ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ЕН 15233 – 2013

МЕТОДОЛОГИЯ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ ЗАЩИТЫ ДЛЯ ПОТЕНЦИАЛЬНО ВЗРЫВООПАСНЫХ СРЕД

EN 15233:2007
Methodology for functional safety assessment of protective systems for potentially explosive atmospheres

(IDT)

Издание официальное

Москва
Стандартинформ
2013

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой национальной организацией «Ех-стандарт» (АННО « Ех-стандарт») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 403 «Оборудование для взрывоопасных сред (Ех-оборудование)»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013г. № 1723-ст

4 Настоящий стандарт идентичен региональному стандарту ЕН 15233:2007 «Методология оценки функциональной безопасности систем защиты для потенциально взрывоопасных сред» (EN 15233:2007 «Methodology for functional safety assessment of protective systems for potentially explosive atmospheres»)

5 ВВЕДЕН ВПЕРВЫЕ

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

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

© Стандартинформ, 2013

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
2 Нормативные ссылки
3 Термины и определения
4 Общие требования
4.1 Основное понятие
4.2 Степень оценки функциональной безопасности
4.3 Необходимая информация
5 Методика оценки функциональной безопасности
5.1 Принцип
5.2 Описание системы защиты
5.3. Выявление неисправностей
5.4 Определение функциональной безопасности
5.5 Оценка функциональной безопасности
6 Документация
6.1 Документация для изготовителя
6.2 Информация, которую необходимо предоставить потребителю
Приложение А (справочное) Пример оценки функциональной безопасности
Приложение В (справочное) Методы выявления отказов и оценки функциональной безопасности
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Введение

Цель настоящего стандарта – представить принципы согласованной систематической процедуры оценки функциональной безопасности при проектировании и изготовлении систем защиты.

В справочном приложении А приведены методы оценки функциональной безопасности и надежности.

В справочном приложении В приведены примеры функциональной оценки безопасности системы защиты.

В инструкциях по эксплуатации содержится ссылка на необходимость оценки функциональной безопасности, а в документации указаны возможные дополнительные меры предосторожности.

Создание общей методологии оценки функциональной безопасности, надежности и эффективности при эксплуатации систем защиты отвечает интересам изготовителей и потребителей. Таким образом, оценка функциональной безопасности является инструментом, обеспечивающим необходимую связь между изготовителями и потребителями, однако в настоящем стандарте рассматриваются только аспекты, связанные непосредственно с деятельностью изготовителей.

Задача комплексной взрывобезопасности – предупредить образование взрывоопасной среды, а также возникновение источников воспламенения, а в случае возникновения взрыва – немедленно остановить его и/или ограничить его последствия. В связи с этим проектирование и создание систем защиты должно осуществляться после необходимого анализа возможных неисправностей в процессе эксплуатации, ограничивающих или блокирующих способность системы остановить взрыв. Следовательно, оценка функциональной безопасности – абсолютно необходимый процесс.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Methodology for functional safety assessment of protective systems for potentially explosive atmospheres

Methodology for functional safety assessment of protective systems for potentially explosive atmospheres

Дата введения – 2015–07–01

1 Область применения

Настоящий стандарт содержит руководство по процедуре и информации, необходимым для проведения оценки функциональной безопасности при проектировании системы защиты.

Цель настоящего стандарта – предоставить помощь техническим комитетам по стандартизации, ответственным за отдельные группы систем защиты, в подготовке стандартов по безопасности. Такие стандарты должны быть единообразными, насколько это возможно, и должны включать в себя базовую структуру оценки функциональной безопасности, как сформулировано в настоящем стандарте.

При отсутствии стандартов для конкретной системы защиты изготовитель должен использовать настоящий стандарт для оценки функциональной безопасности данной системы защиты.

При выполнении этой процедуры для обеспечения достаточного уровня функциональной безопасности необходимо учитывать следующую информацию:

a) использование по назначению;

b) возможные неисправности в процессе эксплуатации;

c) надежность систем защиты;

d) неправильное применение, которое можно предупредить.

Достаточный уровень функциональной безопасности характеризуется выполнением следующих требований:

1) Система способна остановить взрыв на самой ранней стадии или уменьшить последствия взрыва до приемлемого уровня.

2) В случае отказов, неисправностей или помех[1)] способность выполнять функцию сохраняется, например, за счет применения безотказной или резервной системы.

Настоящий стандарт не распространяется на идентификацию потенциальных источников воспламенения.

Примечание 1 – Идентификация потенциальных источников воспламенения рассматривается в ЕН 15198 [1].

Настоящий стандарт рассматривает только функциональное поведение систем защиты, т. е. опасности, связанные с неисправностями (например ложным срабатыванием), не рассматриваются.

В настоящем стандарте не приведены конкретные методы анализа условий отказа или специальные требования для данного вида системы защиты (см. ЕН 1127-1 [2]). Приведена только методология оценки функциональной безопасности.

В настоящем стандарте содержатся рекомендации для принятия решений по всем видам систем защиты, упоминаемым в директиве 94/9/ЕС, но не указаны средства подтверждения соответствия данного вида системы защиты.

Примечание 2 – Для оборудования применяют стандарт ЕН15198 [1] , так как процедура и информация, необходимые для оценки опасности воспламенения, отличаются от описанной выше процедуры.

[1)] Помеха - это любое воздействие в режиме нормальной эксплуатации, способное помешать нормальному функционированию системы, например, воздействие электромагнитных излучений, тепла, пламени и волны сжатия.

2 Нормативные ссылки

Приведенный ниже стандарт является обязательным для применения настоящего стандарта. Для стандартов с датой опубликования применяют только указанные издания. В тех случаях, когда дата опубликования не указана, применяется последнее издание приведенного стандарта (включая любые поправки).

