанные персоналом предприятия и другими специалистами в области анализа опасности и риска, позволяющие выявить потенциально опасные события и оценить их возможность, интенсивность и последствия.

Для оценки риска процесса может быть использован качественный подход, который позволяет проследить сценарий развития опасного события и оценить его вероятность (примерный диапазон возможности появления) и тяжесть.

Типичное руководство по оценке возможности появления опасных событий без учета действующих СЗ показано в таблице С.1. Данные, приведенные в таблице, носят общий характер и могут быть использованы в тех случаях, когда сведения о конкретном процессе или производстве отсутствуют. Однако если такие конкретные данные имеются, то именно их следует использовать для установления возможности появления опасных событий.

Аналогично в таблице С.2 показан один из способов ранжирования тяжести воздействия опасных событий при их относительном оценивании. Предложенные рейтинги также являются иллюстративными. Тяжесть воздействия опасных событий и их рейтинги строятся для конкретного предприятия (процесса) на базе экспертных оценок и имеющегося опыта.

Таблица С.1 — Частота возможности появления опасного события (без учета СЗ)

Тип события	Возможность возникновения
	Качественное ранжирование
Множественные отказы различных приборов или клапанов, множественные ошибки персонала при нормальных внешних условиях или спонтанные отказы технологического оборудования	Низкая
Отказы резервированных приборов, клапанов или большие выбросы в зонах загрузки/разгрузки	Средняя
Утечки в процессе, отказы отдельных приборов или клапанов, ошибки персонала, приводящие к небольшим выбросам опасных материалов	Высокая
Примечание — Считается, что система соответствует настоящему стандарту, если утверждается, что отказ функции управления происходит реже чем 10^{-1} в год.	

Таблица С.2 — Критерии ранжирования тяжести воздействия опасных событий

Ранг тяжести	Результат
Значительное	Значительный ущерб оборудованию. Останов процесса на длительное время. Катастрофические последствия для персонала и окружающей среды
Серьезное	Ущерб оборудованию. Кратковременная остановка процесса. Серьезные последствия для персонала и окружающей среды
Малое	Незначительный ущерб оборудованию. Отсутствие остановки процесса. Малый ущерб для персонала и окружающей среды

С.5 Матрица слоев безопасности

Для оценки риска можно использовать матрицу риска, объединяющую вероятность появления опасных событий и рейтинг тяжести их воздействия. Аналогичный подход можно применить и для построения матрицы, которая бы определяла потенциальное снижение риска, связанное с используемой ПСБ для слоя защиты. Подобная матрица риска показана на рисунке С.2, на котором в матрицу был введен целевой уровень безопасности процесса. Иными словами, матрица базируется на конкретном опыте эксплуатации и критериях риска, принятых в данной компании, на принятых в этой компании принципах разработки, эксплуатации и защиты, а также на значении уровня безопасности, установленном компанией в качестве целевого уровня безопасности процесса.

С.6 Общая процедура:

a) установить целевой уровень безопасности процесса;

b) провести анализ возможных опасностей (например, методом HAZOP), чтобы выявить все опасные события, представляющие интерес;

c) построить сценарий развития опасного события и оценить возможность появления этого события, пользуясь при этом данными и руководящими материалами конкретной фирмы;

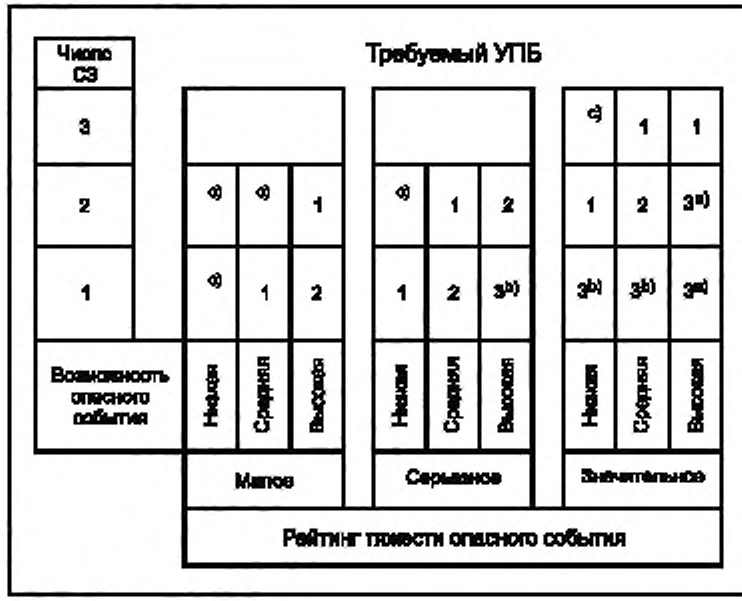
d) пользуясь руководящими материалами компании, установить рейтинг тяжести опасных событий;

e) определить используемые на объекте СЗ (см. рисунок С.2). Оцениваемую возможность появления опасных событий следует снижать в 10 раз для каждого СЗ;

f) определить необходимость применения дополнительного слоя защиты, реализуемого ПСБ, путем сравнения остаточного риска с величиной целевого уровня безопасности процесса;

g) определить уровень полноты безопасности системы, пользуясь рисунком С.2;

h) пользователь должен следовать С.1, перечисление b).



[a] Одна функция безопасности ПСБ с УБП 3 не обеспечивает при таком уровне риска достаточного его снижения. Чтобы снизить риск, требуются дополнительные изменения.

[b] Одна функция безопасности ПСБ с УБП 3 может не обеспечить при таком уровне риска достаточного его снижения. Требуется дополнительный анализ.

[c] Вероятно, нет необходимости в слое защиты на основе ПСБ.

Примечания

1 Общее число слоев защиты включает все СЗ, защищающие процесс, в том числе и классифицируемые ПСБ (при необходимости).

2 Возможность появления опасного события — это возможность того, что опасное событие произойдет при отключенных СЗ. В качестве руководящего указания см. таблицу С.1.

3 Тяжесть опасного события — воздействие, связанное с опасным событием. В качестве руководства см. таблицу С.2.

4 Такой поход не считается пригодным в случаях с УПБ 4.

Рисунок С.2 — Пример матрицы слоев безопасности

Приложение D
(справочное)

Полукачественный метод. Калиброванный граф риска

D.1 Введение

Данное приложение базируется на общей схеме формирования графа риска, описанной в МЭК 61508-5, Е.1. Настоящее приложение адаптировано таким образом, чтобы лучше соответствовать потребностям технологических процессов в промышленности.

В данном приложении описан метод калиброванного графа риска, применяемый для определения УПБ функций безопасности ПСБ. Этот полукачественный метод позволяет при известных факторах риска, связанных с процессом и базовой системой управления, определить УПБ функций безопасности ПСБ.

В принятом подходе используется ряд параметров, которые в совокупности описывают природу опасной ситуации, возникающей в случае отказа ПСБ или при ее отсутствии. В каждом из четырех наборов параметров выбирается по одному. Выбранные параметры затем объединяются, чтобы решить, какому уровню полноты безопасности должны соответствовать функции безопасности ПСБ. Эти параметры:

- позволяют получить ранжированную оценку рисков и
- представляют собой ключевые факторы оценки риска.

Подход, связанный с применением графа риска, может быть также использован для определения необходимости снижения риска в случае, когда последствия связаны с существенным ущербом для окружающей среды или с материальными потерями. Цель настоящего приложения — предложить руководство по применению метода.

Сначала в настоящем приложении рассматриваются вопросы защиты персонала от опасности. Представлена одна из возможностей применения к технологическому процессу общего графа риска, приведенного в МЭК 61508-5 (рисунок Е.1). В заключение рассматривается применение метода графа риска для защиты окружающей среды и имущества.

D.2 Синтез графа риска

Риск определяется как комбинация вероятности возникновения вреда и серьезности этого вреда (см. МЭК 61511-1, раздел 3). Обычно применительно к технологическому процессу риск является функцией следующих четырех параметров:

- последствия опасной ситуации (С);
- нахождение в опасной зоне (вероятность того, что в подверженной опасности области находятся люди) (F);
- вероятность того, что опасности можно избежать (Р);
- интенсивность запросов (число случаев за год, когда опасная ситуация возникает в отсутствие рассматриваемой функции безопасности ПСБ) (W).

Если граф риска применяется для определения УПБ функции безопасности, выполняемой в непрерывном режиме, то следует рассмотреть необходимость изменения параметров, используемых в графе риска. Такие параметры (см. таблицу D.1) должны представлять собой факторы риска, которые наилучшим образом соотносятся с характеристиками рассматриваемого объекта. Необходимо также будет рассмотреть соответствие уровней полноты безопасности результатам решений по выбору параметров, поскольку для снижения риска до допустимого уровня может понадобиться некоторая настройка. Например, параметр W может быть переопределен как общее время работы системы, выраженное в процентах от общего времени ее существования. При таком выборе W1 опасность не является непрерывно действующим фактором и период времени, в котором отказ будет приводить к появлению опасности, будет составлять малую долю года. В этом примере следует пересмотреть и другие параметры, чтобы соответствующие критерии принятия решения и пересмотренные результаты определения УПБ гарантировали допустимый риск.

Таблица D.1 — Описание параметров графа риска для промышленных процессов

Параметр		Описание
Последствия	С	Число жертв и/или серьезных травм, которые, вероятно, появятся в результате опасного события. Определяется путем подсчета числа людей в подверженной опасности области с учетом их уязвимости по отношению к опасному событию
Нахождение в опасной зоне	F	Вероятность того, что в подверженной опасности области во время опасного события находятся люди. Определяется путем расчета доли времени, в течение которого в области находились люди, по отношению ко времени действия опасного события. При этом следует исходить из большей вероятности нахождения людей в опасной области, что позволит изучить нештатные ситуации, которые могут возникнуть при развитии опасного события (следует также оценить, не приведет ли это к необходимости пересмотра параметра С)

Окончание таблицы D.1

Параметр		Описание
Вероятность того, что опасности можно избежать	P	Вероятность того, что люди могут избежать опасной ситуации, которая существует при отказе функции безопасности ПСБ, выполняемой по запросу. Она зависит от того, существуют ли независимые способы предупреждения людей об опасности, прежде чем она возникнет, и о путях эвакуации
Интенсивность запросов	W	Количество случаев в год, когда опасное событие происходит при отсутствии рассматриваемой функции безопасности ПСБ. Его можно определить, рассмотрев все отказы, приводящие к опасному событию, и оценив общую частоту происшествий. Другие СЗ также должны учитываться

D.3 Калибровка

Процесс калибровки преследует следующие цели:

a) описать все параметры таким образом, чтобы дать возможность команде, занимающейся оценкой УПБ, сделать объективное заключение, основанное на характеристиках объекта;

b) обеспечить соответствие выбранного для данного объекта УПБ корпоративному критерию риска и обеспечить при определении УПБ учет возможного риска со стороны других источников;

c) обеспечить проверку процесса выбора параметров.

Калибровка графа риска — это процесс присвоения численных значений параметрам графа риска. При этом формируется базис для оценки существующего риска процесса и оказывается возможным определить требуемую полноту безопасности рассматриваемой функции безопасности ПСБ. Каждому параметру присваивается диапазон значений, таких, что, будучи примененными в комбинации, они позволяют получить количественную оценку риска, существующего в отсутствие данной функции безопасности. Так, устанавливается мера степени доверия функции безопасности ПСБ. Граф риска связывает определенные комбинации параметров риска с УПБ. Связь между комбинациями параметров риска и УПБ устанавливается путем рассмотрения величины допустимого риска, связанного с конкретной опасностью. В приложении I см. описание процесса калибровки (I.2 и I.4.7).

Рассматривая калибровку графа риска, важно принять во внимание требования к риску, возникающие как со стороны собственников, так и со стороны регламентирующих органов. Риск для жизни может быть рассмотрен с двух позиций:

- индивидуальный риск — определяется как риск в течение года для лиц, наиболее подверженных риску. Обычно задается максимально допустимое его значение, которое обычно учитывает совокупность воздействий от всех источников опасности;
- общественный риск — определяется как общий риск в течение года, испытываемый группой лиц. Обычное требование в этом случае состоит в том, чтобы снизить общественный риск по меньшей мере до такого значения, которое может быть воспринято обществом как допустимое и дальнейшее снижение которого связано с непропорциональными по отношению к результату затратами.

Если необходимо снизить индивидуальный риск до определенного максимально допустимого уровня, то нельзя полагать, что такое снижение риска может быть достигнуто применением какой-либо одной ПСБ. Лицо, подвергаемое риску, может находиться под воздействием многих его источников (например, риски падения, пожара, взрыва).

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.

Широко применяемый критерий для общественного риска базируется на вероятности F появления N фатальных исходов. Критерий допустимого общественного риска имеет вид кривой или семейства кривых в логарифмической шкале, связывающих число фатальных исходов с частотой несчастных случаев. Проверка соблюдения требований к общественному риску выполняется путем построения кривой, отражающей зависимость накопленной частоты возникновения несчастных случаев от их последствий [кривая $F(N)$]. Далее следует убедиться, что эта кривая не пересекает кривую допустимого риска. Руководство по разработке критериев для общественных рисков включено в британскую публикацию HSE «Reducing Risks, Protecting People», ISBN 0 7176 2151 0.

Четыре параметра риска, перечисленные в D.2, включены в дерево решений, представленное на рисунке D.1. Все вышеупомянутые проблемы следует принять во внимание перед тем, как установить значения каждого из параметров. Большинству параметров присваивается определенный диапазон (например, если ожидаемая частота запросов конкретного процесса оказывается в пределах определенного уровня значений запросов в

год, то можно использовать параметр W3). Аналогично в случае запросов, имеющих частоту на порядок ниже, применяется параметр W2, а на следующем, еще более низком уровне — параметр W1. 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. Риск, связанный с каждой из комбинаций параметров, далее оценивается с позиций индивидуального и социального риска. Затем можно определить величину снижения риска, удовлетворяющую требованиям (риск должен быть равен или меньше допустимого). С помощью этого метода для каждой комбинации параметров может быть определен уровень полноты безопасности. Нет необходимости проводить эту работу по калибровке каждый раз, когда требуется определить УПБ для конкретного случая. Как правило, бывает достаточно провести эту работу однократно для каждой опасности. Если исходные предположения, принятые при калибровке, оказываются неверными для конкретного проекта, то могут потребоваться уточнения.

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

Важно, чтобы этот процесс калибровки был согласован в организации на верхнем уровне, отвечающем за безопасность. Принятые решения определяют общий достигнутый уровень безопасности.

В общем случае с помощью графа риска сложно определить возможность зависимого отказа между источниками запроса и ПСБ. При этом может потребоваться провести переоценку эффективности ПСБ.

D.4 Организация и состав команды специалистов для определения УПБ

Маловероятно, чтобы отдельный специалист обладал необходимым умением и опытом для принятия самостоятельного решения относительно всех соответствующих параметров. Для этого обычно используют командный подход, причем задача команды — определить уровни полноты безопасности. В состав такой команды, как правило, входят:

- специалист по технологическому процессу;
- инженер — специалист по управлению процессом;
- инженер по эксплуатации;
- специалист по безопасности;
- специалист, имеющий практический опыт эксплуатации рассматриваемого процесса.

Команда обычно рассматривает поочередно каждую функцию безопасности ПСБ. При этом команде требуется иметь подробную информацию о процессе и вероятном числе лиц, подвергающихся риску.

D.5 Оформление документов по результатам определения УПБ

Очень важно, чтобы все решения, принимаемые в процессе определения УПБ, были зафиксированы в документах, связанных с управлением конфигурацией. Из документации должно быть ясно, почему командой были выбраны данные конкретные параметры, связанные с функцией безопасности. Заполненные формы принятых предположений и основанных на них результатах определения УПБ каждой функции безопасности должны быть скомплектованы в досье. Если установлено, что в области, обслуживаемой одной командой, имеется целый ряд систем, выполняющих функции безопасности, то может оказаться необходимым пересмотреть правомерность допущений, принятых при калибровке. В досье следует также включать следующую дополнительную информацию:

- граф риска с описанием всех диапазонов параметров;
- номера всех используемых проектных и измененных документов;
- ссылки на известные допущения и результаты любых исследований, которые были использованы при оценке параметров;
- ссылки на отказы, которые приводили к запросам, и на ошибочные модели развития события, в которых эти отказы были использованы для определения частоты запросов;
- ссылки на источники данных, использованных при определении интенсивности запросов.

D.6 Пример калибровки, основанной на типовых критериях

Таблица D.2, в которой даны описания параметров и диапазоны каждого из них, была составлена в соответствии с конкретными критериями, типичными для химических процессов, по процедуре, рассмотренной выше. Прежде чем использовать эту таблицу в контексте любого проекта, важно подтвердить, что она отвечает требованиям тех лиц, которые несут ответственность за безопасность.

Для модификации параметра, характеризующего последствия, введена концепция степени защищенности, поскольку во многих случаях отказ не приводит к немедленному фатальному исходу. Уязвимость лица, подвергающегося опасности, — это важный аспект анализа риска, поскольку, например, доза опасного воздействия, полученная человеком, может оказаться недостаточной для того, чтобы вызвать фатальный исход. Уязвимость по отношению к последствиям опасного события есть функция концентрации опасности, которой подвергся человек, и длительности воздействия этой опасности. Пусть, например, отказ приводит к повышению давления в сосуде, но не выше давления, при котором он был испытан. Обычно подобный отказ может привести к утечке через фланец.

В этом случае события, скорее всего, будут развиваться достаточно медленно, и у обслуживающего персонала будет возможность избежать последствий. Даже в случае большой утечки жидких компонентов развитие опасности будет достаточно медленным, и обслуживающему персоналу с большой вероятностью удастся избежать опасности. Конечно, встречаются случаи, в которых отказ может приводить к разрыву трубопровода или стенки сосуда; в таких случаях уязвимость персонала может быть высокой.

Анализ признаков развития опасного события может привести к увеличению количества людей, находящихся в опасности. Всегда следует рассмотреть наихудший сценарий развития событий.

Важно осознать разницу между «уязвимостью» (V) и «вероятностью того, что опасности можно избежать» (P), что позволит не учитывать дважды один и тот же фактор. Уязвимость — это мера, которая связана со скоростью развития событий после возникновения опасности, в то время как параметр P — это мера, связанная с предотвращением опасности. Параметр P_A следует применять только в тех случаях, когда опасность может быть предотвращена в результате действий оператора, после того как он придет к выводу, что ПСБ отказала.

Существуют некоторые ограничения на выбор параметров нахождения в опасной зоне. Параметр нахождения в опасной зоне требуется выбирать по наименее защищенному лицу, а не по среднему для всех лиц. Обоснованием этому является стремление обеспечить, чтобы ни такое лицо, ни тем более остальные люди не подвергались высокому риску.

Если какой-либо из параметров не попадает в определенный диапазон, то требования к снижению риска следует установить каким-либо иным методом или провести повторную калибровку графа риска, используя описанные выше методы.

Рисунок D.1 должен всегда использоваться с повторной калибровкой, чтобы настроить критерии риска для производственного помещения. Данный метод нельзя пытаться использовать для любого производственного помещения без подходящих критериев риска. Путь, которым выполняется калибровка, будет зависеть от того, как выражены критерии допустимого риска. Описания параметров должны быть подобраны так, чтобы они соответствовали диапазону предназначенного применения и допустимости риска. Значения C, F, P или W могут быть изменены. В качестве примера в таблице D.2 показана калибровка, где значение W подбирается с помощью параметра калибровки D так, чтобы настроить его на указанные критерии риска.

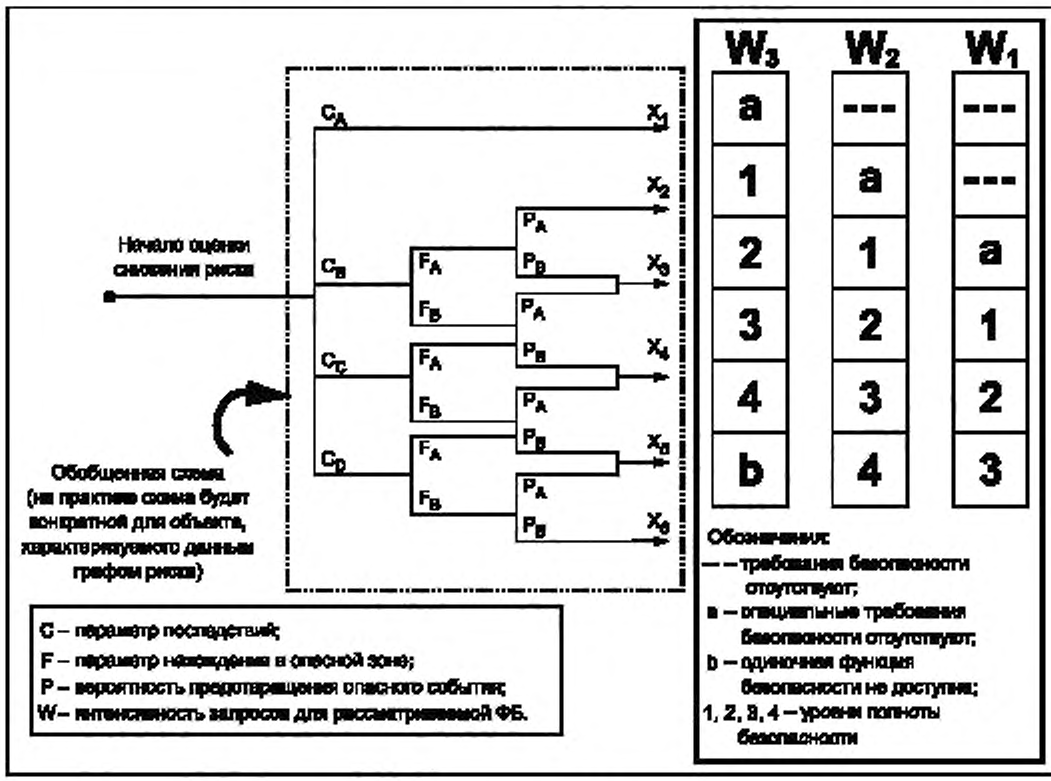


Рисунок D.1 — Граф риска. Общая схема

Таблица D.2 — Пример калибровки графа риска 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 высокотоксичный материал. V = 1 Разрушение или взрыв	C_A C_B C_C C_D	Минимальный ущерб Диапазон 0,01—0,1 Диапазон > 0,1—1,0 Диапазон > 1,0	a) Система классификации относится к случаям фатального исхода или травм для людей. b) При интерпретации параметров C_A, C_B, C_C и C_D следует принимать во внимание последствия несчастного случая и нормальное их устранение
Нахождение в опасной зоне (F). Определяется как доля времени пребывания людей в области, подвергающейся опасности, по отношению к величине периода работы. Примечания 1 Если время пребывания в опасной зоне 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 в опасной зоне 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 зоне. Нахождения в опасной зоне меньше чем 0,1. От частого до постоянного пребывания в опасной зоне	c) См. выше комментарий a)
Вероятность избежать опасного события (P). если отказывает система защиты	P_A P_B	Принимается, если выполняются условия графы 4. Принимается, если условия не выполняются	d) P_A следует выбирать, только если справедливы следующие условия: - предусмотрены средства оповещения оператора об отказе ПСБ; - 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 явно достаточное для выполнения необходимых действий
Интенсивность (частота) запросов (W). Количество случаев в год возникновения опасного события при отсутствии ПСБ. Для того 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	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 между *D* и 10 *D*.	e) Цель введения фактора W — оценить частоту появления опасности без ПСБ. Если частота запроса очень велика, то УПБ следует определять либо другим методом, либо путем повторной калибровки графа риска. Следует отметить, что методы графа риска могут оказаться не лучшим решением задачи, если объект работает в

Окончание таблицы D.2

Параметр риска		Классификация	Комментарии
и эксплуатируется не в соответствии с МЭК 61511, то ее функционирование ограничено уровнем безопасности ниже, чем УПБ 1. Частота запросов (W) равна частоте запросов к рассматриваемой функции безопасности ПСБ		При частотах запросов больших, чем 10 *D*, потребуется более высокий уровень полноты безопасности	непрерывном режиме (см. МЭК 61511-1, пункт 3.2.39.2). f) *D* является параметром калибровки, значение которого следует определять, исходя из корпоративного критерия допустимого риска с учетом других источников риска для людей, ему подвергающихся. Числовые значения, которые будут использоваться для каждого значения W в таблице, должны быть получены с помощью процедуры калибровки графа риска, описанной в D.3 или приложении I
Примечание — Данный пример предназначен для иллюстрации принципов построения графов риска. Граф риска для конкретного приложения и конкретных опасных ситуаций должен быть согласован с условиями, учитываемыми при определении допустимого риска (см. D.1—D.6).			

D.7 Применение графа риска, когда последствия — это причинение вреда окружающей среде

Подход, использующий граф риска, может быть также применен для определения требований уровня полноты безопасности, когда последствия отказа включают причинение серьезного вреда окружающей среде. Необходимый УПБ зависит от характеристик субстанции, попадающей в окружающую среду, и от чувствительности последней. Ниже приведена общая таблица, в которой последствия опасного события сформулированы в терминах окружающей среды. На каждом отдельно размещенном предприятии может быть использовано некое вещество, о наличии которого следует уведомить местные власти. Уже на стадии проектирования следует установить, что может быть приемлемым для конкретного местоположения.

Описанные выше последствия опасного события могут быть использованы для анализа совместно со специальной формой графа риска, которая приведена ниже (см. рисунок D.2). Следует отметить, что в этой версии графа риска не используется параметр F, поскольку в этом случае понятие нахождения в опасной зоне не применяют. Остальные параметры P и W используют, и их определения могут быть идентичны тем, которые были применены выше.

D.8 Применение графа риска для случая имущественных потерь

Метод графа риска можно применить для определения требований к полноте безопасности и в том случае, когда последствия отказа включают потери имущества. Потери имущества — это общие экономические потери, связанные с отказом функционирования по запросу. Они включают потери на восстановление, если был причинен вред оборудованию, а также потерю испорченной или утраченной продукции. Уровень полноты безопасности, соответствующий последствиям, связанным с такими потерями, может быть определен с помощью обыкновенного анализа стоимости. Если метод графа риска применяют для определения уровней полноты безопасности, связанных с последствиями опасного события для окружающей среды, то его целесообразно использовать и для случая имущественного ущерба. При этом требуется определить параметры C_A—C_U, которые могут изменяться в широких пределах для разных компаний.

Граф риска, аналогичный использованному для случая защиты окружающей среды, может быть сформирован и в случае имущественных потерь. Следует отметить, что в этой версии графа риска не используют параметр F, поскольку в этом случае понятие нахождения в опасной зоне не применяют. Остальные параметры P и W используют, и их определения могут быть идентичны тем, которые приведены выше.

Таблица D.3 — Общие последствия для окружающей среды

Параметр риска		Классификация	Комментарии
Последствия (C)	C_A	Выброс, причинивший не очень серьезный вред, но такой, что об этом необходимо доложить местной администрации.	Умеренный выброс из фланца или клапана. Незначительный разлив жидкости. Небольшое загрязнение земли, не влияющее на подземные воды.
	C_B	Выброс в пределах ограждения (предприятия, объекта) с причинением значительного вреда.	Облако вредных газов над установкой как следствие выброса из фланца или отказа уплотнения в компрессоре.

Окончание таблицы D.3

Параметр риска		Классификация	Комментарии
	C_C	Выброс за ограждение с причинением существенного вреда, однако последствия могут быть быстро ликвидированы без значительных длительных последствий.	Выброс пара или аэрозоля с одновременным выбросом жидкости (или без него), причинивший временный ущерб флоре или фауне. Сброс жидкости в реку или море.
	C_D	Выброс за ограждение с причинением существенного вреда, когда последствия не могут быть быстро ликвидированы или имеются значительные длительные последствия	Выброс пара или аэрозоля с одновременным выбросом жидкости (или без него), причинивший длительный ущерб растениям и фауне. Выброс твердых веществ (пыли, катализатора, золы). Выброс жидкости с попаданием в подземные воды

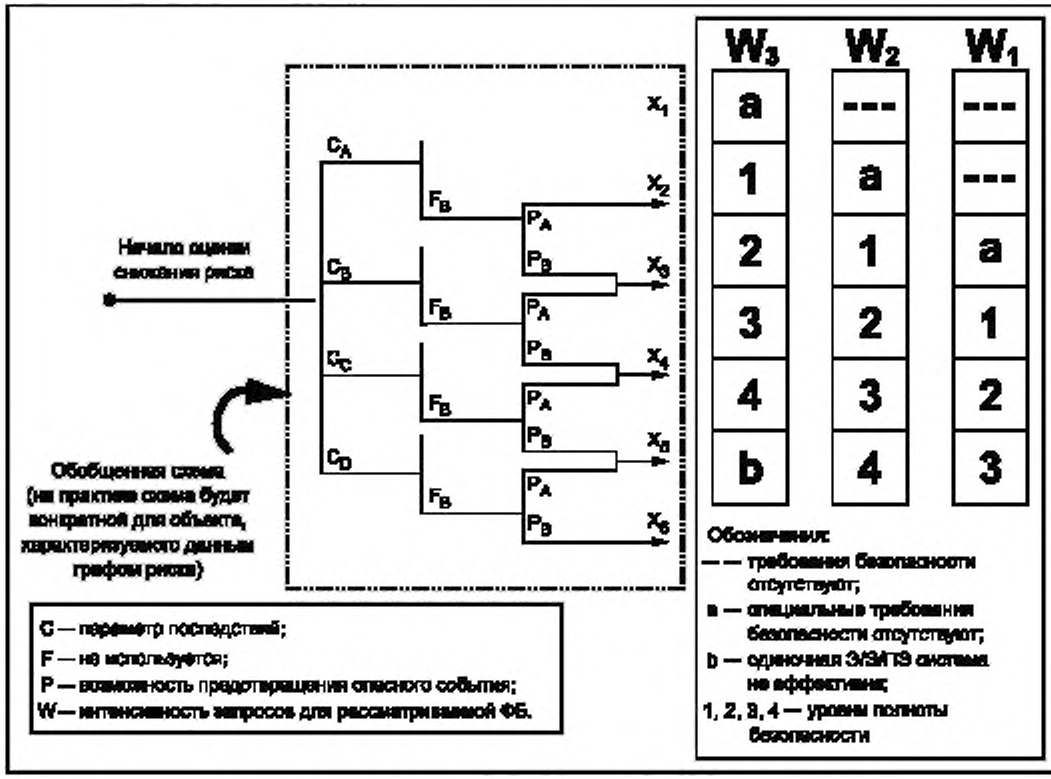


Рисунок D.2 — Граф риска. Случай ущерба для окружающей среды

D.9 Определение УПБ для функции безопасности ПСБ, когда последствия опасного события включают более одного вида потерь

Часто последствия отказа при выполнении действий по запросу связаны с несколькими категориями потерь. В таких случаях требования к УПБ, связанные с каждой из категорий потерь, следует определять отдельно. При этом для анализа каждого вида выявленного риска можно использовать различные методы. Если происходит отказ функции, выполняемой по запросу, УПБ, установленный для такой конкретной функции, должен учитывать кумулятивное воздействие всех выявленных рисков.

Приложение Е
(справочное)

Качественный метод. Граф риска

Е.1 Общие сведения

В данном приложении описан метод графа риска для определения УПБ функций безопасности ПСБ. Это качественный метод, который позволяет определить УПБ функций безопасности ПСБ при известных факторах риска, связанных с процессом и с его основной системой управления процессом.

В предлагаемом подходе использован ряд параметров, которые совместно описывают природу опасной ситуации, возникающей в случае отказа или отсутствия ПСБ. В каждом из четырех наборов параметров выбирают по одному параметру. Комбинация выбранных параметров позволяет установить уровень полноты безопасности для функций безопасности ПСБ. Указанные параметры:

- позволяют получить ранжированную оценку уровней риска и
- представляют собой ключевые факторы оценки риска.

Подход, использующий граф риска, может быть также применен для определения необходимости снижения риска в тех случаях, когда последствия включают серьезный ущерб для окружающей среды или имущественные потери.

Представленный в настоящем приложении метод подробно описан в VDI/VDE 2180 (2015).

Е.2 Типовая реализация функций безопасности ПСБ

Существует четкое различие между общими задачами обеспечения безопасности объекта и эксплуатационными требованиями к безопасности процесса, реализуемыми с помощью средств управления процессом. В связи с этим применяется следующая классификация систем управления процессом:

- основная система управления процессом;
- система мониторинга процесса;
- приборная система безопасности.

Цель такой классификации — сформулировать требования к каждому типу систем, необходимые для выполнения полных требований предприятия при экономически разумных затратах. Эта классификация позволяет детально очертить круг вопросов, решаемых при планировании, сооружении и эксплуатации объекта, а также при его последующей модификации в части системы управления процессом.

ОСУП используются для обеспечения правильного функционирования процесса в нормальных условиях. Такая система реализует измерение, управление и/или запись всех соответствующих переменных процесса. ОСУП или действует в непрерывном режиме, или к ее действиям прибегают для вмешательства в ход процесса до того, как оказывается необходимой реакция ПСБ. (В ОСУП обычно нет необходимости соблюдать требования МЭК 61511-1.)

Системы мониторинга процесса действуют при определенных условиях, когда одна или более из переменных процесса оказываются вне нормального диапазона изменения. Системы мониторинга выполняют предаварийную сигнализацию нарушений допустимого состояния процесса, чтобы привлечь внимание оперативного персонала или стимулировать вмешательство человека в работу объекта. (Система мониторинга обычно не нуждается в необходимости соблюдать требования МЭК 61511-1.)

ПСБ либо предотвращают опасное состояние объекта («система защиты»), либо снижают последствия опасного события.

Если ПСБ отсутствует, то возможно возникновение опасного события с травмами для персонала.

В отличие от функций ОСУП, для функций ПСБ обычно характерна низкая частота запросов. Это происходит прежде всего потому, что вероятность опасного события низка. Кроме того, объект всегда оснащен ОСУП и системами мониторинга, которые способствуют снижению частоты запросов к ПСБ.

Е.3 Синтез графа риска

Граф риска базируется на том принципе, что риск пропорционален частоте появления опасного события и размеру его последствий. Первоначально принимается, что приборных систем безопасности нет, зато присутствуют ОСУП и системы мониторинга, не являющиеся приборными системами безопасности.

Последствия связаны с причинением вреда здоровью и безопасностью или причинением вреда окружающей среде.

Частота появления опасных событий зависит от комбинации следующих факторов:

- частоты и возможного времени пребывания людей в опасной зоне;
- возможности избежать опасного события;
- вероятности возникновения опасного события при отсутствии ПСБ (все остальные средства снижения внешнего риска предполагаются действующими), так называемой «вероятности нежелательного события».

Из сказанного следует, что существуют четыре параметра риска:

- последствие опасного события (S);
- частота пребывания в опасной зоне, умноженная на время воздействия опасных условий (A);
- возможность избежать последствий опасного события (G);
- вероятность нежелательного происшествия (W).

Если граф риска применяют для определения УПБ функции безопасности ПСБ, выполняемой в непрерывном режиме, то необходимо рассмотреть изменения параметров, используемых в графе риска. Рекомендуется, чтобы параметры, представляющие факторы риска, наилучшим образом соответствовали характеристикам рассматриваемого применения. Необходимо также рассмотреть связь УПБ с решениями по выбору параметров, поскольку для обеспечения снижения риска до приемлемого уровня может понадобиться настройка. Например, параметр W может быть определен заново как процентное отношение времени активной работы системы безопасности к общему времени ее работы на объекте. При таком выборе W1 опасность не является непрерывно действующим фактором, и период времени, в котором отказ будет приводить к появлению опасности, будет составлять малую долю года. В этом примере следует пересмотреть и другие параметры, чтобы соответствующие критерии принятия решения и пересмотренные результаты определения УПБ обеспечивали допустимый риск.

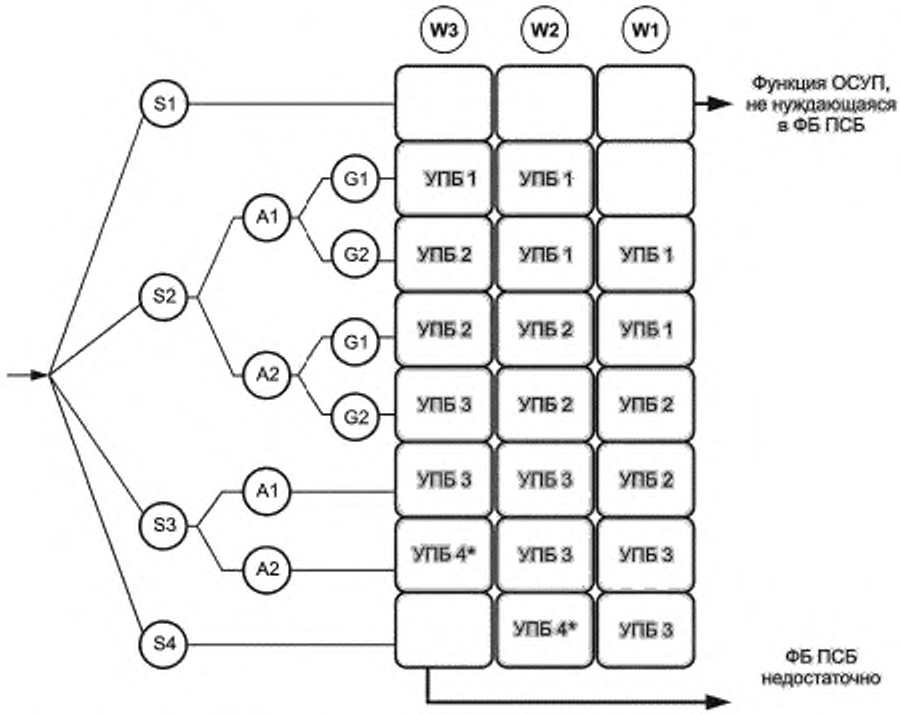
Е.4 Реализация графа риска. Защита персонала

Граф риска, соответствующий описанной выше комбинации параметров, показан на рисунке Е.1. Параметры с более высокими значениями индексов соответствуют более высокому риску (S1 < S2 < S3 < S4; A1 < A2; G1 < G2; W1 < W2 < W3). Классификация параметров, соответствующая рисунку Е.1, приведена в таблице Е.1. Граф применяется отдельно для каждой функции безопасности и позволяет определить для нее требуемый УПБ.

При определении риска, который должен быть предотвращен ПСБ, оценку риска следует проводить, исходя из отсутствия на объекте рассматриваемой ПСБ. Основные исходные параметры такой оценки — это тип и масштабы развития воздействий, а также ожидаемая частота появления опасного состояния технологического процесса.

Риск может быть последовательно определен и проверен с помощью метода, подробно изложенного в VDI/VDE 2180, который позволяет по установленным параметрам определить классы требований. Как правило, чем выше порядковый номер класса требований, тем большая часть риска снимается приборной системой безопасности и, следовательно, в общем случае более строгими являются требования и результирующие показатели.

Для промышленных процессов УПБ 4 не обеспечивается только ПСБ. Для снижения риска по крайней мере до УПБ 3 необходимы специальные средства управления, не связанные с процессом.



* Не рекомендуется использовать ФБ ПСБ.

Примечание — Разные цвета предназначены облегчить идентификацию разных значений УПБ.

Рисунок Е.1 — Граф риска по VDI/VDE 2180. Защита персонала и связь с УПБ

Е.5 Вопросы, которые следует рассмотреть при применении графов риска

Применяя метод графа риска, очень важно рассмотреть требования, предъявляемые собственником и регламентирующими органами.

Интерпретацию и оценку каждой ветви графа риска следует описывать и документально оформлять в ясных и понятных терминах для обеспечения последовательности использования метода.

Очень важно, чтобы граф риска и его окружение были согласованы с руководством компании, отвечающей за безопасность.

Таблица Е.1 — Данные, относящиеся к графу риска (см. рисунок Е.1)

Параметр риска		Классификация	Комментарий
Последствия опасного события. Уровень тяжести (S)	S1	Легкие травмы у персонала	1 Эта система классификации отражает события, связанные с травмами или смертью людей. Для случаев ущерба окружающей среде и имуществу потребуются другие системы классификации
	S2	Серьезные травмы у одного или более человек. Один смертельный исход	
	S3	Смерть нескольких человек	
	S4	Катастрофические последствия, многочисленные жертвы	
Частота фактов пребывания в опасной области, умноженная на время пребывания (А)	A1	От редкого до более частого пребывания в опасной зоне	2 См. выше комментарий 1
	A2	От частого до постоянного пребывания в опасной зоне	
Возможность избежать последствий опасного события (G)	G1	Возможно при некоторых условиях	3 Этот параметр учитывает следующее: - управление процессом контролируемое (т. е. выполняемое квалифицированными или неквалифицированными лицами) или неконтролируемое; - темп развития опасного события (например, внезапно, быстро или медленно); - легкость распознавания опасности (например, видна непосредственно, распознается с помощью или без помощи технических средств); - возможность избежать последствий опасного события (например, эвакуация возможна, невозможна или возможна при определенных обстоятельствах); - наличие фактического опыта в области безопасности (такой опыт мог быть приобретен на аналогичных или подобных объектах или опыт отсутствует)
	G2	Почти невозможно	
Возможность возникновения нежелательного события (W)	W1	Очень малая вероятность появления нежелательных событий. Возможно лишь редкое их появление	4 Назначение фактора W — оценить частоту появления нежелательных событий при отсутствии приборной системы безопасности (Э/Э/ПЭ или иные технологии), но при применении каких-либо внешних средств снижения риска
	W2	Малая вероятность появления нежелательных событий. Возможно лишь редкое их появление	
	W3	Относительно высокая вероятность появления нежелательных событий. Возможно частое их появление	

Приложение F
(справочное)

Анализ слоев защиты

F.1 Введение

В данном приложении описан метод, получивший название «Анализ слоев защиты» (АСЗ). Исходными данными для применения этого метода являются результаты анализа, полученные методом HAZOP. Далее учитывают каждую выявленную опасность путем документального оформления всех вызвавших ее причин. Кроме этого учитывают все слои защиты, которые предотвращают либо ослабляют эту опасность. По этим данным определяют общую меру снижения риска и анализируют необходимость дальнейшего его снижения. Если необходимо дальнейшее снижение риска и его предполагается проводить путем введения функции безопасности ПСБ, то метод АСЗ позволяет определить соответствующий этой функции УПБ.

Данное приложение не содержит подробного описания метода, а предназначено для иллюстрации общих принципов его применения. Более подробно метод описан в Guideline for Safe Automation of Chemical Processes, American Institute of Chemical Engineers, CCPS, 345 East 47th Street, New York, NY 10017, 1993, ISBN 0-8169-0554-1.

Пример применения метода АСЗ см. также в МЭК 61511-2, F.11.

Численные значения, представленные в данном приложении, не должны применяться в качестве универсальных и использоваться в конкретном слое защиты при анализе приложений.

Жизненный цикл ПСБ, определенный в МЭК 61511-1, требует определения УПБ при создании функции безопасности ПСБ. Метод АСЗ, описываемый ниже, позволяет группе, состоящей из специалистов разного профиля, определить УПБ для функций безопасности ПСБ на действующем объекте. В состав группы должны входить следующие специалисты:

- оператор, имеющий опыт работы с рассматриваемым процессом;
- инженер — эксперт по данному процессу;
- технолог;
- инженер — специалист в области управления процессами;
- специалист по техническому обслуживанию аппаратуры (в том числе электрической), имеющий опыт эксплуатации данного процесса;
- специалист в области анализа риска.

Один из участников группы должен быть обучен применению метода АСЗ.

Информация, требующаяся для применения метода АСЗ, содержится в данных, собранных и полученных в результате применения анализа опасности и работоспособности (HAZOP). Связь между данными, требующимися для применения АСЗ, и данными, полученными методом HAZOP, показана в таблице F.1. На рисунке F.1 показана типичная форма, которую можно использовать при применении метода АСЗ.

Метод АСЗ анализирует опасности, чтобы определить, требуются ли функции безопасности ПСБ, и если требуются, то он позволяет для каждой из таких функций определить УПБ.

F.2 Влияющее событие

Пользуясь бланком, приведенным на рисунке F.1, описание (последствие) каждого влияющего события, полученное методом HAZOP, заносят в графу 1.

F.3 Уровень тяжести события

Далее согласно таблице F.2 выбираются уровни тяжести влияющего события: малый (*M*), серьезный (*S*) или значительный (*E*) — и заносятся в графу 2 на рисунке F.1.

Таблица F.1 — Данные, которые HAZOP готовит для АСЗ

Информация, требующаяся для АСЗ	Информация, полученная HAZOP
Влияние события	Последствия
Уровень тяжести события	Тяжесть последствий
Исходная причина	Причина
Вероятность возникновения исходной причины	Частота возникновения причин
Слои защиты	Используемые меры защиты
Требуемое дополнительное ослабление	Рекомендуемые новые меры защиты

F.4 Исходные причины

Все причины, инициирующие появление опасного события, записывают в колонку 3 на рисунке F.1. Влияющие события могут иметь много исходных причин, и важно перечислить их все.

Примечание — Если независимые слои защиты не были должным образом выбраны, то значения частоты и вероятности отказов по запросу не могут быть перемножены, как показано на рисунке F.1. См. приложение J.

№	1	2	3	4	5			6	7	8	9	10	11
					Слой защиты								
	Описание влияющего события F.2, F.13.2	Уровень тяжести, F.3 F 13.2	Исходная причина F.4, F.13.3	Вероятность исходной причины в год F.5, F 13.4	Общий проект процесса, F 13.5	ОСУП, F 13.6	Сигнализация и т.п., F.13.7	Дополнительное ослабление ограничение доступа F 7, F 13.8	Дополнительные НСЗ, ограждения, предохранительные клапаны, F.7 F.13.9	Вероятность промежуточного события, в год F 9. F 13.10	УПБ функции безопасности ПСБ, F.10, F.13.11	Вероятность ослабления влияющего события, в год F.11, F.13 11	Примечание
1	Пожар из-за разрушения колонны	*S*	Отсутствие охлаждающей воды	0,1	0,1	0.1	0,1	0,1	PRV 0,01	10^{-7}	10^{-2}	10^{-8}	Высокое давление вызвает разрушение колонны
2	Пожар из-за разрушения колонны	*S*	Отказ контура управления паром	0,1	0,1		0,1	0,1	PRV 0, 01	10^{-6}	10^{-2}	10^{-8}	То же
№													

Уровни тяжести события. *E* — значительный, *S* — серьезный, *M* — малый.

Вероятность характеризуется числом событий в год. Другие числовые данные являются средними вероятностями отказов при наличии запроса.

Рисунок F.1 — Отчет по результатам АСЗ

Таблица F.2 — Уровни тяжести влияющего события

Уровень тяжести	Последствие
Малый (*M*)	Воздействие, первоначально ограниченное локальной зоной появления события с тенденцией к расширению последствий при отсутствии корректирующих действий
Серьезный (*S*)	Опасное событие может привести к тяжелым травмам или к фатальному исходу как в локальной зоне, так и вне ее
Значительный (*E*)	Опасное событие, в пять или более раз более жесткое, чем серьезное событие

F.5 Вероятность появления исходных причин

Численное значение вероятности появления исходных причин, измеряемое числом событий в год, заносят в графу 4 рисунка F.1. Типичные значения вероятности появления таких причин приведены в таблице F.3. Для определения вероятности исходной причины очень важен опыт упоминавшейся группы специалистов.

Значения в таблице F.3 не должны использоваться для конкретных оценок (см. примечание 1).

Таблица F.3 — Вероятность появления исходных причин

Низкая	Отказ или серия отказов с очень низкой вероятностью появления в течение ожидаемого времени жизни объекта, например: - три или более одновременных отказов приборов или ошибок оператора; - самопроизвольный отказ отдельного резервуара или иного оборудования процесса	$f < 10^{-4}$ *в год*

Окончание таблицы F.3

Средняя	Отказ или серия отказов с низкой вероятностью появления в течение ожидаемого времени жизни объекта, например: - отказы резервированного прибора или клапана; - комбинация отказов приборов и ошибок оператора; - одиночные отказы небольшой технологической линии или фитинга	$10^{-4} < f < 10^{-2}$ в год
Высокая	Отказы, которых следует ожидать в течение времени жизни объекта, например: - утечки в процессе; - одиночные отказы прибора или клапана; - ошибки человека, способные привести к выбросам материала	$10^{-2} < f < 100$ в год
Примечания 1 Данная таблица представлена в качестве иллюстрации. Указанные частоты не могут быть взяты в качестве универсальных частот и не могут использоваться в конкретных оценках. 2 *f* — частота инициирующего события (вероятность инициирующего события).		

F.6 Слои защиты

На рисунке 2 показано несколько слоев защиты, которые обычно применяют для промышленных процессов. Каждый слой защиты представляет собой совокупность технических средств и/или административных мер, которые функционируют совместно с другими слоями защиты. Слои защиты, которые выполняют свои функции с высокой степенью надежности, могут считаться независимыми слоями защиты (НСЗ) (см. F.8).

Проектные решения, направленные на уменьшение вероятности появления исходных событий, приведены в колонке 5 на рисунке F.1. Примером может служить использование защитной рубашки для трубопровода или емкости. Такая рубашка должна предотвращать выброс материала в случае нарушения целостности основного трубопровода или емкости.

В следующей графе колонки 5 на рисунке F.1 приведена информация, связанная с ОСУП. Если контур управления, реализуемый ОСУП, предотвращает появление опасного события при возникновении исходных причин, то его влияние характеризуют заявленным для него значением PFD (средней частоты отказов при наличии запроса).

В последней графе колонки 5 на рисунке F.1 указывается влияние аварийной сигнализации, которая привлекает внимание оператора и стимулирует его вмешательство в процесс. Характерные величины ВОНЗ для слоев защиты приведены в таблице F.4.

Значения в таблице F.4 не должны использоваться для конкретных оценок (см. примечание).

Таблица F.4 — Типичные значения ВОНЗ слоев защиты (предотвращение и ослабление)

Слой защиты	ВОНЗ
Контур управления	$1{,}0 \cdot 10^{-1}$
Работа оператора (опытного и в отсутствие стресса)	$1{,}0 \cdot 10^{-1}$ до $1{,}0 \cdot 10^{-2}$
Работа оператора в условиях стресса	0,5 до 1,0
Реакция оператора на аварийную сигнализацию	$1{,}0 \cdot 10^{-1}$
Давление внутри сосуда, вызываемое внутренними и внешними причинами, превышает максимально возможное	10^{-4} или меньше, если сохраняется целостность емкости (т. е. коррозия под контролем, инспекцию и обслуживание проводят согласно расписанию)

Примечание — Числа в таблице F.4 представлены в качестве иллюстрации из диапазона значений, которые могут появиться при оценках. Указанные значения не могут быть взяты в качестве универсальных частот и не могут использоваться в конкретных оценках. Вероятности ошибок человека могут быть соответственно оценены на индивидуальной основе.