ЕН 13237–2003 Потенциально взрывоопасная атмосфера. Термины и определения по оборудованию и защитным системам, предназначенным для использования в потенциально взрывоопасной атмосфере (EN 13237:2003 Potentially explosive atmospheres – Terms and definitions for equipment and protective systems intended for use in potentially explosive atmospheres)

3 Термины и определения

В настоящем стандарте применены термины по ЕН 13237–2003, а также следующие термины с соответствующими определениями.

3.1 **отказ (failure):** Событие или нерабочее состояние, характеризуемое неспособностью любого компонента системы или части компонента или любого функционального блока выполнять свою функцию.

[ИСО/МЭК Руководство 73:2002] [3]

3.2 **функциональная безопасность** (functional safety): Часть общей безопасности, при использовании по назначению, с учетом функционирования и целостности системы защиты, включая любые устройства обеспечения безопасности, влияющие на характеристики системы защиты.

Примечания

1 Понятие «функциональная безопасность» охватывает все аспекты, когда безопасность зависит от правильного функционирования системы защиты и других технических систем, имеющих отношение к безопасности.

2 Данное определение отличается от определения, приведенного в ЕН 61508-4 [4], что позволяет отразить различия в терминологии, используемой в сфере взрывобезопасности.

3.3 **система защиты (protective system):** Устройство, не являющееся компонентом оборудования, предназначенное для незамедлительной остановки зарождающегося взрыва и/или ограничения диапазона его влияния, продаваемое отдельно.

[ЕН 13237:2003, А.5]

3.4 **определение функциональной безопасности** (functional safety estimation): Определение вероятности возникновения отказов, нарушающих функциональную безопасность системы защиты

3.5 **оценка функциональной безопасности** (functional safety evaluation): Процедура, позволяющая установить соответствие функциональной безопасности системы защиты установленным критериям определения готовности к эксплуатации.

4 Общие требования

4.1 Основное понятие

Оценка функциональной безопасности представляет собой ряд логических этапов (см. рисунок 1), позволяющих проектировщикам и инженерам по технике безопасности систематически проводить оценку функционирования системы защиты или ее части. Цель оценки функциональной безопасности – обеспечение необходимого уровня функциональности и надежности в соответствии с требованиями современного уровня развития технологии, техническими и экономическими требованиями на время проектирования.

Процедура оценки состоит из следующих четырех этапов:

a) описание системы защиты (5.2);

b) выявление неисправностей (5.3);

c) определение функциональной безопасности (5.4);

1) функциональные возможности;

2) надежность;

d) оценка функциональной безопасности (5.5).

Эти четыре этапа являются основой для принятия решения о том, достигнут ли намеченный уровень функциональной безопасности, необходимый для использования по назначению. Результат оценки должен быть подробно описан в технической документации (см. раздел 6).

Если необходимое функционирование и уровень надежности не достигнуты, требуется внести улучшения в систему защиты или определить соответствующее использование по назначению.

Примечание – Выбор применимых мер не рассматривается в настоящем стандарте.

Если оценку проводит изготовитель, результат оценки должен быть подробно описан в технической документации (см. раздел 6).

Решения при проведении оценки функциональной безопасности должны быть подтверждены результатами качественных методов оценки, которые, при необходимости, должны дополняться результатами количественных методов.

4.2 Степень оценки функциональной безопасности

Оценку системы защиты проводят на основе информации, указанной в 4.3.

Оценка функциональной безопасности должна ограничиваться рассмотрением использования по назначению, а также случаев неправильного использования, которые можно достаточно обоснованно прогнозировать при эксплуатации конкретной системы защиты.

Примечание – Достаточно обоснованно прогнозируемые случаи неправильного использования – это неправильная эксплуатация системы защиты оператором из-за небрежности или неправильного понимания. Неправильная эксплуатация не относится к режиму нормальной эксплуатации. Неправильное использование не является частью нормального режима работы. Намерение не является частью предсказуемого неправильного применения.

4.3 Необходимая информация

Информация, необходимая для осуществления оценки функциональной безопасности, должна включать в себя , в соответствии с обстоятельствами:

a) использование по назначению;

b) характеристики безопасности, использовавшиеся при проектировании системы защиты;

c) требования к техническому обслуживанию;

d) фактические и ожидаемые условия окружающей среды;

e) соответствующие проектировочные чертежи;

f) результаты проектных расчетов, проведенных проверок;

а также следующие данные, при их наличии:

g) протоколы испытаний;

h) сведения об авариях;

i) публикации по соответствующим аспектам безопасности.

При отсутствии сведений об авариях для данной системы защиты необходимо использовать данные для подобных систем защиты. Отсутствие аварий, небольшое число аварий или незначительные аварии не являются основанием для допущения наличия низкого уровня риска.

Возможные дополнительные меры предосторожности должны быть оформлены документально.

Информация должна обновляться в ходе проектирования и при внесении изменений в существующую конструкцию.

Для проведения количественной оценки необходимо использовать данные из баз данных, руководств, технических условий лабораторий и изготовителей, при условии, что эти данные пригодны для проведения оценки. Любые неточности в данных должны быть документально оформлены.

Примечание – Эти данные используются для определения ожидаемых эксплуатационных требований к надежности, ремонтопригодности, долговечности, возможности утилизации, неопасным отказам и отказоустойчивости и к маркировке, предупреждающим надписям, обозначению, возможности контроля и к инструкциям. Данные, основанные на согласованном экспертном заключении, полученном косвенным путем из опыта, а не на данных измерений, допускается использовать в дополнение к качественной оценке.