F.7 Дополнительное ослабление

Ослабляющие слои относят к одной из трех категорий — механические, структурные и процедурные. Примерами могут служить:

- устройства сброса давления;
- ограждения;
- ограниченный доступ.

Ослабляющие слои могут уменьшить тяжесть нежелательного события, но не предотвращают его появления. Примерами могут служить:

- система пожаротушения при появлении огня или дыма;
- пожарная сигнализация;
- меры по эвакуации персонала.

Группа специалистов, занимающаяся АСЗ, должна определить соответствующие ВОНЗ для всех ослабляющих слоев защиты и перечислить их в графе 6 на рисунке F.1.

F.8 Независимые слои защиты

Слои защиты, удовлетворяющие критериям для независимых слоев защиты (НСЗ), заносят в графу 7 на рисунке F.1.

Для того чтобы слой защиты считался независимым, он должен удовлетворять следующим критериям:

- защита должна обеспечивать значительное (минимум в десять раз) снижение определенного риска;
- функция защиты должна выполняться с высокой степенью готовности (0,9 и более);
- слой защиты должен обладать следующими важными характеристиками:

a) специфика — НСЗ проектируется специально для того, чтобы предотвратить или ослабить последствия одного потенциально опасного события (например, неуправляемая реакция, выброс токсичного материала, разгерметизация аппарата, пожар). Причин возникновения этой опасной ситуации может быть много, и, следовательно, действие НСЗ может происходить по многим сценариям, вызванным многочисленными исходными событиями;

b) независимость — НСЗ не зависит от других слоев защиты, связанных с той же выявленной опасностью;

c) гарантия надёжности — можно рассчитывать, что НСЗ будет выполнять предназначенные для него функции. При его проектировании учитывают как случайные, так и систематические отказы;

d) проверяемость — НСЗ должен облегчать проведение регулярного подтверждения соответствия функций защиты. При этом необходимы проверочные испытания и обслуживание системы безопасности.

Только такие слои защиты, которые пройдут испытания на соответствие требованиям эксплуатационной готовности, специфики, независимости, гарантии надежности и проверяемости, могут быть классифицированы как независимые.

F.9 Вероятность промежуточного события

Вероятность промежуточного события подсчитывают умножением вероятности появления исходной причины (графа 4 на рисунке F.1) на значение ВОНЗ для слоев защиты и ослабления (графы 5, 6 и 7 на рисунке F.1). Найденное значение имеет размерность числа событий в год, и его заносят в графу 8 на рисунке F.1.

Если вероятность промежуточного события меньше, чем корпоративный критерий для событий этого уровня тяжести, то дополнительные слои защиты не требуются. Дальнейшее снижение риска следует проводить с учетом экономической целесообразности.

Если вероятность промежуточного события больше, чем корпоративный критерий для событий этого уровня тяжести, то требуется дальнейшее снижение риска. Перед тем как решить вопрос о введении дополнительного слоя защиты в виде ПСБ, следует рассмотреть возможность использования методов и решений, обеспечивающих большую безопасность. Прежде чем применять дополнительные слои защиты на основе ПСБ, необходимо рассмотреть методы и решения, безопасные в своей основе. При этом данные на рисунке F.1 обновляют, производят перерасчет вероятности промежуточного события и сравнение найденного значения с корпоративным критерием.

Если величину вероятности промежуточного события не удается сделать меньшей, чем корпоративный критерий, то требуется применить ПСБ.

F.10 Уровень полноты функции безопасности ПСБ

Если оказывается необходимым ввести новую функцию безопасности ПСБ, то следует подсчитать требуемый уровень ее полноты. Для этого величину корпоративного критерия для заданного уровня тяжести события необходимо разделить на величину вероятности промежуточного события. Значение ВОНЗ для функции безопасности ПСБ, лежащее ниже найденного в результате деления значения, принимают как максимальное для ПСБ и заносят в графу 9 на рисунке F.1.

F.11 Вероятность ослабления влияющего события

Далее подсчитывают значение вероятности ослабления влияющего события. Для этого значения граф 8 и 9 на рисунке F.1 перемножают, и результат заносят в графу 10 на рисунке F.1. Эту процедуру продолжают до тех пор, пока группа специалистов не рассчитает вероятности ослабления событий для всех обнаруженных влияющих событий.

F.12 Полный риск

В качестве заключительного шага следует сложить вероятности ослабления влияющих событий для всех событий с серьезными и высокими уровнями тяжести, вызывающие одну и ту же опасность. Например, вероятности ослабления влияющих событий для всех событий с серьезными и высокими уровнями тяжести, вызывающих пожар, сложить и использовать в формуле вида:

риск фатального исхода при пожаре = (общая вероятность ослабления влияющих событий, связанных с выбросом воспламеняющегося материала) × (вероятность возгорания) × (вероятность пребывания людей в опасной зоне) × (вероятность фатального исхода при пожаре).

Далее следует сложить вероятности ослабления влияющих событий для всех событий с серьезными и высокими уровнями тяжести, связанных с выбросом токсичных материалов, и использовать в аналогичной формуле:

риск фатального исхода при выбросе токсичных материалов = (общая вероятность ослабления влияющих событий, связанных с токсичными выбросами) × (вероятность пребывания людей в опасной зоне) × (вероятность фатального исхода вследствие токсичного выброса).

Экспертная оценка специалиста по анализу рисков и знания группы специалистов играют важную роль в уточнении и адаптации перечисленных выше показателей в формулах к условиям и практике работы объекта, а также к обществу, подвергаемому опасности.

Теперь можно определить полный риск для корпорации, связанный с данным процессом. Для этого следует объединить результаты, полученные расчетным путем по приведенным выше формулам.

Если полученное значение соответствует корпоративному критерию для персонала, подвергающегося опасности, или меньше его, то АСЗ можно считать завершенным. Однако поскольку персонал может подвергаться риску также со стороны других установок и проектов, то представляется разумным провести дальнейшее ослабление и снижение риска, если это окажется экономически оправданным.

F.13 Пример

F.13.1 Общие положения

Ниже приведен пример применения методологии АСЗ по отношению к опасному событию, выявленному методом HAZOP.

F.13.2 Влияющее событие и уровень его тяжести

Пусть с помощью метода HAZOP выявлено, что отклонение высокого давления в реакторе полимеризации периодического действия является опасным событием. Реактор из нержавеющей стали соединен последовательно с насадочной колонной из пластмассы, армированной стальной нитью, и конденсатором, выполненным из нержавеющей стали. Трещина в армированной насадочной пластмассовой колонне может привести к выбросу воспламеняющегося газа, что, в свою очередь, может вызвать пожар при наличии источника воспламенения. Группа специалистов, пользуясь таблицей F.2, установила, что событие относится к уровню тяжести *S* (серьезный), поскольку оно может привести к серьезным травмам и даже фатальному исходу в опасной зоне. Влияющее событие и его тяжесть вносят соответственно в графы 1 и 2 на рисунке F.1.

F.13.3 Исходные причины

Методом HAZOP были зафиксированы две исходные причины повышения давления: прекращение подачи охлаждающей воды в конденсатор и отказ контура управления паром в реакторе. Обе эти причины внесены в графу 3 на рисунке F.1.

F.13.4 Возможность исходных событий

Прекращение подачи охлаждающей воды на данном предприятии происходит, как показывает практика, один раз в 15 лет. Группа исследователей в качестве консервативной оценки приняла, что прекращение подачи охлаждающей воды происходит один раз в 10 лет. В графу 4 на рисунке F.1 вносят значение 0,1 событий в год. Представляется разумным проследить до конца влияние этой причины и лишь затем обратиться к другой причине — к отказу контура управления паром в реакторе.

F.13.5 Проектирование слоев защиты

Производственная зона была спроектирована в соответствии с принятой классификацией применения электрического оборудования во взрывозащищенных зонах, и для нее реализован план управления безопасностью. Одним из элементов этого плана является управление процедурой замены электрического оборудования. По оценке группы АСЗ, риск воспламенения снижается в 10 раз благодаря управлению процедурами замены. Следовательно, влияние этого фактора равно 0,1. Это значение вносят в графу «Общий проект процесса» колонки 5 на рисунке F.1.

F.13.6 ОСУП

Высокое давление в реакторе сопровождается высокой температурой. В ОСУП предусмотрен контур управления, который изменяет подачу пара в рубашку реактора в зависимости от температуры в реакторе. Если температура в реакторе превышает заданное значение, то ОСУП прекратит подачу пара в рубашку реактора. Так как прекращение подачи пара способно предотвратить высокое давление, то ОСУП является слоем защиты. ОСУП является очень надежной цифровой системой управления, и оперативный персонал никогда не наблюдал отказа, в результате которого перестал бы работать контур управления температурой. Группа АСЗ принимает решение, что ВОНЗ составляет 0,1, и вносит значение 0,1 в графу «ОСУП» колонки 5 на рисунке F.1 (0,1 — это минимально допустимое значение для ОСУП).

F.13.7 Аварийная сигнализация

Система имеет в своем составе датчик расхода охлаждающей воды в конденсатор. Этот датчик подключен к разным входам ОСУП и контроллера регулирования температуры. При малом потоке охлаждающей воды в конденсатор срабатывает аварийная сигнализация, требующая от оператора вмешаться в ход процесса и перекрыть подачу пара. Аварийная сигнализация может считаться слоем защиты, так как она размещается в другом по отношению

к контуру регулирования температуры контроллере ОСУП. Группа АСЗ принимает решение, что и в этом случае среднюю вероятность отказа при запросе можно принять равной 0,1, так как оператор всегда находится в операторском помещении. В графу «Сигнализация» колонки 5 на рисунке F.1 заносят значение 0,1.

F.13.8 Дополнительное ослабление

Во время работы установки доступ в рабочую зону ограничен. Обслуживание производят только в те периоды, когда оборудование остановлено и отключено. План безопасного ведения процесса требует, чтобы все лица, не относящиеся к оперативному персоналу, отмечались при входе в рабочее помещение и предупреждали о своем приходе оператора. Группа АСЗ полагает, что наличие таких усиленных ограничений доступа приводит к снижению риска для оперативного персонала на порядок. Поэтому в графу 6 «Дополнительное ослабление, ограничение доступа» на рисунке F.1 вводят значение 0,1.

F.13.9 Независимый(е) слой(и) защиты (НСЗ)

Реактор оборудован предохранительным клапаном, рассчитанным таким образом, чтобы пропустить весь объем газа, образовавшегося за период повышения температуры и давления, вызванного отсутствием охлаждающей воды. Далее с учетом запасов и состава материала был оценен вклад предохранительного клапана в снижение риска. Поскольку предохранительный клапан настроен на давление ниже расчетного давления фиберглассовой колонны и ошибка оператора, в результате которой колонна во время работы была бы изолирована от предохранительного клапана, невозможна, то предохранительный клапан рассматривается как слой защиты. Сам предохранительный клапан демонтируют и испытывают каждый год, и ни разу за 15 лет работы не наблюдалось забивания клапана или смежных труб. Так как предохранительный клапан соответствует критерию НСЗ, то на основании рассмотренного выше опыта работы и опубликованных промышленных данных значение ВОНЗ принято равным 0,01 и соответствующее значение занесено в графу 7 на рисунке F.1.

F.13.10 Вероятность промежуточного события

Числа, занесенные в первую строку всех граф, перемножают, и результат заносят в графу 8 «Вероятность промежуточного события» на рисунке F.1. Произведение этих величин в настоящем примере составляет 10^{-7}.

F.13.11 ПСБ

Ослабление и снижение риска, полученные благодаря слоям защиты, оказываются достаточными, чтобы удовлетворить корпоративному критерию. Можно, однако, получить дальнейшее ослабление, причем при минимальных затратах, поскольку в системе предусмотрены датчик давления в сосуде, а также соответствующая сигнализация в ОСУП. Группа АСЗ принимает решение ввести дополнительную функцию безопасности ПСБ, которая состоит из выключателя и реле, прекращающих подачу питания на соленоидный клапан, связанный с клапаном на линии подачи пара в рубашку реактора. Эта функция безопасности ПСБ разрабатывается для наиболее низкого значения диапазона УПБ 1, и ее ВОНЗ равна 0,01. Значение 0,01 вносят в графу 9 «УПБ функции безопасности ПСБ» на рисунке F.1.

Затем рассчитывают вероятности ослабления влияющего события. Этого достигают путем перемножения чисел в графах 8 и 9. Результат, равный $1 \cdot 10^{-9}$, заносят в графу 10 на рисунке F.1.

F.13.12 Следующая функция безопасности ПСБ

Затем группа АСЗ рассматривает вторую исходную причину (отказ контура управления расходом пара в реакторе). Вероятность отказа управляющего клапана определяют по таблице F.3, и в графу 4 «Вероятность исходной причины» на рисунке F.1 вносят число 0,1.

Слои защиты, предусмотренные при проектировании процесса, аварийная сигнализация, дополнительное ослабление и ПСБ — все это также служит защитой при отказе контура управления паром. Единственный отсутствующий слой защиты — это ОСУП. Группа АСЗ рассчитывает промежуточную вероятность ($1 \cdot 10^{-6}$) и вероятность ослабления влияющего события ($1 \cdot 10^{-8}$). Эти величины вносят соответственно в графы 8 и 10 на рисунке F.1.

Группа АСЗ будет продолжать анализ до тех пор, пока не будут рассмотрены все отклонения, обнаруженные методом HAZOP.

Заключительный шаг — сложение вероятностей ослабления влияющих событий для событий с серьезными и высокими уровнями тяжести, которые вызывают ту же опасность.

В настоящем примере, если бы для всего процесса было выявлено только одно влияющее событие, эта величина была бы равной $1{,}1 \cdot 10^{-8}$. Так как вероятность воспламенения была рассчитана по данным проекта (0,1), а вероятность пребывания людей в опасной зоне с учетом дополнительного ослабления составляет (0,1), то уравнение для риска фатального исхода, вызванного пожаром, сводится к следующему:

риск фатального исхода от пожара = (общая вероятность ослабления влияющих событий, связанных с выбросом воспламеняющегося материала) × (вероятность получения фатальной травмы при пожаре = 0,5)

или риск фатального исхода от пожара = $(1{,}1 \cdot 10^{-8}) \cdot (0{,}5) = 5{,}5 \cdot 10^{-9}$.

Это число ниже корпоративного критерия для данной опасности, и дальнейшее снижение риска не является экономически оправданным. Таким образом, работу группы АСЗ можно считать завершенной.

Приложение G
(справочное)

Анализ слоев защиты, используя матрицу риска

G.1 Общие положения

Приложение G описывает метод оценки опасностей и рисков, который использует анализ слоев защиты (АСЗ), чтобы определить функции безопасности, которые уменьшают частоту событий, связанных с нарушением целостности первичной защитной оболочки (LOPC), до допустимого уровня. Данный метод способствует применению предварительных мер защиты, которые предотвращают LOPC, но он позволяет по мере необходимости рассматривать системы смягчения последствий. Если системы смягчения последствий реализованы, то данный метод требует более точной оценки результата, полученного от развертывания системы смягчения. Так как данный метод не определяет частоту ущерба, связанного с LOPC, то он не рассматривает условия событий после выброса, такие как вероятность воспламенения или нахождения в опасной зоне. Это упрощает метод и нацеливает команду оценки на сокращение событий LOPC посредством учета безопасности в проектных решениях, а также предварительных слоев защиты.

Данный метод использует матрицу риска, чтобы сформировать критерии риска для команды оценки. Матрица риска калибруется, чтобы учесть серьезность последствия, возможного в результате события LOPC. Критерии связаны с безопасностью, экологией и потерей экономического потенциала.

Данный метод исследует опасные события, определенные с помощью любого метода идентификации опасности, подходящего для определенной стадии жизненного цикла процесса. Как минимум, в результате идентификации опасности должны быть описаны опасные события, для которых была выполнена их оценка, и должна быть определена исходная причина (причины) и мера (меры) защиты, которая(ые) предотвращает(ют) или смягчает(ют) это событие (события).

Оценка риска выполняется, используя АСЗ, где определяется риск процесса и выполняется его сравнение с допустимым риском, как определено полуколичественной матрицей риска. Если риск процесса выше допустимого, то определяются функции безопасности и распределяются по независимым слоям защиты (НСЗ), как показано на рисунке G.1 (адаптирован из CCPS, 2007). Некоторые НСЗ являются предотвращающими и направлены на предотвращение опасного события. Другие НСЗ являются ослабляющими и направлены на снижение ущерба, вызванного опасным событием.



Рисунок G.1 — Графическое представление слоев защиты, показывающее предотвращающие и ослабляющие НСЗ

Данный метод поддерживает выбор предотвращающих НСЗ, которые снижают частоту опасного события (например, нарушение целостности первичной защитной оболочки или повреждение оборудования). Использование любого слоя защиты требует дополнительного рассмотрения вторичного последствия, которое следует в результате его успешной работы. Это особенно важно для смягчающих НСЗ (см. шаг 7 ниже).

После завершения исследования сформированным функциям безопасности распределяются значения снижения риска в соответствии с рекомендациями, которые установлены для каждого типа НСЗ и связанной с ним функции. Если снижение риска определено для ПСБ, то это снижение риска приводит к значению УПБ в соответствии с МЭК 61511-1, таблица 4.

Данный метод не рассматривает продолжительность режимов работы при выполнении анализа риска (последовательный, пакетный, пуско-наладочный режимы или режим обслуживания). В данном методе риск каждого рабочего режима должен быть снижен до допустимой частоты независимо от количества времени выполнения процесса в конкретном рабочем режиме.

Допустимая частота опасного события определяется оценкой последствия наихудшего вероятного сценария с точки зрения влияния на здоровье и безопасность персонала объекта и гражданского населения, воздействия на окружающую среду и влияния на экономику (собственность и снижение деловой активности). Предполагается, что команда качественно оценит наихудшее возможное последствие независимо от его вероятности и определит НСЗ, чтобы снизить риск события. Необходимо еще раз подчеркнуть, что данный метод стремится уменьшить частоту опасного события (например, нарушения целостности первичной защитной оболочки или повреждения оборудования), поэтому данный метод не рассматривает использование условных модификаторов для нахождения в опасной зоне, воспламенения или смертельного случая, которые, как правило, используются, чтобы оценить частоту конкретных видов ущерба, нанесенного событием.

Примечания

1 Данный метод эффективно использует наличие команды и информации для оценки воздействия на экономику событий нарушения целостности первичной защитной оболочки. Реализация любых рекомендаций для связанных с экономикой событий определена процессами, одобренными бизнесом.

2 Используемые значения частот, вероятностей и снижения риска представлены только в качестве иллюстрации и не могут быть взяты в качестве универсальных значений для конкретных оценок.

Приложение G не является полным изложением метода, но оно иллюстрирует его общие принципы и основано на более подробном описании данного метода в следующих ссылках:

Layer of Protection Analysis-Simplified — Process risk assessment, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2001, ISBN 0-8169-0811-7

Guidance on the Application of Code Case 2211 — Overpressure Protection by System Design, Welding Research Council, PO Box 1942, New York, NY 10156, 2005, ISBN 1-58145-505-4

Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries — Pressure relieving and depressuring system, American Petroleum Institute, 1220 L Street, NW, Washington, D.C. 20005, 2007

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2007, ISBN 0-4719-7940-6

Guidelines for Initiating Events and Independent Protection Layers in LOPA, American Institute of Chemical Engineers, CCPS, 3 Park Avenue, New York, NY 10016-5991, 2015, ISBN: 978-0-470-34385-2.

G.2 Процедура

G.2.1 Общие положения

К идентификации НСЗ приводит такая процедура АСЗ, которая может снизить риск процесса в соответствии с критериями риска. Ниже представлено пошаговое описание процесса работы, который продемонстрирован на рисунке G.2.

G.2.2 Шаг 1. Общая информация и определение узла

Члены команды, дата начала работы, дата исследования и номер регистрации документа записаны в рабочей таблице. Координатор анализирует границу узла, чтобы гарантировать, что каждый член команды знаком с технологическим процессом и его схемой (см. рисунок G.3). Рассматриваемые технологические схемы и схемы Т и КИП (P&ID) должны быть представлены наряду с любой другой документацией, которая рассматривается командой во время исследования.

G.2.3 Шаг 2. Описание опасного события

Отклонение, или «что если», или FMEA. Команда должна описать каждое опасное событие, выбранное при анализе, включающем отклонение, вопрос «что если» или вид отказа, который использовался в процессе идентификации опасности, и рассмотреть, как оно развивается до нарушения целостности первичной защитной оболочки или повреждения оборудования.

В таблице G.1 представлен фрагмент результата анализа методом HAZOP, выполненного для узла, представленного на рисунке G.3. Это один из многих возможных сценариев, которые приводят к избыточному давлению в этом технологическом блоке. Этот сценарий был выбран в целях иллюстрации.

Описание опасного события. Распространение событий должно быть описано ясно, и все же кратко, начиная от возникновения опасности процесса и до наихудшего вероятного последствия, предполагая, что меры защиты отсутствуют. Важно полностью описать опасное событие так, чтобы каждый член команды понял то, что анализируется. Необходимо также учесть, что эта документация поможет в управлении процессом изменений и в дальнейших повторных подтверждениях соответствия. Таким образом, важно, чтобы описание было четким и понятным.

В качестве примера в таблице G.2 представлено отклонение давления в сторону повышения, которое вызвано отказом контура управления производством, и давление в результате превысило максимально допустимое рабочее давление (MAWP) в емкости. Устанавливается последствие: «Интенсивный поток приводит к давлению выше 1,5 · MAWP. Возможны повреждение емкости и выброс в окружающую среду в течение 5 мин». (Необходимо отметить, что эти 1,5 · MAWP разрешены только определенными нормами проектирования емкости.) Это описание обеспечивает более поздним командам понимание степени превышения давления и скорости, с которой давление повышается до недопустимого уровня.

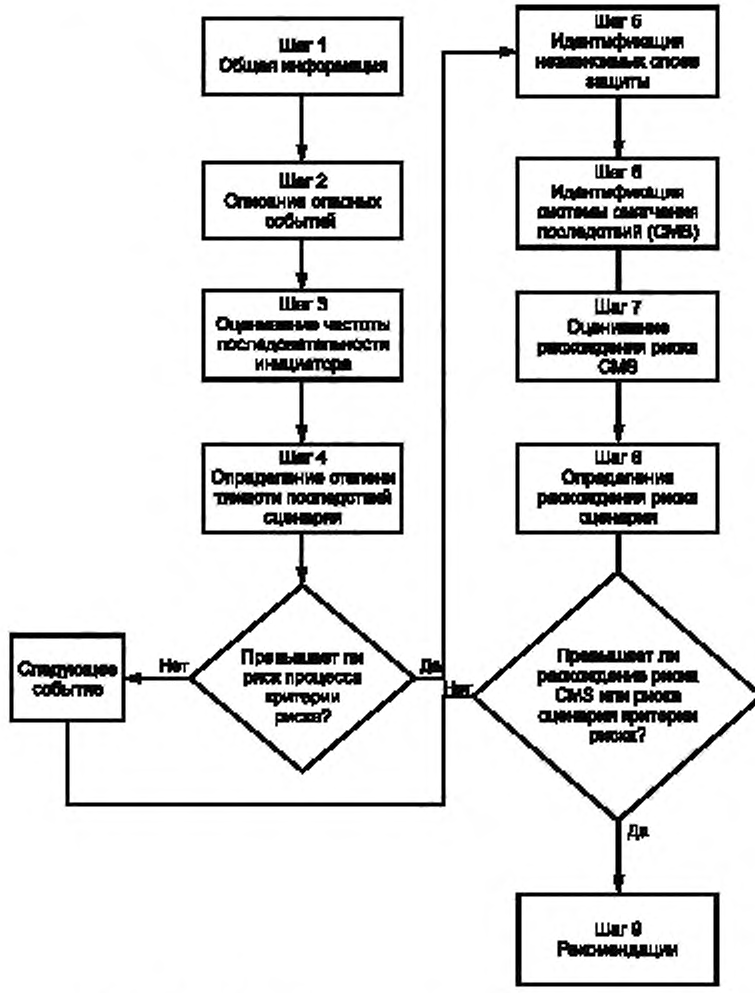


Рисунок G.2 — Рабочий процесс, используемый в приложении G

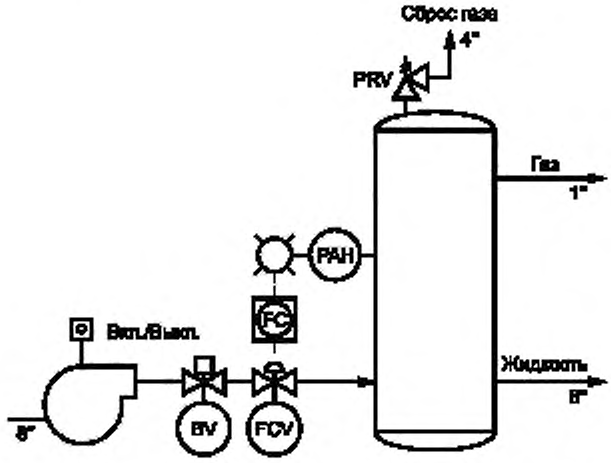


Рисунок G.3 — Пример границы узла процесса для отобранного сценария

Таблица G.1 — Выбранный сценарий из рабочей таблицы HAZOP

Имя системы. 1. Емкость 101 с исходным продуктом.

Чертеж. Чертеж ABC 123.

Цель проекта и метод (методы) управления процессом. Смесь X поступает в емкость 101 для разделения газа и жидкости.

Отклонение	Причина	Последствие	Уровень последствия		Мера защиты	Ранг риска		Рекомендация анализа опасности процесса (АОП)
			Категория	*S*		*L*	*RR*	
1 Высокое давление	1 Сбои контура управления производством	Интенсивный поток приводит к давлению выше 1,5·MAWP. Возможны повреждение емкости и выброс в окружающую среду в течение 5 мин	*S*	4	1 Аварийный сигнал высокого давления	B	2	
			E	4		B	2	
			A	3	2 Закрытие входного блокирующего клапана высокого давления	B	1	
					3 Регулятор давления			
					4 Реакция оператора на аварийный сигнал высокого давления			

Примечание — Для ранжирования категорий и уровня тяжести (*S*) последствия см. таблицу G.4.

G.2.4 Шаг 3. Оценка частоты исходного события

Как только опасное событие описано, документально оформляется исходная причина (причины), которая приводит(ят) к опасному событию. Событие может быть инициировано единственной исходной причиной или несколькими причинами. Команда должна рассмотреть различные типы причин, такие как ошибка человека, отказы оборудования, ошибки процедур и т. д.

Могут быть случаи, когда команде кажется, что нет никакой вероятной причины или комбинации причин. Это может произойти при проектировании процесса с учетом безопасности или потому, что, по мнению команды, возникновение подобного сценария противоречило бы законам химии или физики. В этих случаях в рабочей таблице в графе «Исходная причина» записывается «Нет никакой вероятной исходной причины» вместе с изложением этого рассуждения, и команда должна перейти к рассмотрению следующего сценария.

Частота. Частота исходного события оценивается без учета какого-либо НСЗ (мер защиты). Указания, представленные в таблице G.3, основаны на опубликованных данных промышленности и эффективной инженерной практике. Команда должна определить, основаны ли данные на динамике эксплуатационных показателей предприятия или на опыте работы с исходными причинами, выявленными на предприятии при подобных условиях. Если команда решает, что необходимо использовать более высокую частоту отказов (например, 1/год, а не 1/10 лет), то обоснование этого решения оформляется документально, и в рабочую таблицу вносится новое значение частоты. В данном примере частота отказов контура управления производством равна 1/10 лет.

Обеспечивающие условия. Некоторые отклонения процесса могут привести к опасным событиям только в присутствии совпадающего условия, названного обеспечивающим условием. Данная процедура позволяет рассмотрение обеспечивающего условия, когда это условие не зависит от исходной причины и необходимо для распространения опасного события. Комбинация обеспечивающего условия и исходной причины приводит к распространению опасного события.

Частота исходного события может быть оценена на основе средней вероятности рассматриваемого обеспечивающего условия и частоты исходной причины. Например, если оператор по ошибке оставляет клапан открытым и происходит нарушение на последующих стадиях технологического процесса, то может возникнуть обратный поток через открытый клапан. Нарушение процесса, как предполагается, происходит с частотой 1/год. Оператор открывает и закрывает клапан 3 раза в день. Предполагается, что возможность его отказа равна 1/100. Положение клапана проверяется каждые 8 ч (следующей сменой операторов). Таким образом, средняя вероятность того, что клапан открыт равна:

$$P\ (\text{открыт}) = (3/24\ \text{ч}) \cdot (1/100) \cdot 8\ \text{ч} = 0{,}01.$$

Частота исходного события равна 0,01 · 1/год = 1/100 лет.

Общая частота. Общая частота события — это самая высокая частота перечисленных исходных причин. Если у опасного события есть более трех исходных причин близкой частоты, то при определении наибольшего значения общей частоты события должно быть уделено внимание анализу аспектов возможной общей причины для всех исходных причин. В примере (таблица G.2) рассматривается только одна причина, таким образом, частота исходного события — 1/10 лет.

Таблица G.2 — Выбранный сценарий из рабочей таблицы АСЗ

Имя системы. 1. Емкость 101 с исходным продуктом.
Чертеж. Чертеж АВС 123.
Цель проекта и метод (методы) управления процессом. Смесь X поступает в емкость 101 для разделения газа и жидкости.

Отклонение	Оценка уровня тяжести последствия *S* и величины снижения риска *RRF*				Оценка частоты исходного события				Определение НСЗ и *RRF*			
	Последствие	Категория	*S*	Требуемая *RRF*	Исходная причина	Тип	Частота	Общая частота	Мера защиты (не НСЗ)	НСЗ	Тип	*RRF*
1 Высокое давление	Интенсивный поток приводит к давлению выше 1,5 · MAWP. Возможны повреждение емкости и выброс в окружающую среду в течение 5 мин	*S*	4	1000	1 Сбои контура управления производством	ОСУП	10	10	1 Недостаточно времени для реакции оператора на аварийный сигнал высокого давления	1 Закрытие входного блокирующего клапана высокого давления	ПСБ	10
		E	4	1000								
		A	3	100								

Примечание — Для ранжирования категорий и уровня тяжести (*S*) последствия см. таблицу G.4.

Таблица G.2 — Продолжение на шаге 6

Определение системы ослабления последствия *CMS* и *RRF*			Определение расхождения риска *CMS*					Определение расхождения риска сценария			Рекомендация (АСЗ)	
CMS	Последствие *CMS*	*RRF*	Категория	*S*	Требуемая *RRF* для *CMS*	Общая *RRF* НСЗ	Расхождение *RRF* для *CMS*	Требуемая *RRF*	Общая *RRF* (НСЗ + *CMS*)	Расхождение *RRF* сценария	Рекомендация	Целевое значение *RRF*
Клапан сброса давления	1 На факел не отводится	100	*S*	*	ПР	10	ПР	1000	1000	ПР		
			E	*	ПР		ПР	1000		ПР		
			A	*	ПР		ПР	100		ПР		

Таблица G.3 — Пример исходных причин и соответствующей частоты

Исходная причина	Следствие	*MTBF*[a] (*t*)
БСУП	Полный контур управления, включая датчик, контроллер и исполнительный элемент	10
Действие оператора (типовая инструкция)	Действие выполняется в соответствии с процедурой ежедневно или еженедельно. Оператор обучен необходимым действиям. [Это значение на основе опыта может быть уменьшено в 10 раз (одно событие за 10 лет). Команда должна документально оформить инструкции по выполнению действия, процедуры и/или применяемое обучение, обеспечивающее достижение одного события за 10 лет]	1
	Действие выполняется в соответствии с процедурой ежемесячно или ежеквартально. Оператор обучен необходимым действиям	10
	Действие выполняется в соответствии с процедурой ежегодно после цикла работы или временного отключения. Оператор обучен необходимым действиям	100
Приборные устройства безопасности (ДРУГИЕ)	Инструментованное устройство безопасности срабатывает самопроизвольно, например закрывает блокирующий клапан, отключает насос и открывает выпускной клапан	10

[a] Можно предположить, что перечисленные исходные причины происходят более часто (например, не 1/100 лет, а 1/10 лет) на основании опыта реализации процесса. Но эти значения не могут быть приняты менее частыми без дополнительного обоснования и одобрения безопасности процесса. В качестве обоснования должен быть проведен дополнительный анализ. Он должен включать анализ человеческого фактора, анализ видов и последствий отказов (*FMEA*), анализ дерева событий или анализ дерева отказов.

G.2.5 Шаг 4. Определение уровня тяжести последствия опасного события и величины снижения риска

Опасное событие оценивается, чтобы определить наихудшее возможное последствие с точки зрения влияния на здоровье и безопасность персонала объекта и гражданского населения, воздействия на окружающую среду и влияния на экономику (собственность и снижение деловой активности).

Уровень тяжести. Уровень тяжести последствия оценивается согласно стандартизированным определениям в таблице G.4. Для данного примера (см. таблицу G.2) команда решила, что существовала возможность значительного выброса воспламеняющегося углеводорода. Так как оператор часто находился около установки, то был возможен смертельный случай. Уровень тяжести последствия для обеспечения безопасности был оценен значением «4». В результате ранжирования уровень тяжести последствия для экологии также был определен равный «4», в то время как ранжирование уровня тяжести последствия для имущества дало значение «3».

Оценка риска. Риск процесса определяется общей частотой исходного события (шаг 3) и уровнем тяжести последствия (шаг 4). Их ранжированные значения используются в качестве входных данных для таблицы G.5. Данная матрица показывает величину снижения риска (*RRF*), требуемую для снижения риска процесса до уровня приемлемого риска (ПР). Если *RRF* приводит в результате к значению приемлемого риска, то риск процесса удовлетворяет критериям риска без дополнительных НСЗ. Те опасные события, которые не указаны для приемлемого риска, далее должны быть оценены.

В данном примере (см. таблицу G.2) уровень тяжести последствия, равный 4, и частота опасного события, равная 1/10 лет, дает в результате требуемое снижение риска, равное 1000 (см. таблицу G.5).

В некоторых случаях НСЗ могут не потребоваться с точки зрения риска, но они могут быть определены стандартом, практикой или регламентом. Требования стандартов, практики или регламентов превалируют над этой процедурой.

Таблица G.4 — Таблица решений для уровня тяжести последствия

Значение	Безопасность *S*	Окружающая среда *E*	Имущество *A*
5	Множественные смертельные случаи по всей установке и/или травмы или смертельные случаи среди гражданского населения	Катастрофический вред окружающей среде на обширной территории с длительными сдерживанием распространения и очисткой	Ожидаемая потеря больше чем 10 000 000 долларов и/или существенный ущерб зданиям, расположенным на обширной территории

Окончание таблицы G.4

Значение	Безопасность *S*	Окружающая среда *E*	Имущество *A*
4	Госпитализация трех или больше работников (например, серьезные ожоги, переломы) и/или один или несколько смертельных случаев в пределах установки или ее окрестностей и/или травмы среди гражданского населения	Значительный вред окружающей среде на обширной территории (например, существенный вред дикой природе) с длительными сдерживанием распространения и очисткой	Ожидаемая потеря между 1 000 000 и 10 000 000 долларов и/или длительное время простоя с серьезным влиянием на работоспособность установки и/или незначительное повреждение (например, разбитые окна) в зданиях, расположенных на обширной территории
3	Травмы с необходимостью госпитализации (например, серьезные ожоги, переломы) и/или многократные случаи травм с потерей работоспособности и/или травм среди гражданского населения	Локальный выброс, требующий сдерживания распространения и очистки и/или выброс на обширной территории, наносящий ущерб окружающей среде с быстрой очисткой	Ожидаемая потеря между 100 000 и 1 000 000 долларов и/или время простоя нескольких дней, серьезно влияющее на работоспособность установки
2	Потеря работоспособности и/или регистрируемые травмы (например, кожная сыпь, воспаления, ожоги) и/или незначительное влияние на гражданское население	Локальный выброс, требующий сдерживания распространения и очистки и/или выброс на обширной территории (например, аромат), но не наносящий вред окружающей среде	Ожидаемая потеря между 10 000 и 100 000 долларов и/или время простоя более суток, вызывающее воздействие на работу объекта и/или отчетное количество событий
1	Регистрируемая травма (телесные повреждения, ушиб, рана) и/или отсутствие влияния на гражданское население	Локальный выброс, требующий сдерживания распространения и очистки местным персоналом	Ожидаемый убыток в размере меньше чем 10 000 долларов и/или время простоя меньше одного дня с незначительным воздействием на работоспособность установки

Таблица G.5 — Матрица величины снижения риска

Требуемая величина снижения риска						
Уровень тяжести последствия	5	100 000	10 000	1000	100	10
	4	10 000	1000	100	10	ПР
	3	1000	100	10	ПР	ПР
	2	100	10	ПР	ПР	ПР
	1	10	ПР	ПР	ПР	ПР
		1	10	100	1000	10 000
		Частота (1 за *x* лет)				

G.2.6 Шаг 5. Определение независимых слоев защиты и величины снижения риска

Во время оценки опасности и риска (АОР) определяются меры защиты, которые формируют некоторые средства защиты от рассматриваемого опасного события. Каждая определенная мера защиты оценивается по критериям НСЗ.

Не все меры защиты, удовлетворяющие критериям проектирования и управления, необходимым, чтобы классифицировать эти меры, как НСЗ. Также важно гарантировать соответствующую независимость выбранных мер защиты так, чтобы возможность появления проблем, связанных с отказами по общей причине, общего вида и систематическими отказами, была незначительной по сравнению с требованием к общему снижению риска.

Таблица G.6 представляет руководство по определению *RRF*, например для функций безопасности, которые могут быть классифицированы как НСЗ. Значение величины снижения риска основано на конкретных критериях проектирования и управления НСЗ, которые кратко описаны в таблице G.6. НСЗ, которому будет назначено одно

из перечисленных в таблице G.6 значений снижения риска, должен удовлетворять всем соответствующим ограничениям, представленным в этой таблице.

Мера защиты, которая не удовлетворяет критериям, может быть при необходимости представлена в рабочей таблице с *RRF* = 1. Если из информации о безопасности процесса следует, что мера защиты соответствует критериям, то ей может быть определено только значение *RRF* > 1.

В данном примере (см. таблицу G.2), команда решила, что у оператора нет достаточного количества времени, чтобы отреагировать на сигнал тревоги. Предыдущий анализ ПСБ показал, что для нее определен УПБ 1, таким образом, команда определила для нее значение *RRF*, равное 10 (см. таблицу G.2).

G.2.7 Шаг 6. Определение систем смягчения последствия и величины снижения риска

Успешное действие любого НСЗ приводит к новому рабочему состоянию или к состоянию отключения. Это новое состояние называется вторичным последствием НСЗ. Риск, связанный с вторичным последствием, должен быть приемлемым, либо должен быть применен дополнительный/альтернативный НСЗ. Так как успешное действие большинства смягчающих предотвращающих НСЗ и ослабляющих НСЗ приводит к сокращению уровня тяжести последствия, то все эти НСЗ называют системами смягчения последствия (*CMS*).

CMS, реализованную на НСЗ (*CMS* НСЗ) и снижающую вред опасного события, можно считать таковой, если анализ подтвердит (см. примечание 1), что *CMS* НСЗ разработана и справляется с обработкой конкретного опасного события, а также он определит (см. примечание 2), что *CMS* НСЗ приемлемо управляет риском вторичного последствия.

Примечания

1 Если отсутствуют какие-либо документы, подтверждающие заявление о том, что *CMS* НСЗ должным образом разработана, смонтирована и обслуживается с целью уменьшения последствия конкретного сценария выброса, то для *RRF* не может быть использовано никакое значение.

2 Успешное действие *CMS* НСЗ снижает последствие рассматриваемого опасного события. Снижение последствия в результате надлежащего функционирования *CMS* НСЗ может все еще оказаться недостаточным. Риск, связанный с действием НСЗ, определяется с помощью оценки уровня тяжести этого вторичного последствия и частоты выброса. Эта величина сравнивается с критериями риска, чтобы определить, требуется ли дополнительное снижение риска.

В таблице G.7 перечислены *CMS*, рассмотренные во время исследования, а также значения *RRF* для конкретных функций безопасности, которые могут быть классифицированы как НСЗ. Для команды важно рассмотреть *CMS*, чтобы проверить, что *CMS* разрабатываются и ориентируются на определенный сценарий опасности. В данном методе рассматриваются только *CMS*, которые предварительно снижают частоту основного последствия события (LOPC).

В данном примере (см. таблицу G.2) команда решила, что регулятор давления был разработан для избыточного давления, вызванного отказом контура управления производством. Команда определила для него значение *RRF*, равное 100.

Таблица G.6 — Примеры независимых слоев защиты (НСЗ) с соответствующими величинами снижения риска *RRF* и вероятностями отказа по запросу (ВОНЗ)

НСЗ	Условие	*RRF*	ВОНЗ
Основная система управления процессом (ОСУП)	НСЗ ОСУП должен быть разработан и ориентирован на обеспечение достижения *RRF*. Это, как правило, контур управления, нормальное действие которого предотвратить опасный сценарий. НСЗ ОСУП должен работать в автоматическом режиме на всех стадиях эксплуатации, где может произойти опасный сценарий	10	0,1
Реакция оператора на аварийную сигнализацию со временем отклика ≥ 10 мин (АВАРИЯ)	Оператор не должен выполнять поиск неисправностей или диагностику для принятия конкретных действий. Аварийная сигнализация может быть реализована в ОСУП или независимо от ОСУП	10	0,1
Реакция оператора на аварийную сигнализацию со временем отклика ≥ 40 мин (АВАРИЯ)	От оператора требуются незначительные усилия по поиску неисправностей или диагностике до принятия мер. Аварийная сигнализация может быть реализована в ОСУП или независимо от ОСУП	10	0,1
УПБ 1 (ПСБ)	Уровень полноты безопасности 1	10	0,1
УПБ 2 (ПСБ)	Уровень полноты безопасности 2	100	0,01
УПБ 3 (ПСБ)	Уровень полноты безопасности 3	1000	0,001

Таблица G.7 — Примеры системы ослабления последствий (*CMS*) с соответствующими величинами снижения риска *RRF* и вероятностями отказа по запросу (ВОНЗ)

CMS	Условие	*RRF*	ВОНЗ
Регулятор давления	Обслуживается чисткой. Разработан для опасного события	100	0,01
Мембранное предохранительное устройство сосуда	Разработан для опасного события	100	0,01
Клапан для регулировки вакуума	Разработан для опасного события	100	0,01
Линия перелива	Линия перелива разработана для сброса в зону локализации, которая выполнена по размерам, учитывающим возможность этого опасного события. Любыми клапанами в линии необходимо управлять административно, чтобы при необходимости гарантировать доступность *CMS*	100	0,01

G.2.8 Шаг 7. Определение расхождения риска *CMS*

Для любого НСЗ существуют два возможных состояния, когда к нему выполняется запрос процесса: 1) случай успеха, когда *CMS* работает должным образом в соответствии с проектом, и 2) случай отказа, когда *CMS* не работает в соответствии с проектом. На шаге 7 определение риска *CMS* выполняется с помощью оценки последствия, когда *CMS* работает в соответствии с проектом. На шаге 8 оценка риска выполняется для *CMS*, которая не работает в соответствии с проектом.

Чтобы определить риск *CMS* (т. е. когда она работает должным образом), необходимо сначала оценить уровень тяжести вторичного последствия. Уровень тяжести последствия оценивается согласно стандартизированным определениям в таблице G.4. Риск *CMS* определяется уровнем тяжести последствия *CMS* и частотой использования *CMS*. Эта частота определяется умножением общей частоты исходного события (шаг 3) на значение *RRF* каждого НСЗ, который предотвращает исходное событие от места запроса к *CMS*. Эти НСЗ были определены на шаге 5.

Риск *CMS* оценивается с помощью таблицы G.5. Если расхождение риска *CMS* снижено до значения приемлемого риска (ПР), то никакое дальнейшее снижение риска не требуется. Команда при желании может определить функции, которые улучшают снижение риска. Если расхождение риска *CMS* будет равняться 10, 100, 1000 или 10 000, то команда должна соответственно определить больше НСЗ. Если этих средств защиты в проекте не существует, то делаются рекомендации.

В данном примере (см. таблица G.2 и рисунок G.4) команда решила, что регулятор давления для сброса газа находился в подходящем месте и выброс материала не приводит к недопустимому последствию. Когда клапан сброса давления работает в соответствии с проектом, сценарий реализует выброс материала в систему сброса газа, и для него был определен приемлемый уровень риска.

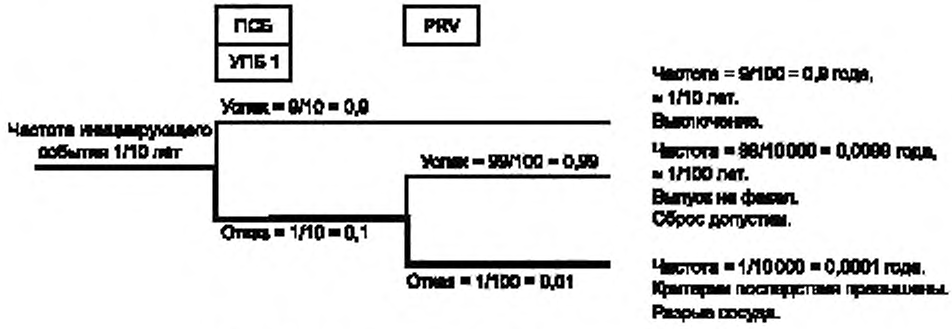


Рисунок G.4 — Приемлемый риск вторичного последствия

После того как исследование было завершено, анализ сброса газа определил, что выброс из регулятора давления мог вызвать перегрузку в системе сброса газа, а также чрезмерное противодавление в системе сброса. На рисунке G.5 обновлено дерево событий, чтобы показать уточненное вторичное последствие — событие сверхдавления с серьезным последствием, которое происходит 1/100 лет.

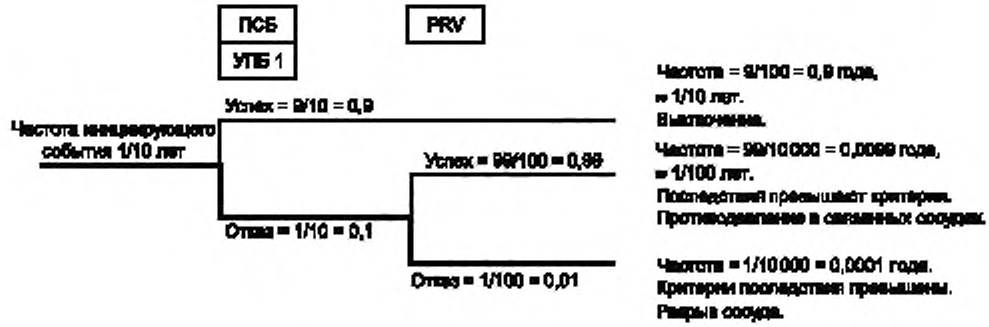


Рисунок G.5 — Неприемлемый риск вторичного последствия

Таблица G.8 представляет собой обновленную таблицу G.2 с пересмотренной оценкой выброса из регулятора давления в систему сброса, показывая последствие, созданное ростом давления в регуляторе давления. Команда решила, что для противодавления, вызванного таким сценарием выброса, было бы возможно вызвать сверхдавление в других устройствах одновременно с событием выброса. Последствие открытия предохранительного клапана рассматривается таким же серьезным, как и в случае его отказа (см. путь распространения отказа предохранительного клапана). В то время как риск, связанный с основным сценарием (разрыв емкости), снижен до уровня приемлемого риска (ПР), риск, связанный со вторичным последствием (перегрузка системы сброса), выше, чем приемлемый риск. Расхождение риска *CMS* составляет *RRF* = 100 для ранжирования безопасности и экологического последствия, в то время как для имущества расхождение риска *CMS* составляет *RRF* = 10.

Расхождение риска *CMS* определяется первоначальной оценкой последствия успешной работы *CMS*, используя таблицу G.4. Затем определяется частота запроса для *CMS* с помощью частоты исходного события сценария (включая обеспечивающие условия), которая уменьшается предотвращающими НСЗ, работающими до запроса к *CMS* (см. деревья событий на рисунках G.4 и G.5). Тогда расхождение риска *CMS* определяется из таблицы G.5.

Применяя это новое требование к снижению риска, было определено, что ПСБ должна быть обновлена до УПБ 3 в соответствии с рекомендациями из API 521 «Guide for Pressure-relieving and Depressuring Systems: Petroleum petrochemical and natural gas industries — Pressure relieving and depressuring system» и ASME «Guidance on the Application of Code Case 2211 — Overpressure Protection by System Design». ПСБ с УПБ 3 снижает частоту запросов к предохранительному клапану и обеспечивает допустимый уровень риска, как показано на рисунках G.5 и G.6.

G.2.9 Шаг 8. Определение расхождения риска сценария

Расхождение риска сценария определяется из его уровня тяжести последствия (шаг 4) и его частоты, учитывая наличие определенных НСЗ (шаг 5) и *CMS* (шаг 6). Каждая частота определяется умножением общей частоты исходного события (шаг 3) на значение *RRF* каждого НСЗ, предотвращающего сценарий, и каждого *CMS*, смягчающего сценарий. НСЗ были определены на шаге 5, а *CMS* были определены на шаге 6.

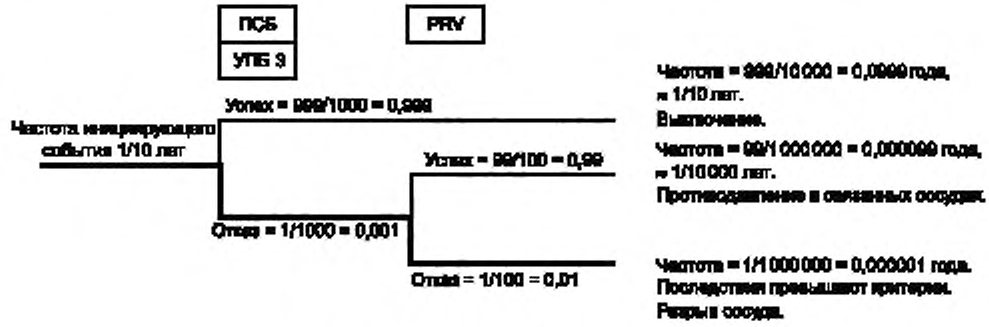


Рисунок G.6 — Управляемый риск вторичного последствия

Риск сценария сравнивается с критериями риска, как показано в таблице G.9, используя таблицу G.5. Если расхождение риска сценария уменьшается до ПР, то дальнейшее снижение риска не требуется. Команда при желании может определить функции, которые увеличивают снижение риска. Если расхождение риска сценария будет равно 10, 100, 1000 или 10 000, то команда должна определить больше НСЗ или *CMS* соответственно. Если в текущем проекте они отсутствуют, то формируются рекомендации.