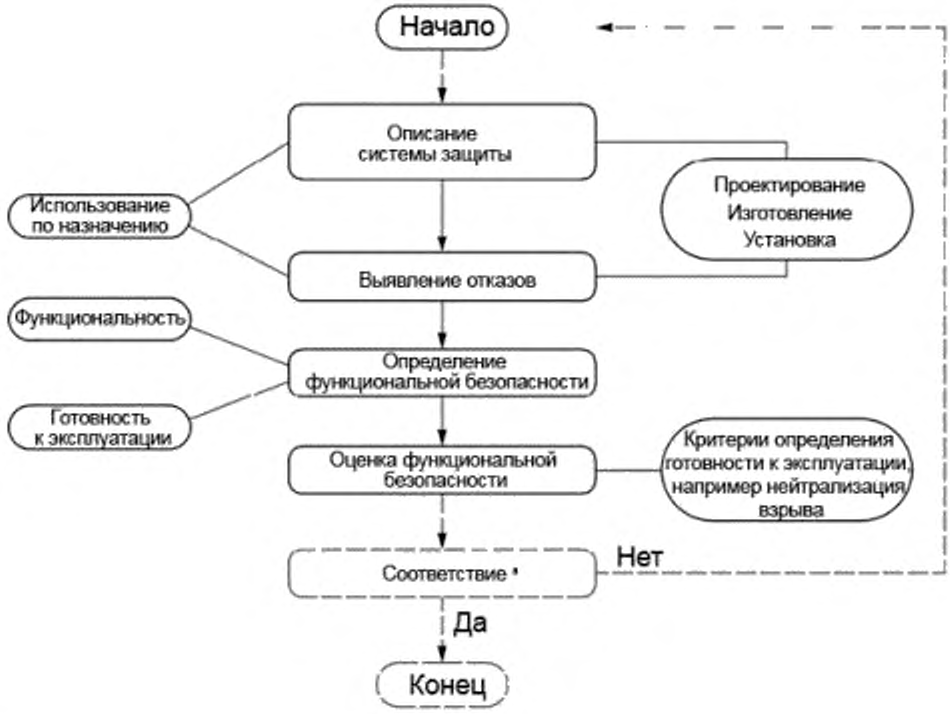
5 Методика оценки функциональной безопасности

5.1 Принцип

Основные этапы процедуры оценки функциональной безопасности представлены на рисунке 1. Оценка состоит из четырех этапов, в ходе которых рассматривается информация, помещенная в блоки овальной формы.

В ходе оценки также необходимо рассматривать требования к техническому обслуживанию.

Изготовитель должен включать все необходимые требования к техническому обслуживанию в инструкции по эксплуатации, а также рассматривать отсутствие технического обслуживания, необходимого для использования по назначению.



[a] Оценка соответствия не входит в оценку функциональной безопасности

Примечание – Этапы, указанные в блоках из пунктирных линий, не рассматриваются в настоящем стандарте

Рисунок 1 – Оценка функциональной безопасности при проектировании систем защиты

5.2 Описание системы защиты

Поэтапную оценку (в соответствии с блок-схемой, представленной на рисунке 1) проводят с учетом функции системы защиты и видов взрывов.

При рассмотрении использования по назначению необходимо проанализировать следующие аспекты:

a) срок службы системы защиты;

b) ограничения с точки зрения эксплуатации, времени и пространства;

c) точное определение функции;

d) выбор материалов для изготовления;

e) эксплуатационные данные, срок службы и конфигурация;

f) описание видов взрывов;

g) ограничения технологических условий;

h) требования к техническому обслуживанию.

5.3. Выявление неисправностей

5.3.1 Общие положения

Как правило, систему защиты оценивают по наличию в ней потенциальных источников отказов. С этой целью необходимо использовать функциональный анализ и анализ логических состояний.

Системы защиты подразделяются на следующие группы:

a) пассивные системы (например пламегаситель, система вентиляции),

b) активные системы (например система подавления).

Пример использования такого подхода приведен в приложении А.

Возможные отказы необходимо анализировать с помощью функционального и систематического анализа и рассматривать по отдельности для всего срока службы.

Примечание – Перечисленные виды неисправностей приведены в качестве примеров. Могут возникать другие неисправности.

5.3.2 Оценка

5.2.3.1 Проектирование и изготовление

На этапе планирования и проектирования необходимо учитывать следующее:

a) должно быть достигнуто соответствие использованию по назначению, например:

1) достаточная теплопроводность для пламегасителей;

2) эффективный сброс давления в выпускных устройствах;

3) достаточная эффективность подавления в системах подавления.

b) защитная система должна иметь адекватные физические размеры. Неисправности могут быть вызваны следующими причинами:

1) недостаточное сопротивление напору,

2) недостаточная термостойкость,

3) недостаточная виброустойчивость и ударопрочность,

4) недостаточная устойчивость к старению или коррозии.

c) необходимо избегать неправильного размещения установки, неправильного монтажного положения или неправильного метода установки с учетом характера взрыва.

d) для выбора правильного режима эксплуатации необходимо учитывать характеристики процесса, температуру окружающей среды, давление окружающего воздуха, а также пороговые значения срабатывания или чувствительность.

e) использование несоответствующего компьютерного обеспечения и аппаратуры управления (аппаратных средств).

f) устойчивость аппаратных средств к электромагнитным помехам.

g) дополнительные средства для безотказного функционирования.

h) при нарушении энергоснабжения использование системы по назначению должно поддерживаться в соответствии с требованиями.