В данном примере (таблица G.9) для достижения допустимого риска в рассматриваемом сценарии необходимо общее снижение риска, равное 1000. При использовании ПСБ с УПБ 3, обеспечивающей значение *RRF*, равное 1000, и регулятора давления, обеспечивающего значение *RRF*, равное 100, для сценария превышения давления в емкости общее снижение риска, обеспеченное проектом НСЗ, будет равно 100 000. Из таблицы G.9 видно, что расхождение риска сценария удовлетворяет допустимому риску.

G.2.10 Шаг 9. Выполнение рекомендаций в случае необходимости

Если *CMS* или расхождение риска сценария не снижают значение риска до ПР, то должны быть сделаны рекомендации. Любая из рекомендаций должна описывать функцию безопасности, классифицируя ее как конкретный тип НСЗ, и обеспечивать требуемое снижение риска. При необходимости командой должны быть представлены другие рекомендации.

Таблица G.8 — Рабочая таблица АСЗ для шага 7 (1 из 2)

Имя системы. 1. Емкость 101 с исходным продуктом.
Чертеж. Чертеж АВС 123.
Цель проекта и метод (методы) управления процессом. Смесь X поступает в емкость 101 для разделения газа и жидкости.

Отклонение	Оценка уровня тяжести *S* последствия и величины снижения риска *RRF*				Оценка частоты исходного события				Определение НСЗ и *RRF*			
	Последствие	Категория	*S*	Требуемая *RRF*	Исходная причина	Тип	Частота	Общая частота	Мера защиты (не НСЗ)	НСЗ	Тип	*RRF*
1 Высокое давление	1 Интенсивный поток приводит к давлению выше 1,5 · MAWP. Возможны повреждение емкости и выброс в окружающую среду в течение 5 мин. Что, если последствие 1.1.1.1	*S*	4	1000	1 Сбои контура управления производством	ОСУП	10	10	1 Недостаточно времени для реакции оператора на аварийный сигнал высокого давления	1 Закрытие входного блокирующего клапана высокого давления	ПСБ	10
		E	4	1000								
		A	3	100								

Таблица G.8 — Продолжение (2 из 2)

Определение системы ослабления последствия *CMS* и *RRF*			Определение расхождения риска для *CMS*					Определение расхождения риска сценария			Рекомендации (АСЗ)	
CMS	Последствие *CMS*	*RRF*	Категория	*S*	Требуемая *RRF* для *CMS*	Общая *RRF* НСЗ	Расхождение *RRF* для *CMS*	Требуемая *RRF*	Общая *RRF* (НСЗ+ *CMS*)	Расхождение *RRF* сценария	Рекомендация	Целевое значение *RRF*
Клапан сброса давления	1 Система предохранения от перегрузок, вызывающая чрезмерное противодавление	100	*S*	4	1000	10	100	1000	1000	ПР		
			E	4	1000		100	1000		ПР		
			A	3	100		100	100		ПР		

Таблица G.9 — Рабочая таблица АС3 для шага 8 (1 из 2)

Имя системы. 1. Емкость 101 с исходным продуктом.
Чертеж. Чертеж АВС 123.
Цель проекта и метод (методы) управления процессом. Смесь X поступает в емкость 101 для разделения газа и жидкости.

Отклонение	Оценка уровня тяжести последствия *S* и величины снижения риска *RRF*				Оценка частоты исходного события				Определение НС3 и *RRF*			
	Последствие	Категория	*S*	Требуемая *RRF*	Исходная причина	Тип	Частота	Общая частота	Мера защиты (не НС3)	НС3	Тип	*RRF*
1 Высокое давление	1 Интенсивный поток приводит к давлению выше 1,5 · MAWP. Возможны повреждение емкости и выброс в окружающую среду в течение 5 мин. Что, если последствие 1.1.1.1	*S*	4	1000	1 Сбои контура управления производством	ОСУП	10	10	1 Недостаточно времени для реакции оператора на аварийный сигнал высокого давления	1 Закрытие входного блокирующего клапана высокого давления	ПСБ	1000
		E	4	1000								
		A	3	100								

Таблица G.9 — Продолжение (2 из 2)

Определение системы ослабления последствия *CMS* и *RRF*			Определение расхождения риска для *CMS*					Определение расхождения риска сценария			Рекомендация (АС3)	
CMS	Последствие *CMS*	*RRF*	Категория	*S*	Требуемая *RRF* для *CMS*	Общая *RRF* НС3	Расхождение *RRF* для *CMS*	Требуемая *RRF*	Общая *RRF* (НС3 + *CMS*)	Расхождение *RRF* сценария	Рекомендация	Целевое значение *RRF*
Клапан сброса давления	1 Система предохранения от перегрузок, вызывающая чрезмерное противодавление	100	*S*	4	1000	1000	ПР	1000	100 000	ПР		
			E	4	1000		ПР	1000		ПР		
			A	3	100		ПР	1000		ПР		

Приложение Н
(справочное)

Качественный подход для оценки риска и назначение уровня полноты безопасности (УПБ)

Н.1 Обзор

В настоящем приложении представлен пример качественного подхода для оценки риска и назначения УПБ, который можно применить к ПСБ для промышленных процессов.

Примечания

1 Методология, описанная в настоящем приложении, использует качественную оценку риска и предназначена для обычного применения при назначении УПБ для функций безопасности ПСБ для промышленных процессов. Используемые параметры риска (см. рисунок Н.2) при применении данной методологии к определенным процессам и их конкретным опасностям могут при их согласовании при включении гарантировать, что ПСБ может обеспечить соответствующее снижение риска.

2 Параметры графа риска для промышленных процессов, используемые в настоящем приложении, представлены в таблице D.1.

3 Настоящее приложение не является исчерпывающим изложением метода, оно предназначено, чтобы проиллюстрировать общие принципы.

Для каждого опасного события должны быть определены требования к полноте безопасности отдельно для каждой из функции безопасности, реализуемых в ПСБ (см. МЭК 61511-1:2016, 6.3.1 и таблицы 3 и 4).

На рисунке Н.1 представлен пример практического способа выполнения оценки риска для конкретного опасного события, позволяющего в результате оценить УПБ для функции безопасности ПСБ. Эта методология должна быть реализована для каждого опасного события, где необходимо снизить риск. Рисунок Н.1 должен использоваться вместе с руководящими указаниями настоящего приложения.

Важно, чтобы граф риска и его калибровка были согласованы на высшем уровне в организации с тем, кто несет ответственность за безопасность.

Оценка риска является итеративным процессом; это означает, что этот процесс, возможно, должен быть выполнен несколько раз.

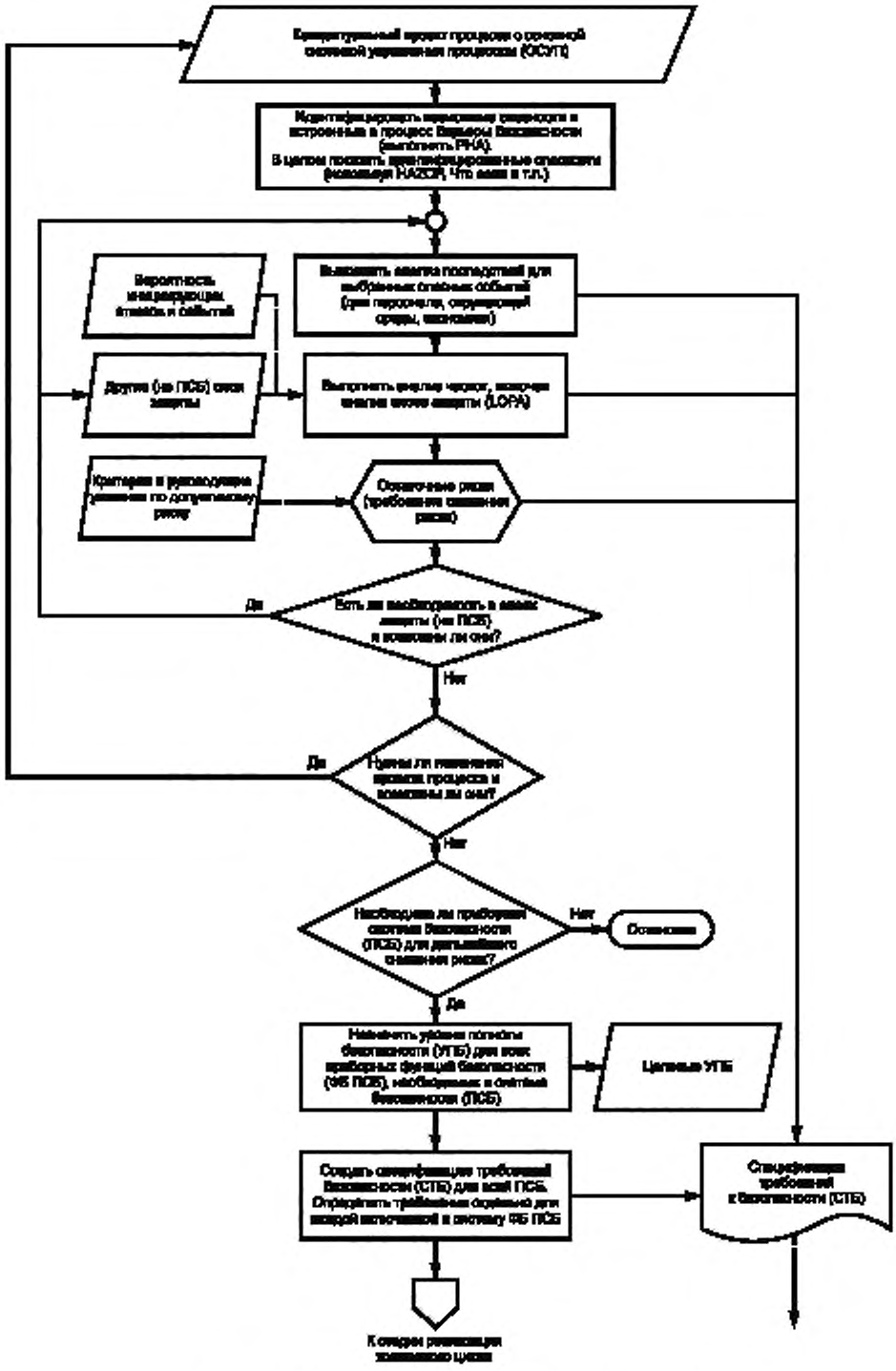


Рисунок Н.1 — Блок-схема процедуры назначения УПБ

Н.2 Оценка риска и назначение УПБ

Н.2.1 Общие положения

Подраздел Н.2 дает представление о том, что и как делается для управления риском и назначения УПБ.

Н.2.2 Идентификация/выявление опасности

Выявить опасное событие, в том числе и от разумного предсказуемого неправильного использования, риск которого должен быть снижен реализацией функции безопасности (ФБ) ПСБ. Перечислить их в колонке опасных событий в таблице Н.1.

Таблица Н.1 — Список функций безопасности ПСБ и опасных событий, которые необходимо оценить

№ ФБ ПСБ	Описание опасного события	Описание функции безопасности ПСБ
01		
02		
03		
04		

Н.2.3 Оценка риска

Для назначения УПБ для функции безопасности ПСБ используется матрица графа риска. Значения УПБ устанавливаются в результате объединения параметра *С* последствия графа риска с суммарной вероятностью параметров *F*, *P* и *W* графа риска. Значение УПБ для каждого опасного события может быть определено отдельно для состояния здоровья, окружающей среды и активов. Общее целевое значение УПБ рассматриваемой функции безопасности ПСБ, будет определяться как максимальное значение УПБ среди этих трех аспектов (состояние здоровья, окружающая среды и активы).

Оценка риска должна быть выполнена для каждого опасного события, определив параметры риска, показанные на рисунке Н.2, и должна быть получена:

- из последствия ущерба *С* и
- вероятности возникновения этого вреда, который является функцией:
  - параметра нахождения в опасной зоне *F*, который является вероятностью того, что в подвергаемой опасности области во время опасного события находятся люди;
  - параметра предотвращения опасного события *P*, описывающего вероятность того, что подвергающиеся опасности люди в состоянии избежать опасной ситуации, которая существует, если возник сбой при запросе к функции безопасности ПСБ;
  - параметра интенсивности запросов *W*, являющегося остаточной интенсивностью запросов или частотой опасных событий в отсутствие рассматриваемой функции безопасности ПСБ.

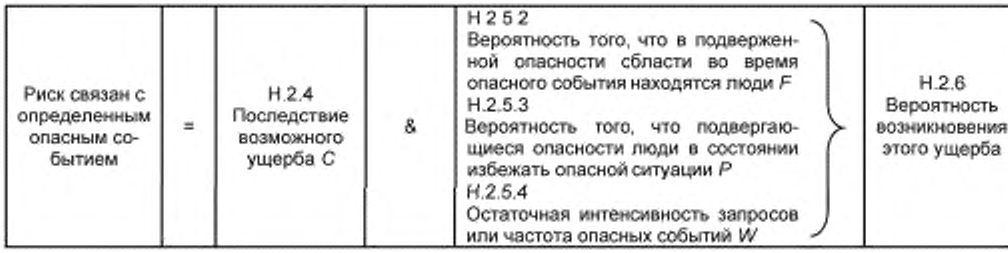


Рисунок Н.2 — Параметры, используемые при оценке риска

Для каждого опасного события может существовать много различных последовательностей событий, которые приводят к этому опасному событию. Все эти последовательности должны быть рассмотрены отдельно, поскольку вероятность наступления события может отличаться (*F*, *P* и *W*).

Н.2.4 Выбор параметра последствия ущерба *С* (таблица Н.2)

Это число смертельных случаев и/или серьезных травм, к которым, вероятно, привело возникновение опасного события. Определяется путем подсчета числа людей в подверженной опасности области с учетом их уязвимости по отношению к опасному событию.

Уровень тяжести *С* — это оценка последствия опасного события. Выбирается надлежащий уровень для опасностей состоянию здоровья, окружающей среде и финансовым вопросам. В графу *С* таблицы Н.2 для каждой отдельной опасности вносится выбранное значение (A—F) уровня тяжести.

Определение надлежащих уровней тяжести заключается в выборе из категорий последствий, откалиброванных на соответствие допустимым уровням риска, установленным службой управления рисками компании и органами власти.

В таблице Н.7 представлены примеры категорий последствий.

Таблица Н.2 — Параметр последствия вреда/уровень тяжести

Параметр последствия ущерба		
Уровень тяжести		*C*
C_F	Катастрофический	F
C_E	Значительный	E
C_D	Серьезный	D
C_C	Ощутимый	C
C_B	Граничный	B
C_A	Незначительный	A

Н.2.5 Вероятность возникновения этого ущерба

Н.2.5.1 Общие положения

Пункт Н.2.5 дает представление об основных параметрах, связанных с вероятностью возникновения ущерба.

Каждый из трех параметров вероятности возникновения вреда (т. е. *F*, *P* и *W*) должен оцениваться независимо друг от друга. Для каждого параметра должен использоваться наихудший случай, чтобы гарантировать, что при указанном значении УПБ ущерба нет.

Н.2.5.2 Выбор параметра нахождения в опасной зоне (таблица Н.3)

Оценка вероятности того, что в подвергаемой опасности области во время опасного события находятся люди. Определяется вычислением доли времени нахождения людей в подвергаемой опасности области во время опасного события. Необходимо учесть возможность нахождения большего числа людей в подвергаемой опасности области, чтобы исследовать нестандартные ситуации, которые могут возникнуть во время подготовки к опасному событию (необходимо также рассмотреть, приводит ли это к изменению параметра *C*).

Вероятность поражения (*F*) является вероятностью того, что в подвергаемой опасности области во время опасного события находятся люди. Вероятность поражения действительна только для оценки риска состояния здоровья людей (*H*). Если нахождение людей будет постоянным или если уже было задано значение для уменьшения вероятности нахождения людей при выборе уровня тяжести ущерба здоровью, то должно быть выбрано значение (F_D) «Постоянно». Вероятность поражения F_C выбирается, если нахождение людей будет частым или если нахождение людей зависит от опасной ситуации. Вероятность поражения F_B выбирается, если в подвергаемой опасности области люди оказались просто случайно и присутствие человека очевидно не связано с опасной ситуацией. Вероятность поражения F_A выбирается только в случае, если подвергаемая опасности область определена и присутствие в ней человека является редким и не зависит от опасной ситуации. В графу *F* таблицы Н.3 вносится выбранное соответствующее число (0—2). Величина параметра нахождения в опасной зоне, равная 1, предопределена для экологических и финансовых опасностей.

Таблица Н.3 — Параметр нахождения в опасной зоне/вероятность поражения *F*

Параметр нахождения в опасной зоне			
Частота присутствия человека в опасной зоне. При выборе категории последствия не должно задаваться ограничение на время нахождения людей в подвергаемой опасности области			
Вероятность поражения			*F*
F_D	Постоянно	= 1	2
F_C	Часто	0,1—1	2
F_B	Случайно	0,01—0,1	1
F_A	Редко	< 0,01	0

Н.2.5.3 Выбор параметра предотвращения (таблица Н.4)

Этот параметр описывает вероятность того, что подвергающиеся опасности люди в состоянии избежать опасной ситуации, которая существует, если возник сбой при запросе к функции безопасности ПСБ. Он зависит от наличия независимых методов предупреждения подвергаемых опасности людей до появления опасности и от наличия методов спасения.

Вероятность предотвращения P является вероятностью предотвращения опасного события, даже если рассматриваемая функция безопасности не предотвращает это событие. Стандартный выбор — значение P_B «Условия предотвращения не выполнены».

Значение P_A может быть выбрано отдельно для опасности причинения вреда здоровью (Н), если все люди из подвергаемой опасности области, вероятно, будут эвакуированы вовремя в безопасную область, если функция безопасности ПСБ не выполнит запрос. Это требует, чтобы:

- у людей было достаточное количество времени для эвакуации и
- существовали независимые средства предупреждения об опасности и эвакуации всех людей из опасной зоны.

P_A также может быть использовано, если опасного события, вероятно, можно вовремя избежать с помощью ручных действий оператора. В такой ситуации P_A также можно использовать для опасностей в экологии и экономике. Это требует, чтобы:

- были доступны независимые средства для предупреждения оператора об опасности функционального отказа и для перевода процесса в безопасное состояние вручную;
- минимум 1 ч должен отделять опасное событие от оповещения о нем оператора.

В графу P таблицы Н.4 вносится соответствующее число (0 или 1) для выбранного параметра предотвращения.

Приложение — В приложении Н выбор значения P_A подразумевает, по крайней мере, 90-процентную вероятность, что опасность будет предотвращена.

Таблица Н.4 — Параметр предотвращения/вероятность предотвращения

Параметр предотвращения		
Вероятность предотвращения опасного события, если возник сбой при запросе к функции безопасности ПСБ. Подразумевает независимые средства, обеспечивающие «остановку оборудования» таким образом, чтобы была предотвращена опасность или была предоставлена возможность позволить всем людям перебежать в безопасное место. Условия, которые должны быть выполнены для P_A: • наличие средств предупреждения оператора о том, что произошел сбой функции безопасности ПСБ; • наличие независимых средств, переводящих процесс в безопасное состояние; • время между оповещением оператора об опасности и опасным событием должно быть более 1 ч		
Вероятность предотвращения		P
P_B	Условия предотвращения не выполнены	1
P_A	Все условия предотвращения выполнены	0

Н.2.5.4 Выбор параметра интенсивности запросов (таблица Н.5)

Число опасных событий в год, которые будут происходить в отсутствие рассматриваемой функции безопасности ПСБ, может быть определено, рассмотрев все отказы, которые могут привести к опасному событию и выполнив оценку общей интенсивности их возникновения. В рассмотрение должны быть включены другие слои защиты.

Параметр интенсивности запросов W выбирается путем оценки или вычисления интенсивности остаточных запросов или частоты опасных событий, если не реализована рассматриваемая функция безопасности ПСБ. Эта частота может быть определена сложением частот отказов и других исходных событий, приводящих к опасному событию. Для систем, не являющихся ПСБ, но реализующих защитные барьеры, должно задаваться определенное значение снижения риска. Общее задаваемое значение снижения риска для барьеров, реализованных в основной системе управления (ОСУП), включая аварийную сигнализацию и реакцию оператора, не может быть больше величины снижения риска, равной 10, по определению в МЭК 61511 (величина снижения риска > 0,1). В графу W таблицы Н.5 вносится выбранное число, соответствующее оцененной или вычисленной интенсивности остаточных запросов.

Таблица Н.5 — Параметр интенсивности запросов (W)

Параметр интенсивности запросов			
Интенсивность запросов			W
W_9	Частая	> 1/1 г.	9
W_8	Часто повторяющаяся	1/(от 1 г. до 3 лет)	8

Окончание таблицы Н.5

Параметр интенсивности запросов			
Интенсивность запросов			*W*
W_7	Вполне вероятная	1/(от 3 до 10 лет)	7
W_6	Вероятная	1/(от 10 до 30 лет)	6
W_5	Случайная	1/(от 30 до 100 лет)	5
W_4	Маловероятная	1/(от 100 до 300 лет)	4
W_3	Невероятная	1/(от 300 до 1000 лет)	3
W_2	Неправдоподобная	1/(от 1000 до 10 000 лет)	2
W_1	Немыслимая	1/(от 10 000 до 100 000 лет)	1

Н.2.6 Оценка вероятности ущерба

Для каждого опасного события и по мере необходимости для каждого аспекта (состояние здоровья, окружающая среда, активы) складывают значения граф *F*, *P* и *W*, а сумму вносят в графу УПБ таблицы Н.6.

Н.2.7 Назначение УПБ

Для определения значения УПБ для каждого из аспектов (состояние здоровья, окружающая среда, активы) используется матрица графа риска (см. таблица Н.6), связывающая уровни тяжести последствия, обозначенные символами от *A* до *F*, с суммарной вероятностью параметров *F*, *P* и *W* (значения от 1 до 12). Общим целевым значением УПБ является максимальное значение УПБ среди этих трех аспектов.

Точка пересечения значения уровня тяжести последствия *C* с соответствующей вероятностью параметров (*F* + *P* + *W*) таблицы Н.6 указывает, какое действие требуется.

Пример — Пусть для конкретной опасности уровень тяжести последствия C для человека определен как катастрофический, а значения F = 1, P = 1 и W = 3, тогда F + P + W = 1 + 1 + 3 = 5. Используя таблицу Н.6, это привело бы к УПБ 2, назначаемому для функции безопасности ПСБ, предназначенной смягчить рассматриваемое опасное событие.

Таблица Н.6 может использоваться для записи результатов процедуры назначения УПБ, используя методологию, описанную в приложении Н.

В таблице Н.6 «NR» означает «неклассифицируемые» средства защиты, начиная со значения ВОНЗ > 0,1.

Таблица Н.6 — Матрица графа риска (форма назначения УПБ для функции безопасности ПСБ)

Проект — Процесс
Выпущен — Предприятие
Дата — Система
Версия — Схема №

Параметр последствия			Матрица графа риска						Параметр нахождения в опасной зоне и			Параметр предотвращения			Параметр интенсивности запросов			
									Частота присутствия человека в опасной зоне. При выборе категории последствия не должно задаваться ограничение на время нахождения людей в опасной зоне			*Вероятность предотвращения опасного события, если возник сбой при запросе к ФБ ПСБ. Подразумевает независимые средства, обеспечивающие «остановку оборудования» таким образом, чтобы была предотвращена опасность или была предоставлена возможность позволить всем людям перебежать в безопасное место. Условия, которые должны быть выполнены:* *- наличие средств предупреждения оператора о том, что произошел сбой функции безопасности ПСБ;* *- наличие независимых средства, переводящих процесс в безопасное состояние;* *- достаточное время между оповещением оператора об опасности и опасным событием*			Оцененная интенсивность запросов ФБ ПСБ			*W*
			Сумма вероятностей (*F* + *P* + *W*)												W_9	Частая	> 1 в г.	9
															W_8	Часто повторяющаяся	1/1—3 г.	8
Уровень тяжести		*C*	1—2	3—4	5—6	7—8	9—10	11—12							W_7	Вполне вероятная	1/3—10 лет	7
C_F	Катастрофический	F	NR	УПБ1	УПБ2	УПБ3	УПБ4	НЕТ							W_6	Вероятная	1/10—30 лет	6
C_E	Значительный	E	NR	NR	УПБ1	УПБ2	УПБ3	УПБ4	Интенсивность поражения		*F*				W_5	Случайная	1/30—100 лет	5
C_D	Серьезный	D	ОК	NR	NR	УПБ1	УПБ2	УПБ3	F_D	Постоянно = 1	2				W_4	Маловероятная	1/100—300 лет	4
C_C	Ощутимый	C	ОК	ОК	NR	NR	УПБ1	УПБ2	F_C	Часто 0,1—1	2	Вероятность предотвращения		*P*	W_3	Невероятная	1/300—1000 лет	3
C_B	Граничный	B	ОК	ОК	ОК	NR	NR	УПБ1	F_B	Случайно 0,01—0,*	1	P_B	Условия предотвращения не выполнены	1	W_2	Неправдоподобная	1/1000—10 000 лет	2
C_A	Незначительный	A	ОК	ОК	ОК	ОК	NR	NR	F_A	Редко < 0,01	0	P_A	Все условия предотвращения выполнены	0	W_1	Немыслимая	1/10 000—100 000 лет	*

Окончание таблицы Н.6

№ ФБ ПСБ	Опасное событие Описание	Функция безопасности ПСБ (ФБ ПСБ). Описание	Последствие		Влияние		Запрос	Вероятность	Полнота		Комментарий
			Ущерб	C	F	P	W	Сумма	УПБ	УПБ	
			H	E	/	1	3	5	1	2	
			E	F				5	2		
			F	C				5	NR		
			H		/			0	0	0	
			E					1	0		
			F					1	0		
			H		/			0	0	0	
			E					1	0		
			F					1	0		
			H		/			0	0	0	
			E					1	0		
			F					1	0		

Таблица Н.7 — Пример категорий последствий

C	Нанесенный человеку ущерб *H*	Вероятность смертельного случая (ВСС)		Максимальные последствия для здоровья из-за опасного события	Дополнительные комментарии к категориям последствия для здоровья
C_F	Катастрофический	ВСС > 1		3 или более погибших. Много (10 или более) в критическом состоянии	Вероятно несколько смертельных случаев
C_E	Значительный	ВСС = 0,1—1,0		1 или 2 погибших. Несколько (3 или более) в критическом состоянии	Отдельный смертельный случай/возможны смертельные случаи
C_D	Серьезный	ВСС = 0,01—0,1		1 или 2 человека в критическом состоянии. 3 или более человек ранены	Несколько человек с травмой/травмами с временной потерей трудоспособности. Один или несколько человек с длительной потерей трудоспособности. Смертельный случай/случаи маловероятны, но возможны
C_C	Ощутимый	ВСС < 0,01		1 или 2 человека ранены. Серьезные недомогания	Один или несколько человек с травмой/травмами с временной потерей трудоспособности. Незначительная вероятность длительной потери трудоспособности. Смертельный случай невероятен
C_B	Граничный	ВСС = 0		Легкая рана/раны. Длительные недомогания	Рана/раны без потери трудоспособности. Требуется лечение
C_A	Незначительный	ВСС = 0		Незначительная рана/раны. Временные недомогания	Рана/раны без потери трудоспособности. Никакое лечение не требуется
C	Экологический вред *E*	Влияния сбросов	Распространение сбросов	Максимальные экологические последствия из-за опасного события	Дополнительные комментарии к экологическим категориям последствия
C_F	Катастрофический	Постоянное	Широкое	Широко распространяющийся или длительный по времени вред. Дезинфекция невозможна или затруднена	Разлив жидкости в реку или море. Крупный выброс пара или аэрозоля. Сбросы наносят длительный или непоправимый ущерб растениям и животному миру
C_E	Значительный	Постоянное	Ограниченное в своем распространении	Ограниченный в своем распространении вред, но постоянный или в течение долгого времени. Дезинфекция невозможна или затруднена	Разлив жидкости в грунтовые воды. Небольшой выброс пара или аэрозоля. Сбросы наносят длительный или непоправимый ущерб растениям и животному миру
C_D	Серьезный	Постоянное	Ограниченное	Ограниченно распространяющийся или ограниченный по времени вред. Дезинфекция невозможна или затруднена	Разлив жидкости на территории. Ограниченный выброс пара или аэрозоля (внутри ограждения). Сбросы наносят длительный или непоправимый ущерб растениям и животному миру
C_C	Ощутимый	Кратковременное	Широкое/небольшое	Вред от широкого до небольшого. Легкая дезинфекция или не нужна	Разлив жидкости в реку или море. Ограниченный выброс пара или аэрозоля. Сбросы наносят временный ущерб растениям и животному миру

Окончание таблицы Н.7

C	Экологический вред E	Влияния сбросов	Распространение сбросов	Максимальные экологические последствия из-за опасного события	Дополнительные комментарии к экологическим категориям последствия
C_B	Граничный	Кратковременное	Ограниченное	Территориально ограниченный временный вред. Легкая дезинфекция или не нужна	Разлив жидкости на территории. Ограниченный выброс пара или аэрозоля (внутри ограждения). Сбросы наносят временный ущерб растениям и животному миру
C_A	Незначительный	Незначительное		Незначительный вред окружающей среде. Дезинфекция не нужна	Слабая утечка во фланце или клапане. Небольшой разлив жидкости или небольшое загрязнение почвы, не влияющее на грунтовые воды. Незначительное воздействие на окружающую среду
C	Финансовый ущерб F	Имущественный ущерб	Производственные потери (т €)	Максимальные финансовые последствия вследствие опасного события	Дополнительные комментарии к финансовым категориям последствия
C_F	Катастрофический	> 10 000	> 50 000	Катастрофические потери производства, доли рынка и имиджа	Катастрофическое повреждение промышленной установки и/или предприятия. Событие, вызывающее остановку производства больше чем на год
C_E	Значительный	1000—10 000	5000—50 000	Значительные производственные потери. Большая потеря доли рынка и/или имиджа	Очень большой ущерб оборудованию и/или имуществу. Событие, вызывающее длительную остановку производства — на несколько месяцев
C_D	Серьезный	100—1000	500—5000	Серьезные производственные потери. Значительная потеря доли рынка и/или имиджа	Серьезное повреждение оборудования и/или имущества. Событие, вызывающее продолжительную остановку производства до месяца
C_C	Ощутимый	10—100	50—500	Ощутимые производственные потери. Граничная потеря доли рынка	Ощутимое повреждение оборудования и/или имущества. Событие, вызывающее продолжительную остановку производства до недели
C_B	Граничный	1—10	5—50	Небольшие производственные потери. Доля рынка и/или имидж не теряются	Незначительное повреждение оборудования. Событие, вызывающее остановку производства до одного дня
C_A	Незначтельный	< 1	< 5	Незначительные производственные потери. Доля рынка и/или имидж не теряются	Незначительное повреждение оборудования. Событие, вызывающее временную (несколько часов) остановку производства

Приложение I
(справочное)

Создание и калибровка графа риска

I.1 Общие положения

Настоящее приложение описывает основные шаги, выполняемые для формирования и калибровки графа риска, который по факторам риска, известным для конкретного обрабатывающего предприятия, позволяет определить уровень полноты безопасности (УПБ) функции безопасности ПСБ.

Граф риска, используемый для оценки необходимых уровней полноты безопасности, для применения на любом обрабатывающем предприятии должен подходить для конкретного применения и быть калиброван, чтобы использовать значения частот допустимых событий, для которых было определено, что они связаны с возможными рисками процессов работы предприятия.

Методы графа риска представлены в МЭК 61511-3 в качестве примера, и пользователь должен удостовериться в том, что они соответствуют применению и гарантируют, чтобы у полученных результатов было правильное значение. Во многих случаях необходимо адаптировать такой метод, чтобы сделать его соответствующим применению, и откалибровать выбранный граф риска, чтобы с помощью него получать правильные значения.

В настоящем приложении не предполагалось описывать исчерпывающее объяснение процесса разработки и калибровки графа риска, оно предназначено для иллюстрации общих принципов. Настоящее приложение основано на методе, описанном более подробно в «Using risk graphs for Safety Integrity Level (SIL) assessment — first edition»; Clive De Salis, C; Institution of Chemical Engineers, 2011.

I.2 Шаги, выполняемые для формирования и калибровки графа риска

Шаги, выполняемые для формирования и калибровки графа риска, могут включать, но не быть ограничены этим, следующее:

- принять решение о том, какие параметры оценки будут включены в граф риска;
- изобразить полную структуру графа риска;
- определить каждый из параметров подробно;
- назначить значения для каждого из параметров, которые соответствуют определениям;
- определить значения частот допустимых событий, которые будут использоваться для каждого определения последствия;
- определить ось калибровки для каждого последствия;
- вычислить все другие значения в графе риска относительно соответствующей оси калибровки;
- преобразовать значения вероятности событий в значения УПБ, используя соответствующую частоту допустимых событий;
- рассмотреть полный граф риска и удалить любые маршруты через граф риска, которые противоречат требованиям.

I.3 Разработка графа риска

В настоящем подразделе кратко описано, как может быть разработан граф риска.

На первых шагах проектирования и калибровки графа риска необходимо определить параметры, для которых должна быть выполнена оценка в процессе формирования полной структуры графа риска, подробного определения каждого параметра и определения диапазона значений, связанного с каждым параметром.

I.4 Параметры графа риска

I.4.1 Выбор параметров

При выборе параметров, использующихся для оценки УПБ для обрабатывающего предприятия, пользователь должен выбрать все надлежащие значения, которые будут оценены. На рисунке I.1 представлены основные параметры, которые должны быть рассмотрены, но другие также могут оказаться важными и должны быть добавлены.

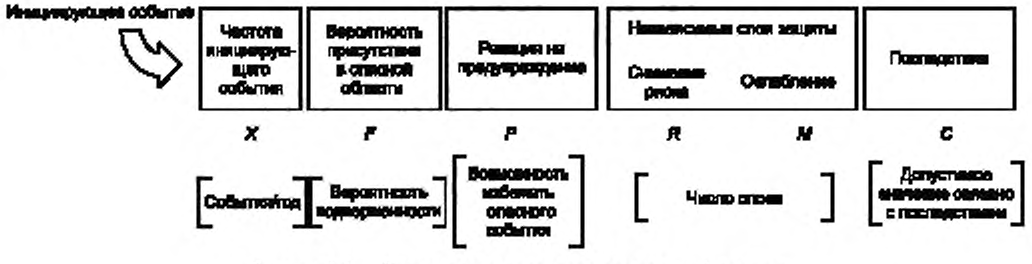


Рисунок I.1 — Рассматриваемые параметры графа риска

Чтобы показать, как может быть разработан граф риска, имеющий большое число параметров, на рисунке I.2 представлен пример, демонстрирующий объединение методов из приложения D (см. рисунок D.1) и приложения C (см. рисунок C.2).

I.4.2 Число параметров

Определив параметры, которые будут использоваться, далее необходимо принять решение о числе значений каждого параметра, которые будут использоваться. Например, может быть достаточно вероятность того, что человек подвергается риску, представлять просто двумя значениями: F1 и F2.

I.4.3 Значение параметра

Затем необходимо определить каждый параметр и каждое значение для этого параметра. Эти определения должны быть достаточно подробно изложены для членов команды оценки, чтобы понять параметр и повторно выбирать правильное значение.

Во время этого шага может быть необходимо пересмотреть решения, принятые либо на одном, либо на обоих предыдущих шагах.

I.4.4 Определение параметра

При определении включаемых параметров рассматривается вся доступная информация.

Например, может иметься информация о частоте события, происходящего на обрабатывающем предприятии, которое находится под управлением ОСУП, и тогда эти данные могут использоваться для того, чтобы определить частоту события и сбои ОСУП при управлении этим событием как общую величину. С другой стороны, могут быть данные об исходном событии независимо от способности ОСУП управлять этим режимом процесса.

Примечание — Если граф риска разрабатывается, исходя из частоты исходного события, то тогда граф риска может включать все другие параметры, с которыми можно определить интенсивность запросов к функции безопасности. Поэтому, чтобы должным образом оценить интенсивность запросов к функции безопасности, должны быть включены другие независимые средства снижения риска.

I.4.5 Граф риска

Граф риска изображается в виде общей диаграммы.

Примечание — Диаграмма обычно будет симметрична по форме и включать все комбинации возможных маршрутов, включая те маршруты в диаграмме, которые позже могут быть исключены. Например, политика компании может состоять в том, чтобы исключить рассмотрение ответа оператора на сигнал тревоги там, где последствием являются, возможно, многократные смертельные случаи. В этом случае в качестве примера диаграмма будет включать линии ответа оператора на этой стадии проекта, но на заключительном этапе опция выбора ответа оператора будет удалена.

Частота инициирующего события *IEF*, событий в год:

1 — не более одного раза в год;

2 — не более одного раза в десять лет;

3 — время жизни предприятия.

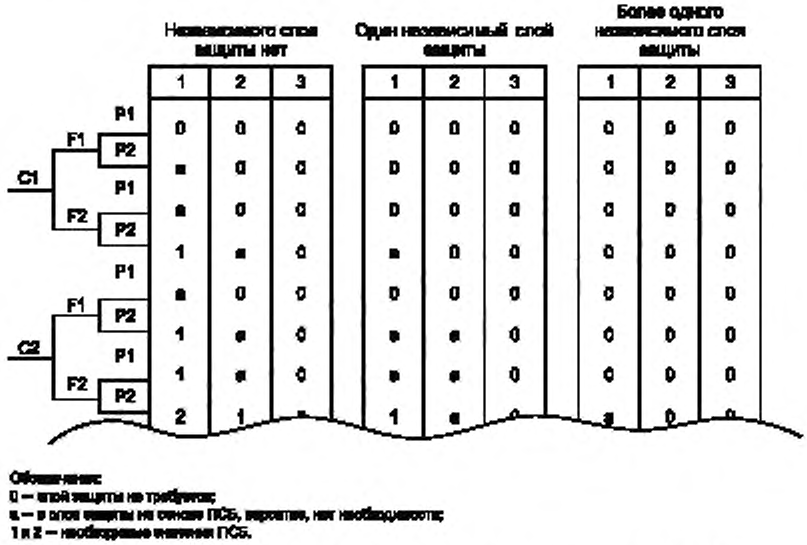


Рисунок I.2 — Иллюстрация графа риска с параметрами из рисунка I.1

I.4.6 Частоты приемлемых событий Tef для каждого последствия

I.4.6.1 Tef-руководство

Руководство по определению частот приемлемых событий.

I.4.6.2 Оценка УПБ частот приемлемых событий

Оценка УПБ частот приемлемых событий отличается для каждого последствия. Назначаемые величины часто связывают с последствием единичного смертельного случая. Если в обосновании безопасности для обрабатывающего предприятия можно использовать линейную прогрессию: единичный смертельный случай = 1, серьезная травма = 0,1 и небольшой ушиб = 0,01, то весь набор этих значений формируется для каждого последствия, определенного в I.4.3 и I.4.4. Но значения прогрессий не всегда линейны. Например, значения могут меняться для многократных смертельных случаев (*N*), и нет ничего необычного в том, что эти значения различны для *N* = 10 или *N* = 50.

I.4.6.3 Граф риска Tef

Необходимо обеспечить, чтобы значения частот приемлемых событий правильно использовались в графе риска. Если частота приемлемого события является числом серьезных травм человека в год, а граф риска предназначен для рассмотрения риска отдельного обрабатывающего предприятия, то эти два условия непосредственно не совместимы. Человек подвергается многократным рискам серьезной травмы в результате его деятельности, и таким образом, проект должен рассмотреть, как преобразовать выражения риска для человека в выражения для рисков единичного события на обрабатывающем предприятии.

I.4.7 Калибровка

I.4.7.1 Общие положения

В данном пункте объясняется значение калибровки при разработке графа риска.

I.4.7.2 Ось калибровки

Ось калибровки для каждого последствия — это путь на графе риска, который строго соответствует этому последствию.

Пример — У графа риска могут быть следующие параметры (см. рисунок I.1):
C3 — единичный смертельный случай;
F2 — вероятность воздействия равняется 1 (т. е. персонал, вероятно, присутствует);
P2 — опасности трудно избежать;
R0 — никакие другие независимые технологические средства по снижению риска не доступны;
M0 — никакие другие независимые меры по снижению риска не доступны;
1 — частота исходного события равна одному событию в год.

Последовательность пути на графе риска в этом примере означает, что результатом является, возможно, единичный смертельный случай, персонал в опасной зоне присутствует, избежать опасности трудно, отсутствуют как независимые средства по снижению риска, чтобы его предотвратить, так и меры по его смягчению, чтобы изменить результат последствия, а также исходное событие происходит каждый год. И это приводит к тому, что погибает один человек в год. Это — ось калибровки для последствия с единичным смертельным случаем, потому что, если частота приемлемого события, требуемая для него, составляет $2 \cdot 10^{-5}$, то вероятность отказа требуемой функции безопасности, предотвращающей это событие, является $2 \cdot 10^{-5}$ FD. Числовое значение каждого параметра в этой последовательности равно 1 и указывает на число присутствующих людей и на вероятность сбоя каждого параметра, который не позволяет предотвратить результат последствия. C3 · F2 · P2 · R0 · M0 · 1 событие в год = 1 смертельный случай · 1 · 1 · 1 · 1 · 1 событие в год = 1 смертельный случай в год.

I.4.7.3 Калиброванные события в год

Для каждой оси калибровки конечный результат записывается в событиях в год, представленных этим путем на графе риска.

I.4.7.4 Число событий в год для пути на графе риска

Используя значения, определенные в I.4.3, I.4.4 и I.4.7.3, вычисляется число событий в год, которые произойдут для каждого пути на графе риска, настраивая каждый раз один параметр.

Это можно проиллюстрировать на том же самом примере из I.4.7.2, в котором будет изменено одно значение, например F2 на F1.

В результате граф риска будет иметь следующие параметры:

C3 — единичный смертельный случай;

F1 — вероятность воздействия равняется 0,1 (т. е. вероятность нахождения персонала в опасной зоне менее 10 %);

P2 — опасности трудно избежать;

R0 — никакие другие независимые технологические средства по снижению риска не доступны;

M0 — никакие другие независимые меры по снижению риска не доступны;

1 — частота исходного события равна одному событию в год.

Последовательность пути на графе риска в этом случае означает, что результатом является, возможно, единичный смертельный случай, персонал в опасной зоне присутствует менее 10 % времени, избежать опасности трудно, отсутствуют как независимые средства по снижению риска, чтобы его предотвратить, так и меры по его смягчению, чтобы изменить результат, а также исходное событие происходит каждый год. И это приводит к тому,

что погибает 0,1 человек в год. Числовое значение каждого параметра в этой последовательности равно 1 и указывает на число присутствующих людей и на вероятность сбоя каждого параметра, который не позволяет предотвратить результат последствия, за исключением значения F2, для которого было определено, что персонал в опасной зоне присутствует менее 10 % времени и поэтому он равен 0,1. С3 · F2 · P2 · R0 · M0 · 1 событие в год = 1 смертельный случай · 0,1 · 1 · 1 · 1 · 1 событие в год = 0,1 смертельный случай в год.

I.4.7.5 Вычисление $ВОНЗ_{ср}$

Для каждой из ветвей графа риска вычисляются частоты событий. Далее необходимо разделить значение частоты допустимых событий для рассматриваемого последствия на вычисленную частоту событий для каждой ветви графа риска. Полученные значения заносятся в граф риска и являются требуемыми значениями $ВОНЗ_{ср}$.

I.4.7.6 Преобразование $ВОНЗ_{ср}$ в УПБ

Далее необходимо преобразовать каждое значение $ВОНЗ_{ср}$ в значение УПБ. При преобразовании для графа риска значений $ВОНЗ_{ср}$ в значения УПБ они никогда не должны округляться в меньшую сторону, т. е. к менее жесткому значению, а всегда должны округляться в большую сторону.

I.4.8 Завершение создания графа риска

I.4.8.1 Общие положения

В данном пункте рассматриваются вопросы о том, чем завершается создание графа риска.

I.4.8.2 Удаление путей

Пути, которые не должны присутствовать в графе риска, удаляются из него.

Например, политика компании может состоять в том, чтобы исключить рассмотрение реакции оператора на сигналы тревоги, последствием которых могут быть многократные смертельные случаи. В случае рассматриваемого примера путь/пути, связанный(е) с реакцией на возможное предупреждение, должен(ны) быть удален(ы) из графа риска, где возможным результатом являются многократные смертельные случаи.

I.4.8.3 Инструкции по применению графа риска

Должен быть подготовлен подробный набор инструкций, описывающих правильное использование графа риска. Эти инструкции должны включать описания ограничений использования графа риска (т. е. пределы применимости).

Приложение J
(справочное)

Многоконтурные системы безопасности

J.1 Общие положения

Полуколичественные подходы, представленные в приложениях настоящего стандарта, очень полезны для быстрой оценки снижения риска, которое необходимо для достижения целевой частоты данного опасного события, установленной в процессе предшествующего анализа риска (см. приложение А о подходе ALARP). Тем не менее основная гипотеза о том, что снижение риска, достигаемое ПСБ, непосредственно связано с ее соответствующей мерой отказов (например, средним значением неготовности — $ВОНЗ_{ср}$), верна только тогда, когда реализована единичная ПСБ. Если разрабатывается несколько последовательно работающих систем безопасности (ПСБ и не ПСБ) для предотвращения данного опасного события, то сокращение риска все же увеличивается при снижении величины отказов этими системами, но связь не так проста, и сокращение риска, которое фактически обеспечивается данной ПСБ, может быть ниже, чем то, которое может быть получено непосредственно при снижении величины отказов этой ПСБ, когда она работает отдельно. Это тем более верно, когда периодически выполняются контрольные проверки систем.

Поэтому, если разработано несколько работающих вместе систем безопасности в соответствии с подходами, представленными в приложениях настоящего стандарта, то важно проверить, что отказы по общей причине и влияние зависимостей между системами безопасности незначительны или должным образом учтены, чтобы фактически обеспечить допустимую частоту опасного события.

Примечание — Дополнительную информацию можно найти в документах, представленных в библиографии.

J.2 Понятие системных зависимостей

На рисунке J.1 представлены обычные вычисления, используемые в полуколичественных подходах. Две ПСБ ($ПСБ_1$ и $ПСБ_2$) работают последовательно. Если происходит запрос от процесса, то сначала должна реагировать $ПСБ_1$. Если в ней происходит отказ, то, в свою очередь, должна реагировать $ПСБ_2$, и если она также отказывает, то происходит опасное событие.

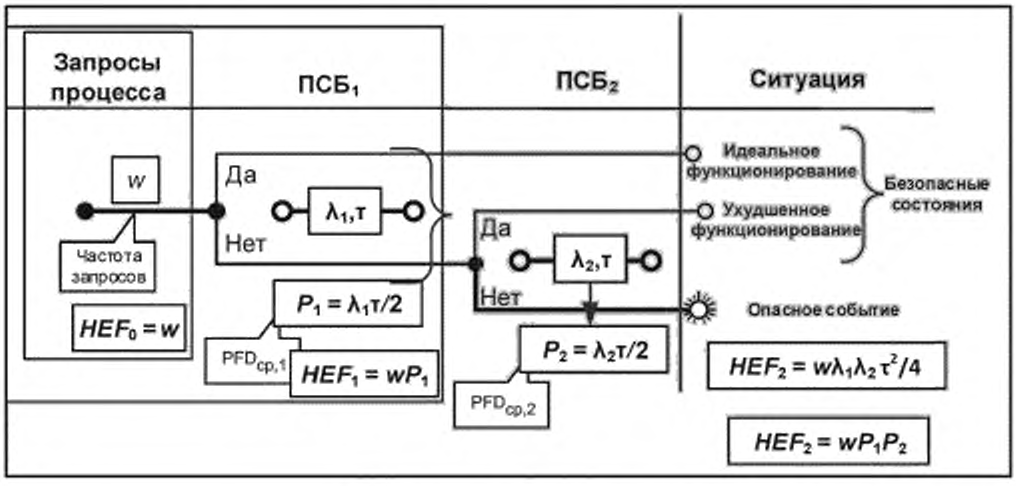


Рисунок J.1 — Обычные вычисления

При использовании полуколичественных подходов признано, что снижение риска, обеспечиваемое ПСБ, равно обратной величине ее меры отказов (например, $P_i = 1/ВОНЗ_{ср,i}$). Поэтому в отсутствие ПСБ частота опасного события HEF_0 равна самой частоте запросов w. Далее функция безопасности $ПСБ_1$ обеспечивает снижение риска $HEF_0/HEF_1 = 1/P_1$, и риск снижается до $HEF_1 = w \cdot P_1$. Затем функция безопасности $ПСБ_2$ обеспечивает снижение риска $HEF_1/HEF_2 = 1/P_2$, и риск снижается до $HEF_2 = HEF_1 \cdot P_2 = w \cdot P_1 \cdot P_2$, которое, как предполагается, удовлетворяет требованиям к допустимой частоте опасного события.

Однако периоды контрольных проверок, значения MTTR, MRT, отказы по общей причине и другие факторы каждого из ПСБ могут взаимодействовать между собой, что даст снижение риска, отличное от предполагаемого, которое было описано перед этим в упрощенном виде.

В простом примере на рисунке J.1 $ПСБ_1$ включает только один датчик *S*, одно логическое решающее устройство *LS* и один исполнительный элемент *FE*, которые соединены последовательно и тестируются одновременно с периодом контрольных проверок. Тогда интенсивность отказов $ПСБ_1$ равна $\lambda_1 = \lambda_{1S} + \lambda_{1LS} + \lambda_{1FE}$, и ее среднее значение неготовности (т. е. $ВОНЗ_{ср,1}$) равно $P_1 = \left(\frac{\lambda_1 \tau}{2}\right)$. Точно так же среднее значение неготовности $ПСБ_2$ (т. е. $ВОНЗ_{ср,2}$) равно $P_2 = \left(\frac{\lambda_2 \tau}{2}\right)$. Поэтому с двумя ПСБ частота опасного события будет $HEF_2 = w \cdot P_1 \cdot P_2 = w\left(\frac{\lambda_1 \tau}{2}\right)\left(\frac{\lambda_2 \tau}{2}\right) = w\left(\frac{\lambda_1 \lambda_2 \tau^2}{2}\right)$, где функция безопасности $ПСБ_1$ обеспечивает снижение риска $HEF_0/HEF_1 = 1/ВОНЗ_{ср,1}$, а функция безопасности $ПСБ_2$ обеспечивает снижение риска $HEF_1/HEF_2 = 1/ВОНЗ_{ср,2}$.