5.3.2.2 Установка

Чтобы предоставить необходимую информацию об установке, изготовитель должен учитывать следующие возможные неисправности:

a) отсутствие или неполный анализ последствий использования системы по назначению (например вакуумные выключатели, опасные зоны,

расположенные перед устройствами сброса давления, сила отдачи, риск получения травм);

b) недостаточность уплотнения или возможность обхода;

c) плохая электропроводка (например короткое замыкание, обрыв в цепи, перегрузка или замыкание на землю);

d) недостаточное электроснабжение и/или резервное энергоснабжение аппаратуры управления и индикации

5.3.2.3 Требования к рабочим характеристикам и техническому обслуживанию

Необходимо рассмотреть неисправности, которые могут возникнуть в процессе эксплуатации и технического обслуживания системы защиты. Изготовитель должен сообщить потребителю, каким образом можно предотвратить эти неисправности. К неисправностям, которые могут возникнуть в процессе эксплуатации и технического обслуживания, относят следующие:

a) загрязнение;

b) неправильное или в недостаточном объеме проведение работ персоналом (неправильная эксплуатация, неправильный монтаж, неправильное техническое обслуживание, неумышленное вмешательство в работу оборудования);

c) отображение сообщений о неисправности и отсутствие аварийной остановки.

Подобные ситуации и возможные неисправности должны быть четко описаны в инструкциях по эксплуатации.

5.3.2.4 Изменение

После внесения любых изменений, связанных с безопасностью, система защиты должна рассматриваться как новая система. В этом случае необходимо провести повторную оценку.

5.4 Определение функциональной безопасности

5.4.1 Общие положения

После выявления неисправности необходимо определить функциональную безопасность системы защиты путем определения вероятности возникновения неисправности.

Для определения функциональной безопасности может применяться качественный, полуколичественный или количественный анализ в зависимости от роли системы защиты в снижении вероятности возникновения неисправности и / или от сложности системы и устройств, связанных с безопасностью.

Требуемая эффективность системы защиты должна оцениваться по следующим показателям:

a) функционирование, т. е. способность выполнять функции, необходимые для использования системы по назначению (например, остановить зарождающийся взрыв, снизить давление взрыва);

b) готовность к эксплуатации, т. е. надежность при выполнении этих функций (по требованию или своевременно).

Способность осуществлять требуемую функцию может частично оцениваться количественно по данным о надежности и / или отказоустойчивости структуры системы.

Необходимо определить и оценить надежность каждого выявленного параметра, способного привести к сбою в осуществлении защитной функции системы, т. е. к нарушению требования к функциональности и готовности к эксплуатации.

5.4.2 Функциональность

Определение функциональной безопасности включает в себя определение технических и рабочих неполадок, исходя из частоты возникновения отказов (например, прогнозирование функционирования системы при отказах аппаратной части, во время эксплуатации и при неправильной эксплуатации, возможных в различных режимах эксплуатации системы и при проведении ее технического обслуживания, а также во время самого события).

Функциональная безопасность системы должна оцениваться по наиболее неблагоприятным ситуациям, т. е. в случаях, когда система защиты не выполняет функцию обеспечения безопасности при заданных характеристиках взрыва. Если нет возможности провести такую оценку, функциональная безопасность должна оцениваться, исходя из ситуаций, в которых возникает частичное отрицательное воздействие на рабочие характеристики системы, например, когда система способна частично уменьшить опасность, возникающую при взрыве, т. е. частично снизить избыточное давление взрыва.

Необходимо оценить, насколько каждый выявленный вид отказа (см. 5.3) способен снизить производительность, и относительную вероятность его возникновения. При этом необходимо оценить и установить роль различных параметров, оказывающих негативное влияние на функционирование системы, например:

a) состояние и рабочие режимы (например требования к установке и эксплуатации, требования к техническому обслуживанию, испытания, возврат исходное положение, блокировки, перепускные устройства);

b) требуемое время срабатывания и длительность реакции (время срабатывания датчика исполнительного механизма и длительность предупредительного действия);

c) функционирование при неисправности и состояния неисправности;

d) безотказное функционирование и надежные состояния;

e) контроль и возможность выявления опасных неисправностей и связанные с этим действия;

f) пороги чувствительности системы защиты с учетом характеристик безопасности;

g) проектные параметры и параметры управления;

h) структура системы, резервирование, отказоустойчивость;

i) взаимодействие и влияние компонентов системы и органов управления, связанных с безопасностью, и устройств защиты;

j) методы проверок / испытаний;

k) зависимость / независимость функциональности системы защиты от других систем;

l) систематические / не выявляемые при испытаниях отказы (см. примечание, 5.4.3,).

5.4.3 Оценка готовности к эксплуатации

Требования к готовности к эксплуатации, исходя из критерия надежности функционирования, должны быть определены и оценены для устройств, связанных с обеспечением безопасности и от которых зависят рабочие характеристики системы защиты.

На этой основе (допускается проводить оценку простых предупреждающих систем, не связанных с системами и устройствами безопасности, соответствие которых требуемым функциям было доказано опытным путем или с помощью расчетов (т. е. путем подтверждения в процессе использования).

При невозможности подтвердить документально предыдущее использование или для новой или более сложной системы, включая системы управления и устройства, связанные с безопасностью, необходимо использовать более комплексный подход, применяя соответствующие методы расчета

надежности (например в соответствии со стандартами серии ЕН 61508 [4], ЕН ИСО 13849-1[5], ЕН 62061[6]).

Для каждой функции безопасности необходимо рассмотреть частоту возникновения обстоятельств, при которых функция безопасности не будет выполняться (частота отказов или вероятность отказа по требованию), при этом важно учитывать следующее:

a) рабочий режим (режим по запросу / непрерывный режим);

b) предполагаемая частота запросов;

c) структура / структурные ограничения;

d) систематические отказы *см. 5.4.3 , Примечание);

Примечание – Учитывают также отказы, которые могут быть не выявлены испытательными или контрольными устройствами, отказы из-за ошибок проектирования, ошибки программного обеспечения, ошибки из-за различия сигналов и неправильной установки.

e) отказы по общей причине;

f) среднее время ремонта;

g) интервалы между проверками / испытаниями;

h) диагностика и доля безопасных отказов.

Результат оценки готовности к эксплуатации должен быть представлен в виде количественной характеристики надежности, т. е. в виде показателя вероятности отказа по требованию или показателя вероятности опасных отказов в час (т. е. частота отказов) при необходимости, при этом оба показателя определяются отдельно для разных функций и для функционирования за системы защиты в целом.

Эти результаты потребуются для оценки функциональной безопасности, а также потребуются потребителю, чтобы проверить, как система защиты будет способствовать общей оценке риска взрыва и создавать предпосылки для снижения общего риска взрыва.

Следовательно, эти результаты должны содержаться в документации.

5.5 Оценка функциональной безопасности

Необходимо оценить приемлемость определенной функциональной безопасности. Следовательно, критерии определения готовности к эксплуатации должны быть установлены заранее на основе использования по назначению. Эти критерии могут быть качественными, полуколичественными или количественными.

Для оценки вероятности критерии определения готовности к эксплуатации могут быть качественными, полуколичественными или количественными.

Сравнение определенной вероятности отказа системы защиты по требованию с заданными критериями определения готовности к эксплуатации покажет, существует ли необходимость применения мер по снижению риска.

При определении мер по снижению риска необходимо в первую очередь рассматривать компоненты или свойства системы защиты, определяющие совокупный риск. Следует рассмотреть каждую установленную меру по снижению риска, проанализировав преимущества для обеспечения безопасности и целесообразность применения каждой меры.

6 Документация

6.1 Документация для изготовителя

В документацию системы защиты должны входить следующие документы.

В документации по оценке функциональной безопасности должно содержаться описание использованной процедуры оценки и полученных результатов. В этой документации указывают следующее:

а) данные о системе защиты, оценка которой проводилась (например технические требования, предельные значения, использование по назначению, е эксплуатационные характеристики) (см. 4.2 и 5.2);

b) любые принятые допущения (например, нагрузки, силы, коэффициенты безопасности);

c) инструкции по эксплуатации согласно перечислениям a), b), c), d) 4.3;

d) дополнительную информацию, на основе которой проводилась оценка функциональной безопасности (см. 4.3);

e) использованные данные и ссылки на источники (например базы данных, записи об авариях, опыт, полученный при увеличении функциональной безопасности на схожем оборудовании) (необходимо учитывать неточность использованных данных и ее влияние на оценку функциональной безопасности);

f) выявленные отказы (см. 5.3);

g) результат окончательного определения функциональной безопасности (см. 5.4);

h) меры безопасности, принятые для устранения выявленных отказов или повышения функциональной безопасности (например из стандартов или других технических требований);

i) результат заключительной оценки функциональной безопасности (см. 5.5).

6.2 Информация, которую необходимо предоставить потребителю

Потребителю должна быть предоставлена информация, указанная в перечислениях a), d), h) и i) 6.1.

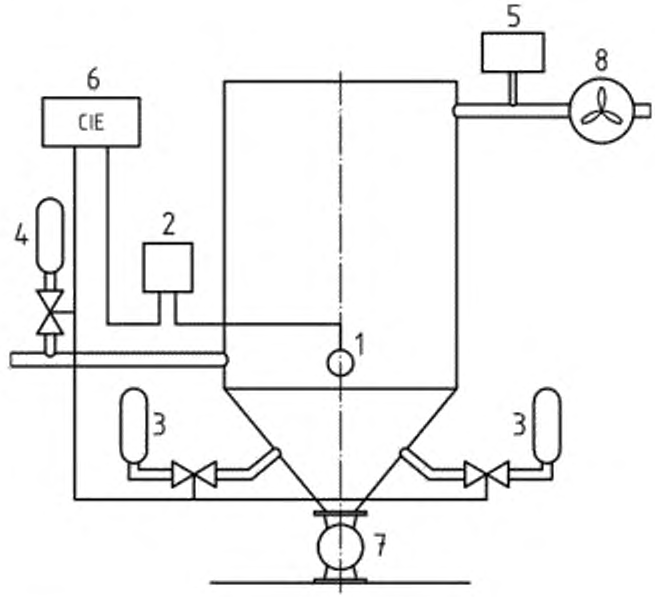
Приложение А

(справочное)

Пример оценки функциональной безопасности

А.1 Введение

Ниже приведен пример оформления результатов оценки функциональной безопасности на основе использования анализа характера, последствий и важности отказов



Обозначения:

1 – датчик давления, соединенный с анализатором,

2 – анализатор для датчика давления;

3 – огнетушители большой производительности для подавления взрыва в фильтровальной установке;

4 – огнетушитель большой производительности для изоляции фильтровальной установки от технологических установок, расположенных за фильтром

5 – оборудование для контроля концентрации пыли

6 – оборудование контроля и индикации

7 – шлюзовой затвор

8 – вентилятор

Примечание – Этот пример условный и неполный, поэтому его необходимо рассматривать только в качестве иллюстрации.

Рисунок А.1 – Подавление взрыва и система изоляции фильтровальной установки

На рисунке А.1 изображены самые важные компоненты системы подавления взрыва и системы изоляции, установленной на фильтровальной установке. Система работает следующим образом:

a) В случае взрыва в фильтровальной установке происходит увеличение давления, которое регистрируется датчиком давления. Изменения давления с течением времени, зарегистрированные датчиком давления, непрерывно анализируются анализатором. По достижении аварийного уровня (определенного значения давления взрыва в течение определенного периода времени) анализатор направит сигнал в блок управления.

b) Блок управления приводит в действие два огнетушителя большой производительности, установленные на фильтровальной установке, чтобы подавить взрыв на этом участке.

c) Одновременно с этим огнетушитель большой производительности, установленный в воздуховоде к фильтровальной установке, срабатывает, чтобы остановить взрыв, что позволяет предотвратить распространение взрыва на оборудование, подключенное к фильтрованной установке.

При взрыве в фильтровальной установке также можно отключить взрывобезопасный поворотный клапан, расположенный на выходном отверстии фильтровальной установки, но в приведенном примере это не рассматривается.

Таким образом, действие системы защиты начинается внутри фильтровальной установки при обнаружении слишком высокой интенсивности нарастания давления, свидетельствующей о возможности взрыва, и завершается срабатыванием огнетушителя большой производительности.

В случае нарушения электроснабжения включаются аккумуляторы системы взрывозащиты, что позволяет поддерживать электроснабжение в течение 4 ч. Потеря функциональных способностей по истечении этого периода (4 ч) не рассматривается. При коротком замыкании, разрыве цепи и т. д. система переведет процесс в безопасное состояние. При анализе не рассматривается остаточный риск возникновения взрыва после остановки технологического процесса.

А.2 Количественный анализ функций безопасности

Блок схема надежности для этой функции приведена на рисунке А.2. Вероятность отказа по требованию представлена в таблице А.1.

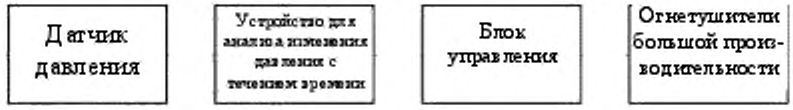


Рисунок А.2 – Блок-схема функционирования системы

А.3 Технические требования к системе

Функция системы заключается в том, чтобы открыть откидной клапан огнетушителя при поступлении сигнала от датчика / устройства для анализа.

Самыми важными элементами в системе подавления взрыва и изоляции являются датчик, блок управления и огнетушитель большой производительности, поэтому в настоящем примере будут рассматриваться только эти элементы системы. Предполагается, что система не способна выполнять функцию обеспечения безопасности при выходе из строя одного из огнетушителей большой производительности (способность системы подавлять взрыв может сохраняться при слабых взрывах; необходимость в изоляции может отсутствовать, если воспламенение в фильтре произошло на значительном расстоянии от точки соединения воздуховода с фильтровальной установкой. Пламя будет погашено системой подавления в фильтровальной установке).

Предполагается, что частота включений системы по требованию будет составлять один раз в год. Взрыв пыли может быть вызван либо разрядом электростатического электричества, либо горящими частицами, попадающими в фильтр.

А.4 Огнетушители большой производительности

А.4.1 Общие положения

Огнетушители большой производительности являются важной частью системы подавления взрыва и изоляции. В гасителях, рассматриваемых в настоящем примере, используются откидные клапаны с электромеханическим приводом. В результате разряда из конденсатора включается моментный

электродвигатель, что вызывает разблокировку откидного клапана. В контейнере с огнегасящим веществом, соединенном с клапаном, с помощью азота нагнетается давление до 60 бар. Под действием азота откидной клапан открывается, и огнегасящее вещество поступает через насадку в зону, которой необходима защита. Схема моментного двигателя и разблокировки продублирована в устройстве подавления взрыва, что создает резервную систему. Как основная, так и резервная схема моментного двигателя и разблокировки находятся в рабочем состоянии.

Для огнетушителя большой производительности использовали анализ характера, последствий и важности отказов. Всего было использовано 77 разных элементов. Приведенные ниже данные о частоте отказов являются фиктивными.

А. 4.2 Частота отказов элементов огнетушителя большой производительности

Проводилась оценка частоты отказов для каждого элемента (примеры приведены в таблице А.1. Частота отказов показывает число отказов на миллион часов эксплуатации.

Таблица А.1 – Примеры частоты отказов компонентов огнетушителя большой производительности

Идентификационный номер	Описание компонента	Число компонентов	Частота отказов (на элемент)	Общая частота отказов
1	Встроенный фильтр	1	0,300	0,300
5	Корпус	1	0,040	0,040
6	Откидной клапан	1	0,040	0,040
7	Вал	1	0,100	0,100
9	Стопорный штифт	1	0,150	0,150
15	Плоская прокладка	1	0,140	0,140
41	Цилиндрический болт	8	0,008	0,064
43	Уплотнительная шайба	2	0,140	0,280
51	Манометрический выключатель	1	1,100	1,100

А.4.3 Последствия и важность отказов

Были рассмотрены потенциальные последствия каждой неисправности. Важность отказа часто оценивают с помощью следующей классификации:

– Уровень важности 1 – очень серьезная неисправность: отказ всей системы;

– Уровень важности 2 – серьезная неисправность: непосредственное повреждение системы отсутствует;

– Уровень важности 3 – менее серьезная неисправность: незначительное влияние на функционирование системы;

– Уровень важности 4 – незначительная неисправность: не влияет на функционирование системы.

В документации по проведению анализа характера, последствий и важности отказов необходимо описать последствия и важность отказов в соответствии с приведенной классификацией (см. таблицу А.2).

Таблица А.2 – Последствия и важность отказов компонентов огнетушителя большой производительности

Идентификационный номер	Компонент	Функции	Тип отказа	Частота отказов (x 10^{6}) (в час)	Последствия отказа(ов)	Уровень важности	Комментарии
2	Встроенный фильтр	Фильтрует азот во время заполнения	Засорение	0,300	Заполнение невозможно	4	Контролируется
5	Корпус	Содержит все функциональные элементы	Трещина, скол	0,040	Потеря давления	2	Контролируется
6	Отводной клапан	Герметизирует контейнер, находящийся под давлением	Трещина, скол	0,040	Потеря давления	2	Контролируется

Продолжение таблицы А.2

Идентификационный номер	Компонент	Функции	Тип отказа	Частота отказов (x 10^6) (в час)	Последствия отказа(ов)	Уровень важности	Комментарии
7	Вал	Ось вращения для откидного клапана	Трещина	0,090	Потеря давления	2	Контролируется
			Заклинивание	0,010	Клапан не открывается по требованию	1	Возможный отказ; профилактические меры – выбор сочетаний материалов и обработка поверхности
9	Стопорный винт	Ручная блокировка размыкающего механизма	Заклинивание		Невозможно заблокировать или разблокировать откидной клапан	3	Обнаруживается при блокировке или разблокировании
			Трещина	0,090	Невозможно заблокировать или разблокировать откидной клапан	3	Обнаруживается при блокировке или разблокировании
			Блокировка не снята	0,010	Клапан не открывается по требованию	2	Контролируется электронной системой

Окончание таблицы А.2

Идентификационный номер	Компонент	Функции	Тип отказа	Частота отказов ($\times 10^6$) (в час)	Последствия отказа(ов)	Уровень важности	Комментарии
15	Плоская прокладка	Прокладка, установленная между корпусами и клапаном и приводным механизмом	Отсутствие герметичности	0,140	Отсутствуют	4	
41	Цилиндрический болт	Используется для прикрепления корпуса электронной части системы	Ослабление, трещина	0,064	Отсутствуют	4	
43	Уплотнительная шайба	Уплотнение болтовых соединений	Отсутствие герметичности	0,280	Отсутствуют	4	
51	Манометрический выключатель	Контролирует давление системы	Не открывается	0,500	Потеря давления не выявляется	2	Возможный отказ; впервые выявляется при первой проверке
			Не закрывается	0,500	Срабатывает аварийная сигнализация	3	Контролируется
			Отсутствие герметичности	0,100	Потеря давления	2	Контролируется
Примечание – В этой таблице представлены сведения только о части компонентов, для которых проводился анализ характера, последствий и важности отказов.							

На основе показателя важности последствий 1 уровня, полученного для огнетушителя большой производительности методом анализа характера,

последствий и важности отказов, может быть рассчитана общая вероятность отказов по требованию.

Подобные расчеты были проведены для устройства управления и датчика.

А.4.4 Результаты расчетов

На основе результатов анализа характера, последствий и важности отказов и/или анализа характера и последствий отказов, проведенных для огнетушителей большой производительности, устройства управления и датчика давления в сочетании с анализатором, была проведена оценка вероятности отказа системы подавления и изоляции взрыва. Были получены следующие результаты.

Таблица А.3 – Вероятность отказа по требованию для функции подавления взрыва

Компонент	Количество компонентов	Общий показатель вероятности отказа по требованию
Датчик в сочетании с устройством анализа	1	$8{,}8 \times 10^{-4}$
Устройство управления	1	$1{,}7 \times 10^{-3}$
Клапан с высокой пропускной способностью	3	$6{,}6 \times 10^{-3}$
Итого для функции системы	-	$9{,}1 \times 10^{-3}$

Как следует из таблицы А.3, функциональные возможности соответствуют требованиям уровня полноты безопасности 2 (SIL2) в соответствии со стандартами серии ЕН 61508.

Приложение В

(справочное)

Методы выявления отказов и оценки функциональной безопасности

В.1 Общие положения

Существует много методов выявления отказов, расчета вероятности и оценки последствий отказов. Каждый метод был разработан для конкретного применения, поэтому может потребоваться внесение изменений при проведении оценки функциональной безопасности конкретной системы.

Некоторые из применяемых методов кратко описаны и на них сделаны ссылки, например в приложении В ЕН 1050:1996 [7] и приложении В ЕН ИСО 17776:2002 [8]. Далее приводится описание двух методов и руководство по их применению для оценки функциональной безопасности.

В.2 Метод анализа характера и последствий отказов (FMEA) и метод анализ характера, последствий и важности отказов (FMECA)

Метод анализа характера и последствий отказов (FMEA) и метод анализ характера, последствий и важности отказов (FMECA) используются для выявления и описания нарушений в работе системы, резервной системы и отказов по общей причине, функций, режимов отказа, причин, последствий, методов выявления, средней наработки до ремонта и интервала испытаний для компонентов, ответственных за функцию безопасности в системах, связанных с безопасностью.

Для выполнения анализа необходимо разделить систему на компоненты. Важно правильно определить уровень разделения на компоненты. Уровень будет зависеть от цели анализа характера и последствий отказов / анализа, характера, последствий и важности отказов и имеющейся в наличии технической документации. В большинстве случаев анализ характера и последствий отказов (или анализ характера, последствий и важности отказов) проводится до анализа

дерева отказов или является основой для определения функциональной безопасности.

Анализ характера и последствий отказов или анализ характера, последствий и важности отказов осуществляет группа технических специалистов, а также персонал, имеющий большой опыт применения системы. Для записи информации о каждом компоненте используют стандартную форму (образец таблиц с результатами анализа характера и последствий отказов/анализа характера, последствий и важности отказов приведен в приложении А):

a) название и тип компонента;

b) функция;

c) режимы неисправности;

d) причины отказов;

e) последствия местной неисправностей;

f) последствия общей неисправностей;

g) обнаружение неисправностей;

h) компенсация / защита (резервная система);

i) комментарии, рекомендации и последующая проверка.

В таблицах с результатами анализа характера и последствий отказов/ анализа характера, последствий и важности отказов одна колонка также используется для количественных расчетов вероятности возникновения режима неисправности и последствий неисправности для компонентов. Проводится классификация вероятности возникновения неисправностей и их последствий (низкая, средняя, высокая/диаграмма рисков и т. д.). Значение и важность каждого класса неисправностей должны быть определены в тексте, последствия должны классифицироваться с учетом вреда для людей, финансовых затрат и воздействия на окружающую среду. При оценке функциональной безопасности для определения вероятности часто требуется количественная или

полуколичественная характеристика, которая должна быть указана изготовителем или может быть определена по данным для подобных систем.

В.3 Анализ дерева отказов (FTA)

Дерево отказов – это метод, с помощью которого любой нежелательный режим неисправности системы может быть описан, исходя из режимов отказа компонентов и действий оператора. Дерево отказов позволяет определить логику возникновения этих неисправностей. Результаты записывают в виде схемы дерева неисправностей.

Схема дерева неисправностей состоит из двух основных элементов: «логических знаков» и «событий». «Логические знаки» позволяют передвигаться вверх по логической цепочке дерева и выявлять взаимосвязи между событиями, необходимыми для возникновения события более высокого уровня. Основные виды логических знаков – И и ИЛИ. Логический знак И означает, что все события, входные по отношению к операции И, должны произойти одновременно, чтобы вызвать событие более высокого уровня. Логический знак ИЛИ означает, что только одно из событий, входных по отношению к операции ИЛИ, необходимо для возникновения события более высокого уровня. Существует также ряд других логических знаков, используемых реже и отображающих логический анализ. После того, как логическая схема будет внесена в дерево отказов, можно установить частоту возникновения высшего события, учитывая данные о частоте / вероятности возникновения событий самого нижнего уровня дерева. Эти сведения о частоте / вероятности возникновения событий обычно применяются к интенсивности отказа электронных, электрических или механических компонентов и могут быть получены из баз данных. Также можно рассчитать вероятность невыполнения оператором необходимых действий. Затем, для расчета частоты возникновения высшего события, может использоваться арифметический анализ, основанный на булевой алгебре. На любом ИЛИ возможно сложение частот возникновения. На любом И возможно умножение одной частоты на любое число возможностей (в качестве приближения первого порядка). При оценке дерева отказов необходимо

четко различать, какие данные относятся к частоте (в единицах события на единицу времени), какие – к вероятности (без указания размеров). Существуют также специальные методики оценки деревьев большого размера и сложной структуры, например с помощью минимальных вырезок событий.

Анализ дерева отказов должен проводиться специалистами, владеющими этим методом. Если логическая схема, отображаемая деревом отказов, окажется неправильной, то и рассчитанная частота также будет неправильной. Также возможно неправильное применение булевой алгебры, если не учитывается отказ по общей причине.

Метод анализа дерева отказов применяется в основном к обособленным элементам системы, собранному оборудованию и при оценке надежности систем защиты.

Применение метода для более сложного оборудования будет слишком сложной процедурой, требующей больших затрат времени, кроме случаев, когда этот метод используется без проведения количественного анализа, чтобы получить обзор взаимодействия между различными компонентами, функциями, выполненный на высоком уровне.

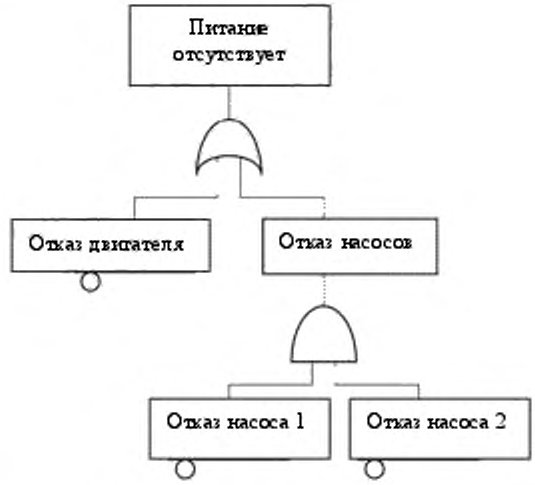


Рисунок В.1 – Дерево отказов для иллюстрации отказа в системе питания

Приложение ДА

(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ЕН 13237:2003	–	*

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

Библиография

[1] ЕН 15198 Методология оценки риска использования неэлектрического оборудования и компонентов во взрывоопасной атмосфере (EN 15198 Methodology for the risk assessment of non-electrical equipment and components for intended use in potentially explosive atmospheres)

[2] ЕН 1127-1 Взрывоопасные среды. Взрывозащита и предотвращение взрыва. Часть 1: Основополагающая концепция и методология (EN 1127-1 Explosive atmospheres. Explosion prevention and protection. Part 1. Basic concepts and methodology)

[3] ИСО/МЭК Руководство 73 Управление риском. Словарь. Руководящие указания по использованию в стандартах (ISO/IEC Guide 73, Risk management – Vocabulary – Guidelines for use in standards)

[4] ЕН 61508-4 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения (EN 61508-4, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations (IEC 61508-4:1998 + Corrigendum 1999)

[5] ЕН ИСО 13849-1:2006 Безопасность машин. Элементы систем управления, связанные с обеспечением безопасности. Часть 1. Общие принципы конструирования (EN ISO 13849-1:2006 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (ISO 13849-1:2006))

[6] ЕН 62061 Безопасность машин и механизмов. Функциональная безопасность электрических, электронных и программируемых электронных систем контроля, связанных с безопасностью (EN 62061, Safety of machinery

– Functional safety of safety-related electrical, electronic and programmable electronic control systems (IEC 62061:2005)

[7] ЕН 1050:1996 Безопасность машин. Принципы оценки риска. (EN 1050:1996. Safety of machinery – Principles for risk assessment)

[8] ЕН ИСО 17776:2002 Промышленность нефтяная и газовая. Установки для добычи из морских месторождений. Руководящие указания по выбору инструментов и методик для идентификации опасностей и оценки риска (EN ISO 17776:2002, Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment (ISO 17776:2000

УДК 621.3.002:5:006:354 ОКС 13.230; 29.260.20 Т58

Ключевые слова: среды взрывоопасные, системы защиты, предотвращение взрыва, функциональная безопасность, дерево отказов

Председатель ТК 403 А.С. Залогин

Разработчик А.Е. Киселев

gost.e-ecolog.ru