Приведенные выше вычисления учитывают только период проверок, но не планирование тестов во времени. На рисунке J.2 показано, что две ПСБ тестируются в одно и то же время. Это известная общепринятая политика испытаний, позволяющая упростить задачи команде обслуживания или минимизировать число остановок процесса для выполнения тестов.

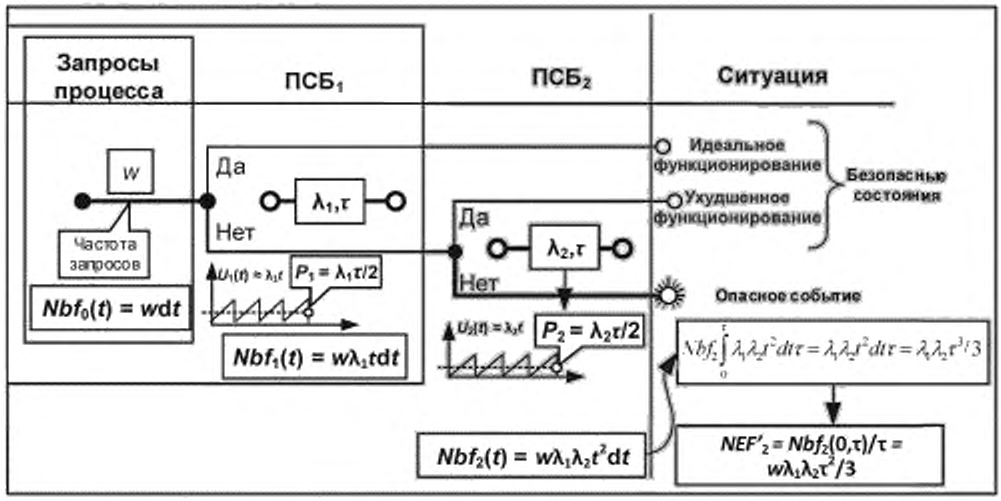


Рисунок J.2 — Точные вычисления

В пределах периода между контрольными проверками значение неготовности $ПСБ_1$ описывается выражением $U_1(t) = 1 - e^{-\lambda_1 t}$, которое можно упростить до $U_1(t) = \lambda_1 t$, при $\lambda_1 t < 1$. Сразу после контрольной проверки значение $U_1(t)$ имеет нулевое значение (если время ремонта незначительно или процесс остановлен), затем оно увеличивается непосредственно до следующей контрольной проверки. В результате получаем известную пилообразной кривую, которая представлена в рисунке J.2. Точно так же получаем пилообразной кривую и для $U_2(t)$. Поэтому $U_1(t)$ и $U_2(t)$ можно считать взаимосвязанными, так как они имеют минимальные значения (сразу после теста) и максимальные значения (непосредственно перед тестом) в одно и то же время. Кажется, что это несущественно, но фактически появляется *системная* зависимость между $ПСБ_1$ и $ПСБ_2$, которые поэтому не являются абсолютно независимыми. Термин «системная зависимость» означает, что эта зависимость является свойством $ПСБ_1$ и $ПСБ_2$, рассматриваемых как единое целое, которое нельзя описать, рассматривая отдельно только $ПСБ_1$ или $ПСБ_2$. Необходимо отметить, что этот тип взаимосвязи не проявляется в непосредственно обнаруженных отказах (например, выявленных диагностическими тестами), потому что неготовность, связанная с этими отказами, достигает целевых значений, которые не имеют отношения к отказам, выявляемым контрольными проверками.

В случае запроса вероятность сбоев $ПСБ_1$ равна $\lambda_1 t$, вероятность сбоя обеих $ПСБ_1$ и $ПСБ_2$ равна $\lambda_1 \lambda_2 t^2$, а вероятность опасного события равна $w\,\lambda_1 \lambda_2 t^2$. Если w — частота запросов, то $Nbf_0 = wdt$ — число запросов, происходящих между t и $t + dt$ (т. е. число опасных событий в отсутствие системы безопасности). С двумя ПСБ число опасных событий, происходящих за dt, будет равно $Nbf_2(t) = w\lambda_1 \lambda_2 t^2 dt$, и простое интегрирование дает число опасных событий, происходящих на отрезке $[0, \tau]$ в виде $Nbf_2(0, \tau) = w\lambda_1 \lambda_2 0, \tau^3/3$. Наконец средняя частота опасных

событий равна $HEF_2' = Nbf_2(0, \tau)/\tau = w\lambda_1\lambda_2\tau^2/3$. Необходимо отметить, что частота запросов w считается постоянной. Тогда $3/\lambda_1\lambda_2\tau^3$. представляет снижение риска, обеспеченное эквивалентной одной системой безопасности, включающей и $ПСБ_1$, и $ПСБ_2$.

Наконец $HEF_2' = 1{,}33HEF_2$, которая, очевидно, больше, чем HEF_2. Выражение для HEF_2' можно записать в виде $HEF_2' = w\left(\frac{\lambda_1\tau}{2}\right)\frac{4}{3}\left(\frac{\lambda_2\tau}{2}\right) = w \cdot P_1 \cdot 1{,}33P_2$, которое показывает, что $ПСБ_1$ на 100 % реализует свои возможности P_1 по снижению риска, а $ПСБ_2$ — только на 3/4 = 75 % P_2, так как она действует на второй позиции.

Если добавить третью ПСБ и проверять ее в то же самое время (т. е. $P_3 = \left(\frac{\lambda_3\tau}{2}\right)$), то частота опасных событий стала бы $HEF_3' = w\lambda_1\lambda_2\lambda_3\tau^3/4 = 2w\left(\frac{\lambda_1\tau}{2}\right)\left(\frac{\lambda_2\tau}{2}\right)\left(\frac{\lambda_3\tau}{2}\right) = 2w \cdot P_1 \cdot P_2 \cdot P_3$, т. е. снижение риска только на 1/2 = 50 % того, что ожидалось от полуколичественных подходов. Запись $HEF_3' = w\left(\frac{\lambda_1\tau}{2}\right)\frac{4}{3}\left(\frac{\lambda_2\tau}{2}\right)\frac{3}{2}\left(\frac{\lambda_3\tau}{2}\right) = HEF_2' \cdot 1{,}5 \cdot P_3$ показывает, что вклад третьей ПСБ равен только 2/3 = 66 % ожидаемой.

Выражение для HEF_2' можно записать в виде $HEF_2' = [w\left(\frac{\lambda_1\tau}{2}\right)]\frac{4}{3}\left(\frac{\lambda_2\tau}{2}\right) = w'\frac{4}{3}\left(\frac{\lambda_2\tau}{2}\right)$ (w' является частотой запросов к $ПСБ_2$). Если w' рассматривать в качестве запросов процесса, то это выражение показывает, что между процессом и ПСБ могут также существовать системные зависимости. Поэтому даже в случае рассмотрения одной ПСБ эти зависимости могут дать меньшее снижение риска, чем ожидалось.

Если теперь разнести по времени проверки и выполнить определенные математические вычисления, то можно найти, что оптимум достигается, когда $ПСБ_2$ проверяется в середине периода контрольных проверок $ПСБ_1$. В этом оптимальном случае частота опасных событий снижается и равна $HEF_2'' = w\frac{5}{24}\lambda_1\lambda_2\tau^2$. Это выражение можно записать в виде $HEF_2'' = w\left(\frac{\lambda_1\tau}{2}\right)\frac{10}{12}\left(\frac{\lambda_2\tau}{2}\right) = wP_1\frac{10P_2}{12}$. Контрольные проверки все еще связаны между собой, но теперь $ПСБ_2$ обеспечивает снижение риска на 12/10 = 120 % от того, что ожидалось. Поэтому связь между контрольными проверками различных ПСБ может воздействовать либо позитивно, либо негативно в зависимости от реализуемой политики контрольных проверок.

Как показано слева на рисунке J.3, многоконтурная система безопасности, анализ которой выполнен выше, эквивалентна одиночной избыточной ПСБ. Это приводит к появлению возможных отказов по общей причине (ООП), которые, вероятно, будут существовать между $ПСБ_1$ и $ПСБ_2$, как показано на этом рисунке справа. Отказы по общей причине также возникают в результате существования системных зависимостей между $ПСБ_1$ и $ПСБ_2$.

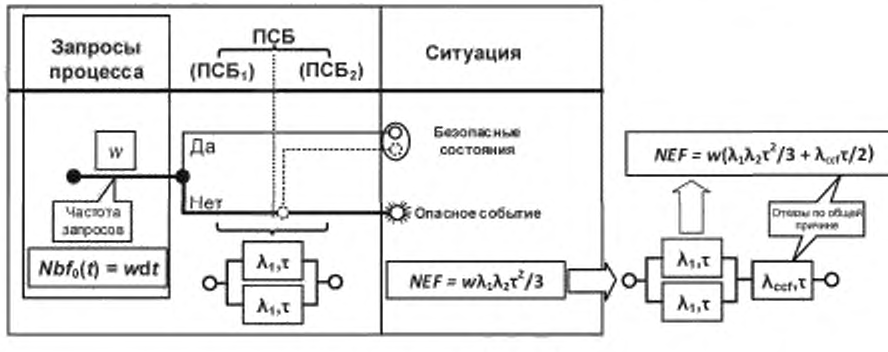


Рисунок J.3 — Избыточная ПСБ

Влияние ООП обычно более важно, чем связь между контрольными проверками, и оно всегда негативно. В вышеупомянутом примере, где контрольные проверки выполняются в одно и то же время, это влияние описывается дополнительным слагаемым $w\lambda_{ccf}\tau/2$ в выражении для частоты опасных событий. Это влияние может быть снижено, если контрольные проверки разнесены между собой по времени, т. е. когда $ПСБ_1$ и $ПСБ_2$ не проверяются в одно и то же время, а любой тест может выявить ООП при условии, что реализованы соответствующие процедуры. Интервал контрольных проверок ООП может быть уменьшен до $\tau/2$, таким образом, в два раза уменьшая вклад ООП в частоту опасных событий. С третьей ПСБ, подобной $ПСБ_1$ и $ПСБ_2$, вклад ООП может быть уменьшен в три раза и т. д.

В заключение необходимо отметить, что снижение риска, обеспеченное многоконтурной ПСБ, где ПСБ работают последовательно, может быть меньше, равно или больше, чем ожидаемое от полуколичественных подходов.

Если разные системы безопасности периодически проверяются в одно и то же время, то полуколичественные подходы приводят к неконсервативным результатам и этот неоконсерватизм растет с уровнем избыточности. Если реализуются сложные контрольные проверки, то результат сравнения между позитивным либо негативным воздействием трудно предвидеть. Поэтому если многоконтурная система безопасности была разработана согласно индивидуальным требованиям, установленным в полуколичественных подходах, то разумно проверить, что целевая допустимая частота опасных событий фактически достигнута.

Примечание — На одиночную систему безопасности с избыточными компонентами влияют те же самые описанные выше системные зависимости, поэтому она может быть проанализирована таким же образом.

J.3 Полуколичественные подходы

Полуколичественные подходы могут использоваться для проверки влияния отказов по общей причине и системных зависимостей на частоту опасных событий.

Если реализован подход разнесения контрольных проверок по времени (чтобы смягчить негативное воздействие связи между ними) и не выявлены какие-либо отказы по общей причине между одиночными ПСБ, формирующими многоконтурную систему безопасности, то можно использовать обычные вычисления. В других случаях необходимы некоторые поправки к ним.

Если выявлены отказы по общей причине, то они должны быть рассмотрены на уровне многоконтурной системы безопасности, как показано на рисунке J.3. Если контрольные проверки разнесены по времени и реализована соответствующая процедура, то интервал контрольных проверок ООП может быть снижен до интервала между последовательными контрольными проверками, разнесенными по времени.

Если подход разнесения по времени контрольных проверок не реализован, то необходимо рассмотреть системные зависимости из-за связи контрольных проверок. Их можно учесть с помощью корректирующих коэффициентов, подобных представленным на рисунке J.4, которые могут помочь оценить необходимые изменения значения частоты опасных отказов. Эта таблица была построена на основе гипотезы, что все компоненты проверяются в одно и то же время. Изменение значения частоты опасных отказов увеличивается с ростом числа отдельных ПСБ и с увеличением длины сценариев, приводящих к опасному событию (так называемого порядка минимальных сечений — МС). Левая таблица на рисунке J.4 описывает многоконтурную систему безопасности, состоящую из двух отдельных ПСБ, а правая таблица — из трех отдельных ПСБ. Корректирующие коэффициенты в этих таблицах вычисляются как отношение m/n (m — коэффициент для всей системы, полученный из вычислений для отдельных ее составных частей, а n — коэффициент для всей системы, полученный из вычислений для всей системы в целом). Например, для МС порядка 2 для многоконтурной системы безопасности, состоящей из двух отдельных ПСБ, сравниваются значения выражения вида $\lambda_1 \cdot \tau/2 \cdot \lambda_2 \cdot \tau/2$ (вычисленные для отдельных составных частей) со значениями выражения вида $\lambda_1\lambda_2{}^2\tau^3/3$ (вычисленными для всей системы в целом), и этот корректирующий коэффициент равен $2 \cdot 2/3 = 4/3 = 1{,}33$.

МСБ	$ПСБ_1$	$ПСБ_2$	
Порядок сечения	Порядок сечения	Порядок сечения	Коэффициент
2	1	1	4/3 = 1,33
3	1	2	6/4 = 1,50
3	2	1	6/4 = 1,50
4	1	3	8/5 = 1,60
4	3	1	8/5 = 1,60
4	2	2	9/5 = 1,80
5	1	4	10/6 = 1,67
5	4	1	10/6 = 1,67
5	2	3	12/6 = 2,00
5	3	2	12/6 = 2,00

МСБ	$ПСБ_1$	$ПСБ_2$	$ПСБ_3$	
Порядок сечения	Порядок сечения	Порядок сечения	Порядок сечения	Коэффициент
3	1	1	1	8/4 = 2,00
4	1	1	2	12/5 = 2,40
4	1	2	1	12/5 = 2,40
4	2	1	1	12/5 = 2,40
5	1	1	3	16/6 = 2,67
5	1	3	1	16/6 = 2,67
5	3	1	1	16/6 = 2,67
5	1	2	2	18/6 = 3,00
5	2	1	2	18/6 = 3,00
5	2	2	1	18/6 = 3,00

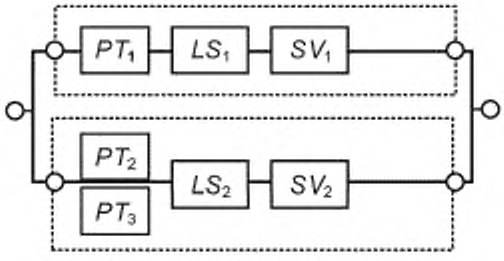
Рисунок J.4 — Корректирующие коэффициенты для вычисления частоты опасных событий для контрольных проверок, выполняющихся в одно и то же время

Таблицы на рисунке J.4 применяются для минимальных сечений (исключая отказы по общей причине) на уровне многоконтурной системы безопасности (МСБ), и для этого необходимо оценить максимальный порядок сечений, вносящий вклад в частоту опасных событий, который используется для определения корректирующих коэффициентов (правые колонки таблиц, представленных на рисунке J.4). Например, если максимальный порядок вносящего вклад сечения равен 3, и если многоконтурная система безопасности включает две ПСБ (левая таблица рисунка J.4), то частота опасных событий, вычисленная с помощью полуколичественного подхода, должна быть умножена на корректирующий коэффициент, равный 1,5.

Для вносящего вклад максимального порядка, равного 4, частота опасных событий должна быть умножена на корректирующий коэффициент в пределах от 1,6 до 1,8. Для минимальных сечений порядка 5 многоконтурной системы безопасности, состоящей из трех ПСБ (правая таблица рисунка J.4), она должна быть умножена на корректирующий коэффициент в пределах от 2,7 до 3 и т. д. Если многоконтурная система безопасности включает соединение нескольких различных структур, то должен использоваться больший коэффициент для обеспечения консервативности.

J.4 Булевы подходы

Чтобы показать, как могут быть выполнены многоконтурные системы безопасности, пример, для которого уже выполнялся анализ в J.2, был немного изменен: теперь $ПСБ_1$ и $ПСБ_2$ не одинаковы, а логические решающие устройства имеют только выявляемые опасные отказы. С двумя избыточными датчиками интенсивность отказов $ПСБ_2$ больше не является постоянной величиной. Этот новый пример детально рассмотрен, и для него построена модель в виде блок-схемы надежности, которая представлена на рисунке J.5 (*PT* — датчик давления, *LS* — логическое решающее устройство и *SV* — предохранительный клапан). Каждая ПСБ включает датчики (один или два), одно логическое решающее устройство и один предохранительный клапан, соединенные последовательно. Девять сценариев отказа (т. е. так называемые минимальные сечения), полученные на основании этой модели, являются следующими: {PT_1, PT_2, PT_3}, {PT_1, LS_2}, {PT_1, SV_2}, {LS_1, PT_2, PT_3}, {LS_1, LS_2}, {LS_1, SV_2}, {SV_1, PT_2, PT_3}, {SV_1, LS_2}, {SV_1, SV_2}. Минимальные сечения (МС), которые связаны с подобными компонентами, являются кандидатами на отказы по общей причине. Поэтому к девяти предыдущим должны быть добавлены три минимальных сечения: $ООП_P$, $ООП_{LS}$ и $ООП_{SV}$. В результате имеем двенадцать минимальных сечений (3 одиночных отказа, 6 двойных отказов и 3 тройных отказа). Затем первая идея может состоять в том, чтобы использовать для каждого из них некоторые упрощенные формулы, подобные предложенным в приложении В МЭК 61508-6:2010. Это возможно при условии, что эти формулы получены для случая системы с неодинаковыми компонентами (например, компоненты с различными видами отказов и/или различными периодами контрольных проверок).



	Интенсивность отказов	Интенсивность ремонта	Тестовый интервал
PT_1	4,50E-06	0,125	4380
PT_2	4,50E-06	0,125	8760
PT_3	4,50E-06	0,125	8760
PT_4	6,25E-04	0,125	Обнаружен
PT_5	6,25E-04	0,125	Обнаружен
PT_6	3,55E-06	0,042	8760
PT_7	3,55E-06	0,042	8760

Рисунок J.5 — Расширение простого примера

Вторая идея состоит в том, чтобы использовать подход дерева отказов, который, оказывается, является очень эффективным, когда компоненты достаточно независимы (например, вероятность одновременно двух отказов в ПСБ низка) и при условии, что вычисления выполнены корректно. Дерево отказов, связанное с упомянутой выше многоконтурной ПСБ, представлено на рисунке J.6.

Дерево отказов позволяет получить непосредственно мгновенное значение неготовности события верхнего уровня, исходя из мгновенных значений неготовности исходных событий. Как сказано выше и как показано на рисунке J.6, неготовность периодически проверяемого события описывается пилообразной кривой (см. примечание). Вычисление дерева ошибок для соответствующего числа моментов времени t_j за установленный период (например, два года) позволяет получить значение неготовности на уровне выходных логических элементов (включая событие верхнего уровня). Эти значения представляют собой более или менее сложные пилообразные кривые согласно политике контрольных проверок. Вычисление средних значений этих кривых за установленный период дает среднее значение неготовности (например, $ВОНЗ_{ср}$). Эта операция по усреднению сталкивается с системными зависимостями из-за наличия связи между контрольными проверками. Следует отметить, что для моделирования отказов по общей причине между PT_2 и PT_3 $ПСБ_2$ используется бета-фактор, равный 1 %.

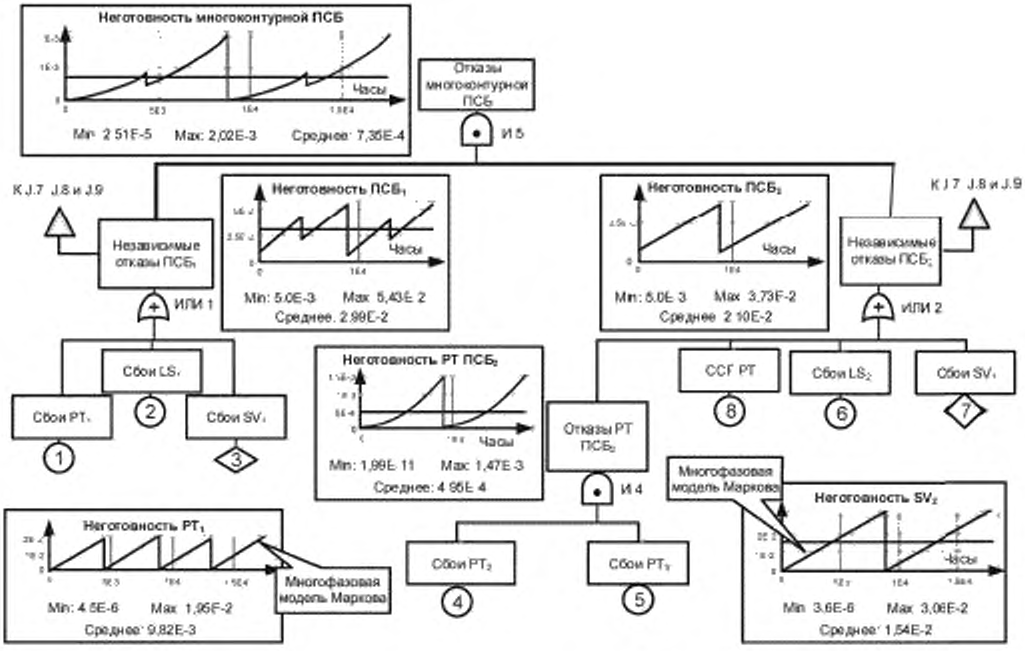


Рисунок J.6 — Моделирование дерева отказов многоконтурной ПСБ, представленной на рисунке J.5

Примечание — Входные пилообразные кривые могут быть получены из многофазной модели Маркова [см. МЭК 61508-6:2010 (приложение В)]. Затем деревья отказов используются, чтобы связать маленькие модели Маркова. Это эффективно, когда эти маленькие модели Маркова независимы друг от друга. С данными, используемыми для этого примера, и для независимых отказов можно получить среднюю доступность $P_1 = 2{,}99 \cdot 10^{-2}$ для $ПСБ_1$ и $P_2 = 2{,}10 \cdot 10^{-2}$ для $ПСБ_2$. С полуколичественным подходом это привело бы к снижению риска $1/P_1P_2 = 1588$, когда оно равно только $1/7{,}35 \cdot 10^{-4} = 1360$ (т. е. различие приблизительно 15 %).

Моделирование возможных отказов по общей причине между $ПСБ_1$ и $ПСБ_2$ не отражено на рисунке J.6. Это сделано на рисунке J.7, где отказы по общей причине между *PTs*, *LSs* и *SVs* рассмотрены с бета-фактором, равным 1 %. Теперь среднее значение неготовности многоконтурной системы безопасности $1{,}018 \cdot 10^{-3}$, и полное снижение риска упало до 982. Это приблизительно 62 % снижения риска, ожидаемого от полуколичественного подхода при гипотезе о полной независимости $ПСБ_1$ и $ПСБ_2$.

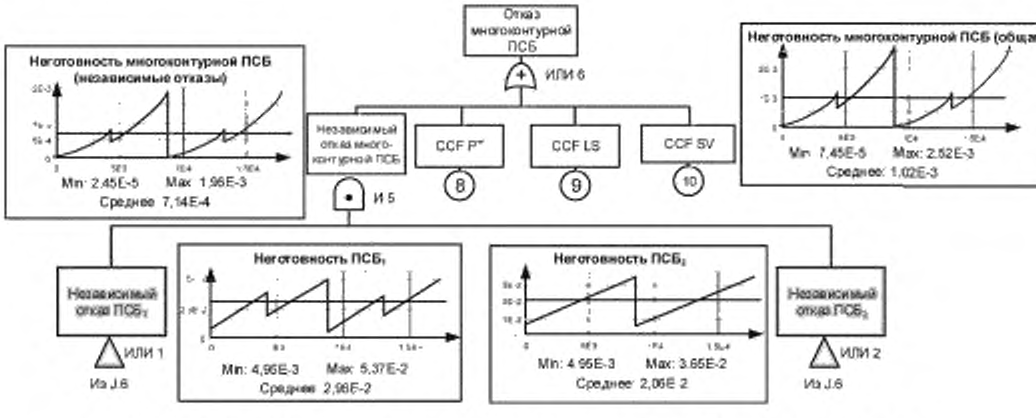


Рисунок J.7 — Моделирование отказов по общей причине ООП между $ПСБ_1$ и $ПСБ_2$

На рисунке J.8 проверки трех *PTs* были разнесены, также как и двух *SVs*. Среднее значение неготовности двух ПСБ, рассматриваемых как единое целое, будет $6{,}68 \cdot 10^{-4}$, а полное снижение риска увеличилось до 1497. Это просто немного ниже, чем ожидаемое от полуколичественного подхода.

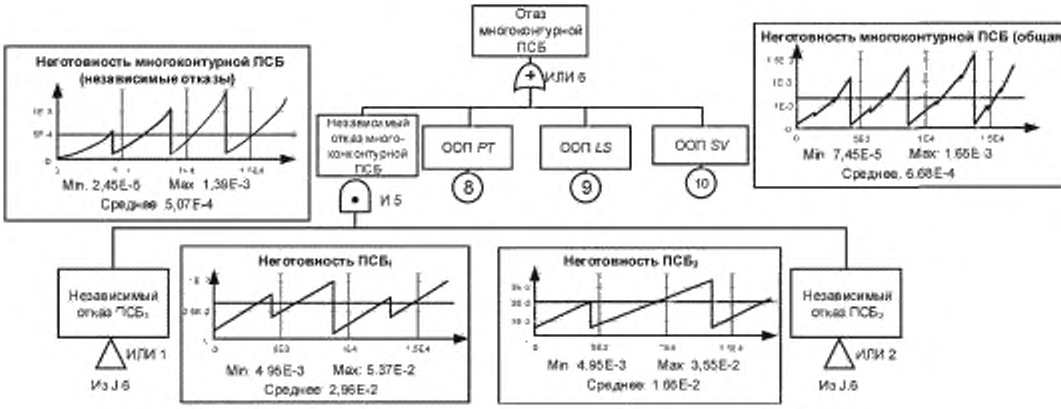


Рисунок J.8 — Влияние разнесения по времени проверок

На рисунке J.9 были разделены виды отказов предохранительного клапана между теми, которые обнаружены при частичном движении, и теми, которые обнаружены при полном движении. Среднее значение неготовности двух ПСБ, рассматриваемых как единое целое, будет $3{,}30 \cdot 10^{-4}$, а полное снижение риска увеличилось до 3034. Это в два раза больше, чем ожидалось при полуколичественном подходе.

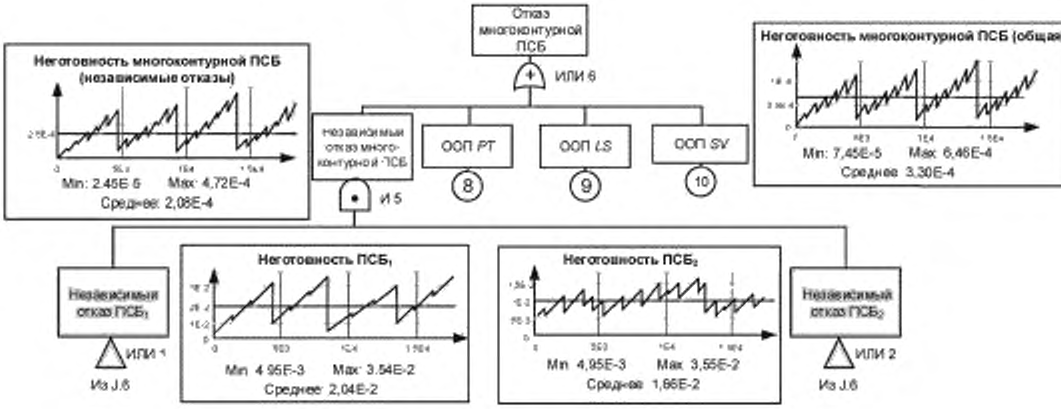


Рисунок J.9 — Влияние частичного движения

J.5 Подход на основе состояний-переходов

Подход на основе дерева отказов очень эффективен, когда компоненты достаточно независимы. Но это не так, если компоненты сильно зависят друг от друга, как в примере при выполнении ремонта в случае второго отказа, если изменяется логика (например, от 2oo3 до 1oo2) вместо ее восстановления, если растет задержка начала ремонта из-за сбора инструментов для ремонта (например, для подводных ремонтных работ судна динамического расположения) и т. д. В этом случае необходимо использовать модели на основе состояний-переходов, обеспечивающие надлежащее представление динамического поведения компонентов. Марковский подход (см. приложение В МЭК 61508-6:2010) является самым популярным подходом на основе пространства состояний, но для многоконтурной системы безопасности должно быть промоделировано большое число компонентов, что, вероятно, вызовет

комбинационный взрыв числа состояний. Поэтому необходимо рассматривать другие подходы, которые свободны от этого недостатка. Среди них очень эффективным оказался подход на основе сетей Петри [см. МЭК 61508-6:2010 (приложение В) и МЭК 62551:2012] при моделировании сложного динамического поведения больших систем. Аналитические расчеты таких моделей невозможны, поэтому необходимо обращаться к моделированию Монте-Карло, и это не представляет реальных трудностей благодаря вычислительной мощности персональных компьютеров в настоящее время.

Рисунок J.10 демонстрирует моделирование методом сетей Петри многоконтурной системы безопасности, представленной на рисунке J.5. Он подобен дереву отказов, представленному в рисунке J.6, за исключением того, что ресурсы ремонта распределяются между всеми компонентами и должны быть привлечены перед началом ремонта (например, необходимые подводные системы для восстановления судна динамического расположения).

На рисунке J.10 представлена блок-схема расчета надежности, управляемая сетью Петри, которая построена на основе блок-схемы надежности на рисунке J.5 (ограничена пунктирной линией), в которой каждый блок был выполнен подстановкой стандартизированных подсетей Петри, например из библиотеки подсетей Петри. Использовались два вида подсетей Петри: опасные необнаруженные отказы (*PTs*, ООП для PT_2 и PT_5, а также *SVs*) и опасные обнаруженные отказы (для *LSs*). Таким образом, использование сетей Петри позволяет работать с очень большими моделями, состоящими из сотен компонентов.

Примечания

1 Базовая сеть Петри состоит из позиций (круги), которые представляют локальные состояния, переходов (прямоугольники), представляющих события, которые могут произойти, стрелок вверх, связывающих позиции с переходами и стрелок вниз, связывающих переходы с позициями. Метки (маленькие черные круги) помещаются в позиции, чтобы определить, какие локальные состояния фактически присутствуют в данный момент.

Метки и стрелки вверх используются, чтобы разрешить переходы, и когда переход разрешен, он может быть «запущен» (это означает, что связанное событие происходит): одна метка удаляется из каждой входной позиции и одна метка добавляется в каждую выходную позицию. Поэтому маркировка позиций (т. е. состояния моделируемой системы) изменяется.

Моментом запуска переходов могут управлять стохастические задержки (например, показательные распределения с постоянной интенсивностью отказов или ремонтов). В этом случае PN называют стохастическими сетями Петри.

2 Более подробную информацию о сетях Петри можно найти в МЭК ТС 62556:2014.

Один из датчиков давления (например, PT_1) обычно находится в рабочем состоянии (W). Если в нем происходит сбой, то этот датчик переходит в опасное необнаруженное состояние (DU) и его переменная индикатора (например, PT_1) получает значение ноль. Если выполняется контрольная проверка, то отказ обнаруживается (DD) и переменная *Nd*, которая учитывает число обнаруженных отказов, увеличивается на единицу. Если ресурс ремонта находится на месте (OL), то ремонт может начаться (R). Если ремонт завершен, то переменная индикатора (например, PT_1) возвращается к значению единица, а значение *Nd* уменьшается на единицу. Такое же моделирование применяется к трем *PTs* и двум *SVs*. Для логических решающих устройств было удалено состояние (DU), но принцип остался тем же.

Когда значение *Nd* становится положительным, (т. е. когда по крайней мере был обнаружен один отказ), то запускается процесс привлечения ресурсов ремонта (подсеть Петри «Привлечение ресурсов ремонта»). И когда это достигается (метка в M), то ресурсы переходят в места нахождения отказов для их устранения (OL). В этом случае метка из позиции OL передается в один из отказов, ожидающий ремонта, и это предотвращает одновременное выполнение других ремонтных работ. Когда ремонт закончен, то одна метка возвращается в позицию M и ресурсы могут быть переданы в местонахождение другого отказа. Этот процесс повторяется до тех пор, пока все отказы не будут устранены (*Nd* = 0) и ресурс ремонта будет расформирован.

Для моделирования виртуальных узлов блок-схемы надежности вводят глобальные утверждения. Символ «*» представляет логическое И, и символ «+» представляет логическое ИЛИ. Например, $B = A^*LS_1$ означает, что выход *B* LS_1 равен 1, когда в LS_1 нет сбоя, и его вход также равен 1. $!!S = C + G$ означает, что в многоконтурной системе безопасности сбоя нет (т. е. $S = 1$), когда в $ПСБ_1$ сбоя нет ($C = 1$) или в $ПСБ_2$ сбоя нет ($G = 1$).

Затем использование моделирования Монте-Карло позволяет формировать статистические выборки переменных *C*, *G* и *S* и получать меры безопасности, связанные с $ПСБ_1$, $ПСБ_2$ и с самой многоконтурной системой безопасности.

Как показано в рисунке J.11, можно получить пилообразные кривые. Они менее гладкие, чем полученные при вычислениях на дереве отказов, но очень похожи. Тем не менее они не должны использоваться для вычисления среднего значения неготовности, так как среднее значение неготовности может быть более точно получено непосредственно в результате моделирования Монте-Карло: среднее значение 1 – *C* дает P_1, среднее значение 1 – *G* дает P_2 и среднее значение 1 – *S* дает полное среднее значение неготовности.

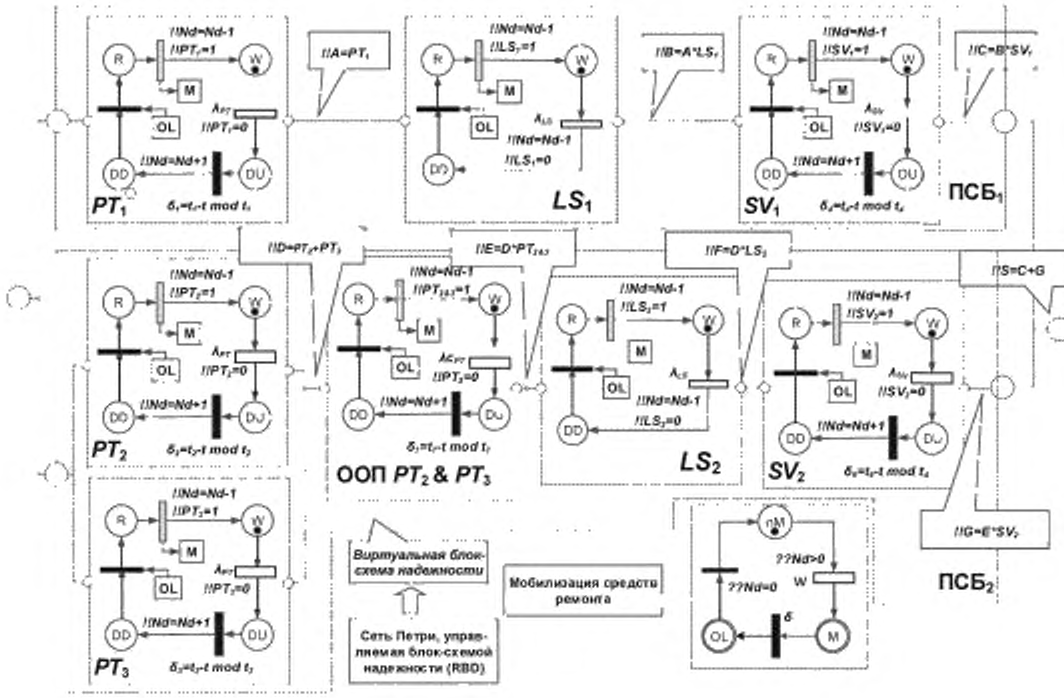


Рисунок J.10 — Моделирование привлечения ресурса ремонта

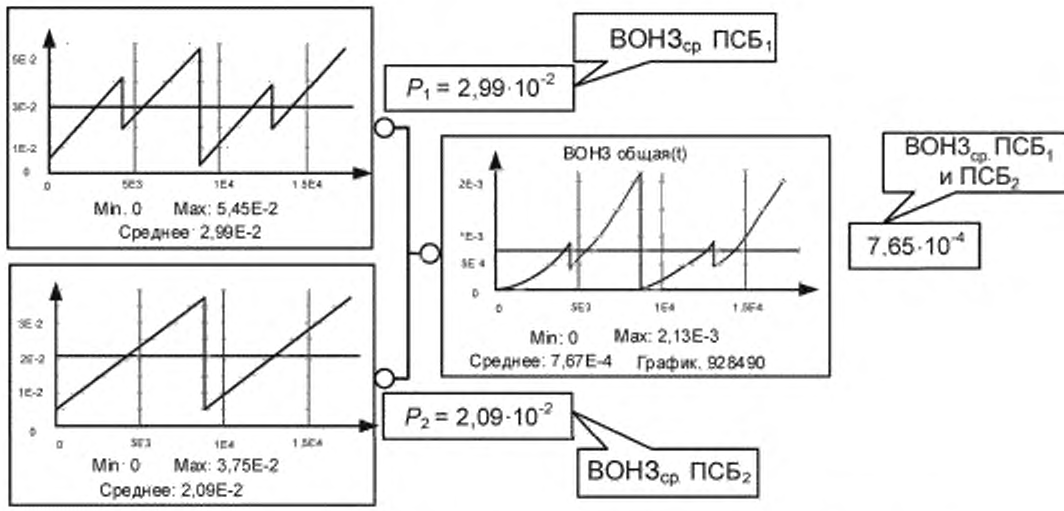


Рисунок J.11 — Пример выходного значения при моделировании методом Монте-Карло

На рисунке J.11 время привлечения ресурсов и время доступа к месту отказа равны 0. Поэтому различие с результатами рисунка J.6 связано только с совместным использованием ресурсов ремонта. Это оказывает очень небольшое влияние на P_1 и P_2 и немного большее на всю многоконтурную систему безопасности: $1/7{,}65 \cdot 10^4 = 1307$ вместо 1360. То есть в данном случае зависимость от общей команды ремонта очень небольшая, и объясняется

тем, что подход на основе дерева отказов, который рассматривает столько же команд ремонта, сколько видов отказов, соответствует случаю, когда вероятность одновременного появления двух отказов мала и/или когда времена ремонта незначительны по сравнению с интервалами испытаний.

Если время привлечения совместно используемых ресурсов не равно 0, то времена ремонта отдельных отказов возрастают. На рисунке J.12 время привлечения было установлено равным 24 ч, а задержка, необходимая для доступа к месту отказа, равна 10 ч. Тогда первый отказ отсрочена на 34 ч и другой — на 10 ч. Это влияет, главным образом, на обнаруживаемые отказы (т. е. отказы логические решающего устройства в нашем примере), что приводит почти к удвоению среднего значения неготовности $ПСБ_1$, $ПСБ_2$ и к его увеличению в 3 раза для многоконтурной системы безопасности: общее снижение риска падает до $1/2{,}19 \cdot 10^3 = 457$. Речь идет о третьем результате, полученном с помощью дерева отказов на рисунке J.6.

Другие примеры, представленные на рисунках J.7, J.8 или J.9, могут быть обработаны таким же образом.

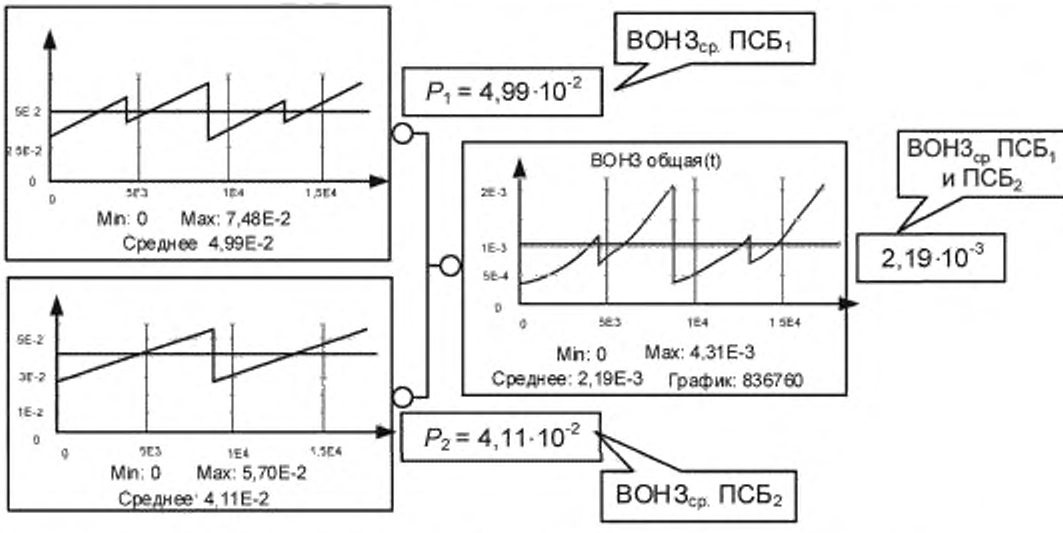


Рисунок J.12 — Влияние ремонтных работ при совместном использовании ресурсов ремонта

Приложение К
(справочное)

Принцип снижения риска настолько, насколько это практически целесообразно (принцип ALARP), и концепция приемлемого риска

К.1 Общие положения

В данном приложении рассмотрен особый принцип (ALARP), который может быть применен в процессе определения приемлемого риска и уровней полноты безопасности. Принцип ALARP сам по себе — это не метод решения задачи определения УПБ, а концепция, которая может быть применена в процессе решения этой задачи. Желающие использовать практически принципы, указанные в этом приложении, должны обратиться к [1]—[5].

К.2 Модель ALARP

К.2.1 Введение

В 3.2 приведены основные критерии, которые используют для контроля за промышленными рисками, и указано, что соответствующая деятельность должна быть направлена на то, чтобы определить:

a) риск велик настолько, что он вообще неприемлем; или

b) риск незначительный либо он может быть сведен до этого уровня; или

c) является ли риск промежуточным между оценками, указанными в перечислениях a) и b), и снижен ли он до самого низкого практичного уровня. При этом «практичность» определяется, с одной стороны, преимуществами, которые влекут за собой снижение уровня риска, и с другой стороны, стоимостью мероприятий по его снижению.

Согласно перечислению c) принцип ALARP рекомендует снижать риск до уровня «практической целесообразности» или до уровня, который является «настолько низким, насколько он практически целесообразен» (ALARP). Таким образом, если риск попадает в область, ограниченную, с одной стороны, областью неприемлемых уровней риска и областью незначительных уровней — с другой, то применение принципа ALARP приводит к тому, что результирующий риск оказывается приемлемым в конкретной ситуации. Согласно этому подходу риск может попасть в одну их трех областей: в недопустимую, приемлемую и вполне приемлемую (см. рисунок К.1).

Риск, превышающий некоторый уровень, считается недопустимым. Такой риск не может быть признан оправданным при любых нормальных обстоятельствах. Если такой риск существует, то он либо должен быть снижен настолько, чтобы попасть в область приемлемого или вполне приемлемого риска, либо должен быть устранен источник опасности.

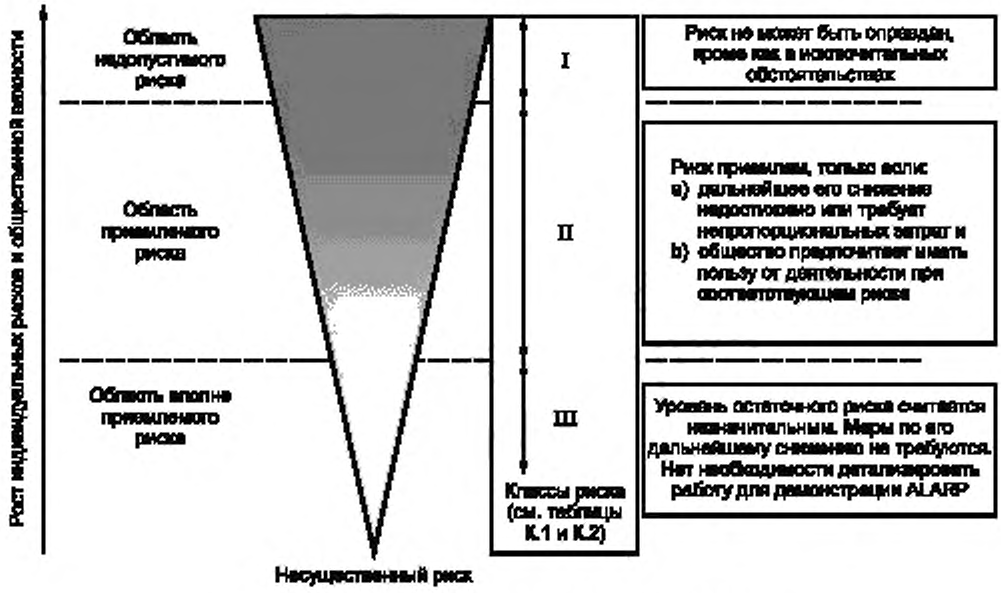


Рисунок К.1 — Приемлемый риск и принцип ALARP

Риск ниже этого уровня считается приемлемым при условии, что он был уменьшен до уровня, при котором выгода от дальнейшего его снижения не оправдана ввиду требующихся для этого больших затрат и при условии, что для управления этим риском применены все соответствующие общепринятые стандарты. Чем выше риск, тем обычно больше расходы по его сокращению. Риск, сниженный таким образом, можно рассматривать как «сниженный до практически целесообразного уровня» (ALARP).

В области, расположенной ниже области допустимых значений, уровни риска считаются настолько несущественными, что контролирующий орган не требует дальнейших улучшений. Это широкая область, риски в которой малы по сравнению с ежедневно испытываемыми нами рисками, не требует детальных исследований для демонстрации ALARP; однако необходимо сохранять бдительность, чтобы быть уверенным в том, что риск остается на прежнем уровне.

Концепцию ALARP можно применять и при качественном, и при количественном способе задания риска. В К.2.2 рассмотрен метод, используемый при количественном задании риска. (В приложении С приведен полуколичественный метод, а в приложениях D и Е — качественные методы определения необходимого снижения риска при конкретном источнике опасности. В рассмотренных методах для принятия решения может быть использована концепция ALARP.)

При применении принципа ALARP необходимо всегда быть уверенным, что все принятые предположения обоснованы и документально оформлены.

К.2.2 Задание приемлемого риска

Для применения принципа ALARP необходимо предварительно определить границы трех областей, показанных на рисунке К.1, значения которых выражены вероятностью возникновения события и его последствиями. Такое определение обычно бывает результатом обсуждения и соглашения между заинтересованными сторонами (например, между регулирующими органами в области безопасности, теми, действия которых приводят к появлению риска, и теми, кто этому риску подвергается).

Чтобы использовать принцип ALARP, надо установить соответствие между последствиями риска и приемлемой частотой его возникновения, что может быть сделано, введя классы риска. В таблице К.1 в качестве примера приведены три класса (I, II, III) для разных частот возникновения риска и разных вариантов его последствий. В таблице К.2 дана интерпретация каждого из классов риска на базе концепции ALARP. Описание каждого из классов риска выполняется на основе рисунка К.1. Подразумевается, что риски, определенные внутри каждого из классов, — это риски, по отношению к которым уже приняты меры по их сокращению. Согласно рисунку К.1 можно выделить следующие три класса рисков:

класс I — недопустимая область;

класс II — область применения концепции ALARP;

класс III — наиболее приемлемая область.

Таблица, подобная таблице К.1, обычно создается для каждой конкретной ситуации или для конкретной подотрасли промышленности, принимая во внимание широкий круг социальных, политических и экономических факторов. Каждому виду последствий ставятся в соответствие вероятность и таблица с классами риска. Например, «вполне вероятен» в таблице К.1 может означать событие, которое возникает с частотой, превышающей 10 раз в год. Его критическим последствием может быть один смертельный исход, и/или многочисленные телесные повреждения, или несколько случаев профессиональных заболеваний.

Задав допустимый риск, можно определить уровни полноты безопасности функций безопасности ПСБ с помощью, например, одного из методов, описанных в приложениях С—F.

Таблица К.1 — Пример классификации инцидентов

Возможность инцидента	Класс риска			
	Катастрофические последствия	Критические последствия	Незначительные последствия	Пренебрежимо малые последствия
Вполне вероятен	I	I	I	II
Вероятен	I	I	II	II
Возможен	I	II	II	II
Маловероятен	II	II	II	III
Невероятен	II	III	III	III
Невозможен	II	III	III	III

Окончание таблицы К.1

Примечания

1 Интерпретацию классов риска с I по III см. в таблице К.2.

2 Фактическое заполнение таблицы индексами классов риска I, II и III зависит от конкретной ситуации, а также от того, какие фактические значения вероятности мы присваиваем понятиям «вероятно», «возможно» и т. д. Таким образом, таблицу К.1 следует рассматривать как иллюстрацию того, каким образом подобная таблица может заполняться, а не как вариант для дальнейшего использования.

Таблица К.2 — Интерпретация классов риска

Класс риска	Интерпретация
Класс I	Неприемлемый риск
Класс II	Нежелательный риск, допустимый, только если его дальнейшее снижение практически невозможно или если связанные с этим расходы непропорционально велики по сравнению с достигаемым результатом
Класс III	Пренебрежимо малый риск
Примечание — Связь между УПБ и классом риска отсутствует. УПБ определяется снижением риска, связанным с конкретной функцией безопасности ПСБ (см. приложения B—F).	

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 61511-1:2016	IDT	ГОСТ Р МЭК 61511-1–2018 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

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

Ключевые слова: безопасность функциональная, жизненный цикл систем, приборные системы безопасности, риск, полнота безопасности, слои защиты, принцип ALARP, граф риска

БЗ 11—2017/56

Редактор *Р.Г. Говердовская*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Половой*

Сдано в набор 09.08.2018. Подписано в печать 04.09.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 9,30. Уч.-изд. л. 8,42.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе 11.
www.jurisizdat.ru gost.e-ecolog.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
123001 Москва, Гранатный пер., 4 gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru