ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 366.6— 2019

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 6

Приложения для обеспечения безопасности промышленных предприятий с повышенным уровнем опасности

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «НИИ экономики связи и информатики «Интерэкомс» (ООО «НИИ «Интерэкомс») совместно с Обществом с ограниченной ответственностью «Корпоративные электронные системы» (ООО «КЭЛС-центр»)

2 ВНЕСЕН Техническими комитетами по стандартизации ТК 100 «Стратегический и инновационный менеджмент» и ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2019 г. № 42-пнст

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: gost.e-ecolog.ru *и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 109074 Москва, Китайгородский проезд, д. 7, стр. 1.*

*В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2019

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 1
3 Термины и определения 2
4 Основные принципы 2
5 Оценка риска 5
6 Назначение принимаемых мер 7
7 Выбор модуля и его эксплуатация 7
7.1 Полевые модули 7
7.2 Логические системы 8
8 Дополнительные аспекты 9

Введение

Комплекс предварительных национальных стандартов по тематике «обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами» состоит из следующих частей:

- Часть 1. Основные положения, принципы и понятия;
- Часть 2. Системы менеджмента;
- Часть 3. Подготовка, запуск и эксплуатация устройств безопасности;
- Часть 4. Верификация полноты аппаратных средств автоматизированной системы безопасности;
- Часть 5. Руководство по практическому применению;
- Часть 6. Приложения для обеспечения безопасности промышленных предприятий с повышенным уровнем опасности (настоящий стандарт).

Меры по обеспечению взрывозащиты являются составной частью концепции обеспечения безопасности промышленных предприятий. Понятная и детальная оценка риска технологического процесса с учетом особенностей производства (например, по методике PAAG/HAZOP, см. ГОСТ Р 51901.11) — стандартная практика обеспечения безопасности промышленных предприятий и основной элемент системы менеджмента безопасности. Систематическая оценка риска должна включать в себя оценку риска взрыва. Меры обеспечения взрывобезопасности определяются с учетом конкретных обстоятельств. Они зависят от степени ожидаемых разрушений и вероятности наступления катастрофических последствий. Меры и требования обеспечения безопасности устройств автоматического управления производственными процессами (PCE) рекомендуется устанавливать с учетом положений настоящего комплекса национальных стандартов.

Для неэлектрических устройств (например, для насосов), используемых во взрывоопасных зонах, нормативные документы, определяющие поставку данных устройств на рынок, требуют установления и задействования специальных функций контроля. Руководство пользователя, прилагаемое изготовителем к рассматриваемому неэлектрическому устройству, устанавливает требования качества к функциям контроля. Основным критерием выступает уровень полноты безопасности (SIL). Пользователи неэлектрических устройств должны обеспечить выполнение установленных требований к функциям контроля с учетом результатов оценки риска.

Настоящий стандарт не предназначен для целей сертификации и носит исключительно рекомендательный характер. Использование настоящего стандарта предполагает, что при организации производства, при практической реализации (наладке и вводе в эксплуатацию) и функционировании производственного оборудования в обязательном порядке соблюдаются все законодательные нормы, необходимые и достаточные меры технической безопасности, меры по предотвращению опасных инцидентов, а также прочие требования, установленные в национальных стандартах и других нормативных и технических документах.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 6

Приложения для обеспечения безопасности промышленных предприятий с повышенным уровнем опасности

Industrial automation systems and integration.
Safety and security arrangements of industrial process plants by means of process control engineering.
Part 6. Safety applications for high severity level industrial process plants

Срок действия с 2020—01—01
до 2022—01—01

1 Область применения

В настоящем стандарте определены положения, касающиеся обеспечения безопасности производственных установок при помощи устройств PCE, а также определены общие принципы работы производственных установок, особенности их практической реализации и функционирования. Используемое оборудование в рамках рассматриваемого технологического процесса, как правило, защищается вспомогательными системами. Приборные системы безопасности (SIS) используются, если другие меры оказываются неприменимыми, неадекватными или (при сравнительно меньшем риске) нерентабельными. Использование простых и понятных инструментов, дающих немедленный эффект, обеспечивает надежное и рентабельное решение проблемы.

Настоящий стандарт определяет связь между обеспечением функциональной безопасности и обеспечением взрывозащиты и определяет возможность установления надлежащих соотношений между:

1) требованиями искробезопасности;

2) возможностью уменьшения риска по запросу;

3) конкретными устройствами PCE (с учетом имеющейся классификации данных устройств по уровню SIL).

Принципы обеспечения взрывобезопасности, установленные в настоящем стандарте, не ограничиваются промышленными предприятиями. Они могут быть использованы и в других производственных отраслях.

В настоящем стандарте конкретные примеры расчетов характеристик безопасности не рассматриваются. Данные расчеты проводятся на основании результатов индивидуальной оценки риска. В настоящем стандарте рассматриваются:

1) вышеуказанные соотношения;

2) основные положения методики оценки рисков.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 51901.11 Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство

ГОСТ Р ИСО 9000 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р МЭК 61508 (все части) Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью

Издание официальное

ПНСТ 366.1—2019 Системы промышленной автоматизации и интеграция. Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами. Часть 1. Основные положения, принципы и понятия

ПНСТ 366.4—2019 Системы промышленной автоматизации и интеграция. Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами. Часть 4. Верификация полноты аппаратных средств автоматизированной системы безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ПНСТ 366.1—2019.

4 Основные принципы

Основные принципы обеспечения безопасности промышленных предприятий с повышенным уровнем опасности выражаются в следующем:

- на предприятиях с непрерывным производством обычно используется принцип «обеспечения функциональной безопасности». Он позволяет (с помощью системы устройств PCE) снизить уровень риска до приемлемого значения;
- концепции безопасности для установок непрерывного технологического процесса учитывают преобладающие риски по формуле: «риск = (степень повреждения) × (вероятность наступления события)»;
- при обеспечении взрывозащиты профилактическая работа по предотвращению образования взрывоопасной среды и по предотвращению активации источников искрообразования имеет приоритет над аварийными мероприятиями по смягчению последствий взрыва.

Ниже принимается допущение, что оценка риска выполнена с учетом всех особенностей каждого конкретного случая:

- в результате взрыва во взрывоопасной среде могут иметь место обширные разрушения и различные травмы и повреждения (от легкого ранения до летального исхода);
- вероятность взрыва зависит от двух факторов:
  - вероятности формирования взрывоопасной среды (зоны);
  - вероятности активирования имеющегося источника искрообразования,
- риск активирования имеющегося источника искрообразования на доступных на рынке взрывозащищенных устройствах, предназначенных для работы в опасных зонах, должен быть достаточно низким. Устройства, изготовленные по соответствующему стандарту, удовлетворяющие установленным требованиям, а также сертифицированные уполномоченными административными органами, могут использоваться в соответствии со своей категорией во взрывоопасной зоне по назначению. Условия эксплуатации данных устройств рассматриваются, документируются и утверждаются в установленном порядке.

Рассмотренные далее технические меры относятся к таким понятиям, как «взрывозащищенный механизм (ex-mechanism)» и «взрывозащищенная система (ex-system)» [куда относят, например, систему инертизации (систему добавления инертного газа во взрывоопасную среду), систему вентиляции, систему терморегулирования, особые типы взрывозащищенных устройств с предотвращением искрообразования и т. п.]. Данная система ассоциируется с техническим контролем. Понятие «технический контроль» в настоящем стандарте не эквивалентно аналогичному понятию «система технического контроля устройств PCE», приведенному в ПНСТ 366.1—2019.

Использование «взрывозащищенной системы» может оказаться достаточным для уменьшения реального риска до требуемого уровня (см. взрывозащищенный механизм № 1 на рисунке 1). В противном случае уменьшение риска должно дополняться как специальными организационными мерами, так и инженерными мерами (например, устройствами PCE). «Взрывозащищенные системы» оцениваются с учетом реального значения коэффициента технического использования устройств обеспечения безопасности, а также их поведения при наступлении неисправности.

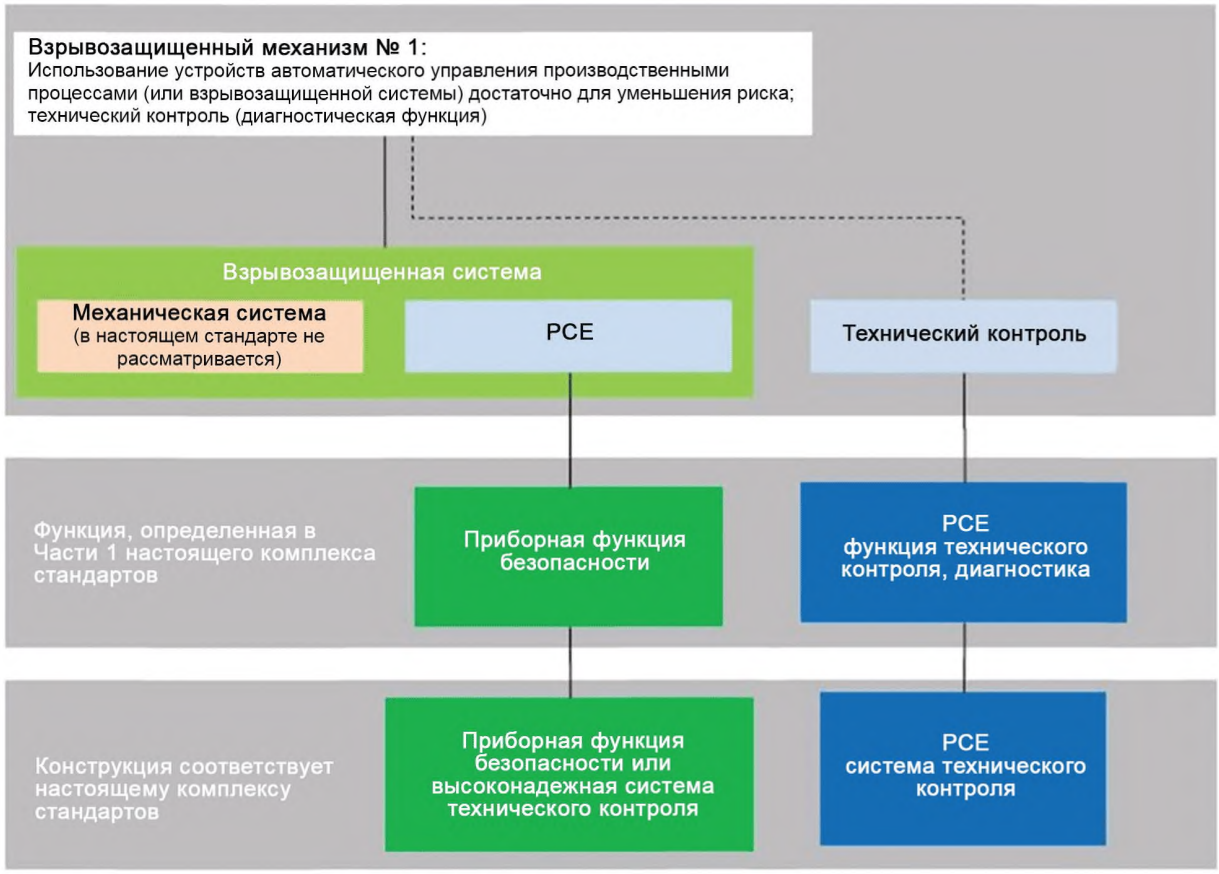

Рисунок 1 — Пример 1: Взрывозащищенный механизм № 1

Примечание — Если уменьшение риска, полученное с помощью взрывозащищенной системы, недостаточно, то технический контроль обеспечивается приборной системой безопасности или высоконадежной системой контроля производственного процесса.

Примеры

1 Обеспечение контроля содержания азота с помощью операционной системы управления (эквивалент взрывозащищенной системы) в рамках распределенной системы управления (DCS).

2 Контроль давления (эквивалент системы технического контроля) с помощью приборной системы безопасности (см. взрывозащищенный механизм № 2 на рисунке 2).

Основанный на оценке риска технический контроль можно рассматривать как работу высоконадежной системы контроля производственного процесса (приборной системы безопасности) в соответствии с настоящим стандартом с учетом принятых допущений. При оценке риска необходимо учитывать возможные принятые дополнительные меры (например, организационные меры).

При оценке риска важно учитывать, что надлежащее сочетание взрывозащищенной системы и системы технического контроля — эффективный инструмент уменьшения риска. Допустимы различные варианты, находящиеся в диапазоне, определяемом рисунком 1 с одной стороны и рисунком 2 — с другой (см. рисунок 3).

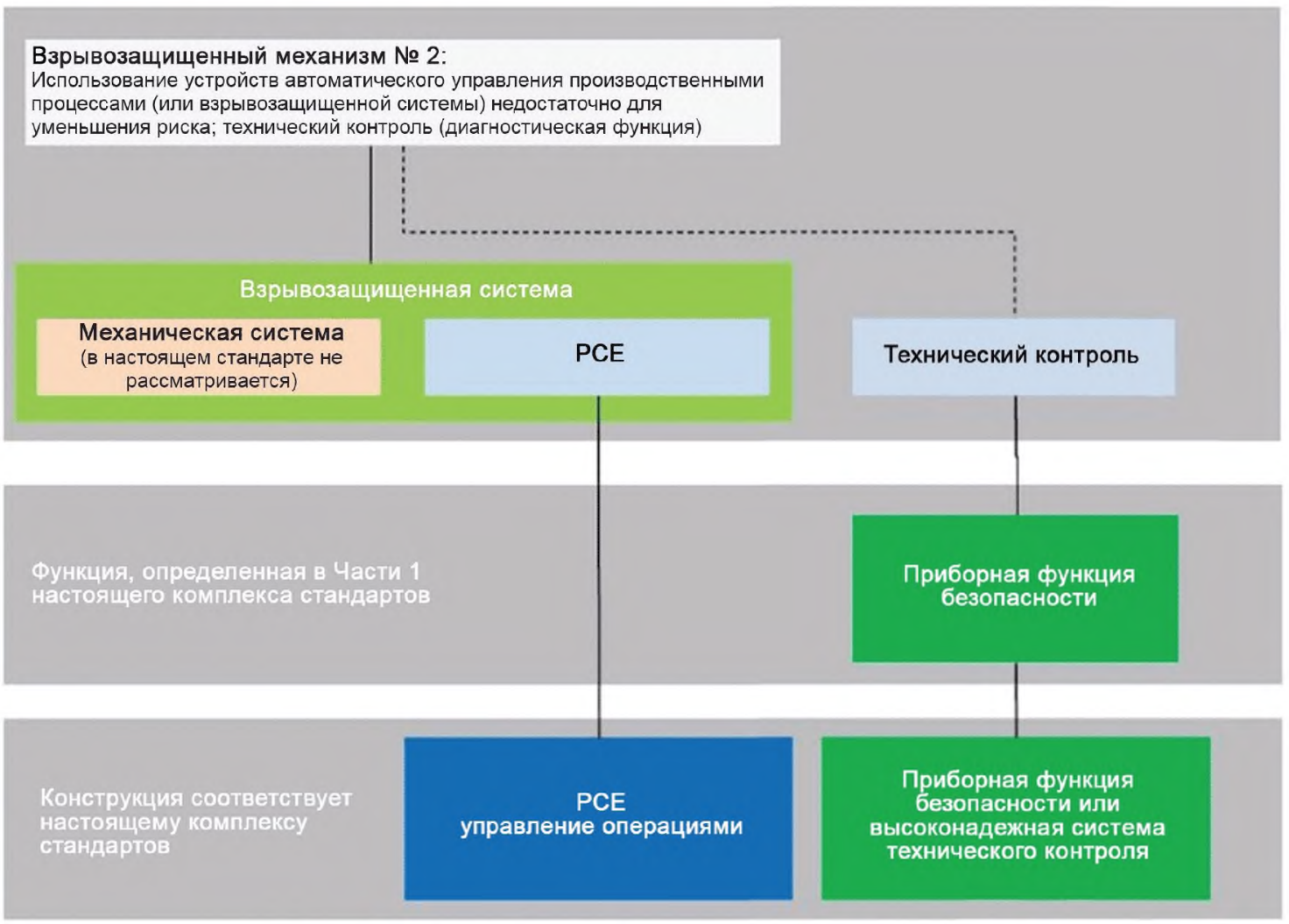

Рисунок 2 — Пример 2: Взрывозащищенный механизм № 2

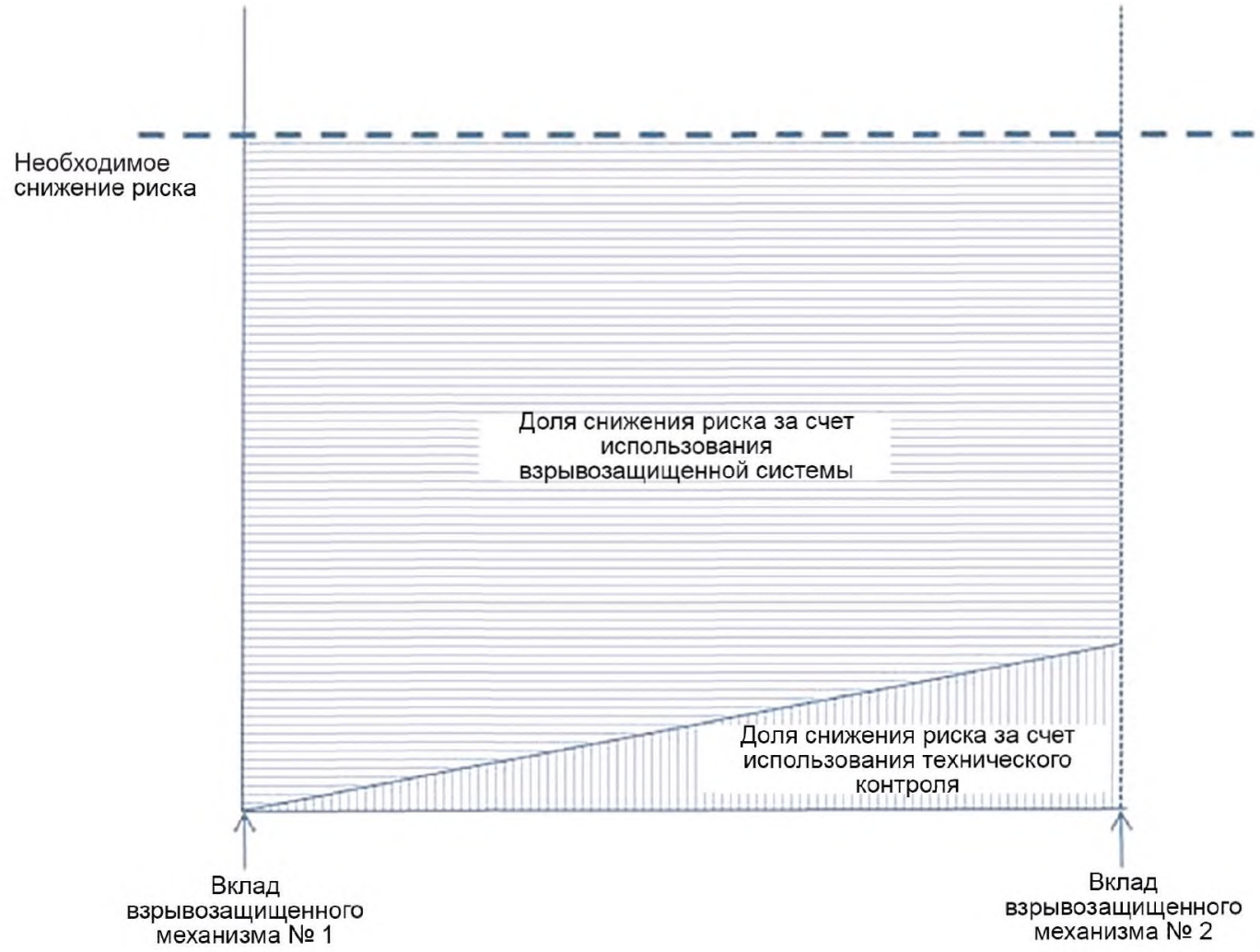

Рисунок 3 — Изменение вклада взрывозащищенной системы и системы технического контроля в уменьшение риска

Надлежащий технический контроль (реализуемый с помощью высоконадежной системы контроля производственного процесса) должен гарантировать, что взрывозащищенная система непрерывно проверяется на корректность работы. Аварийный сигнал выдается так, чтобы обслуживающий персонал успел вмешаться в работу установки. Если технический контроль не дает существенного вклада в уменьшение риска, то, наоборот, отказ системы технического контроля не приведет к вынужденному отказу взрывозащищенной системы и немедленному взрыву. Данные обстоятельства следует учитывать при оценке риска. На рисунке 4 приведено совместное действие взрывозащищенной системы и устройств технического контроля взрывозащищенного механизма.

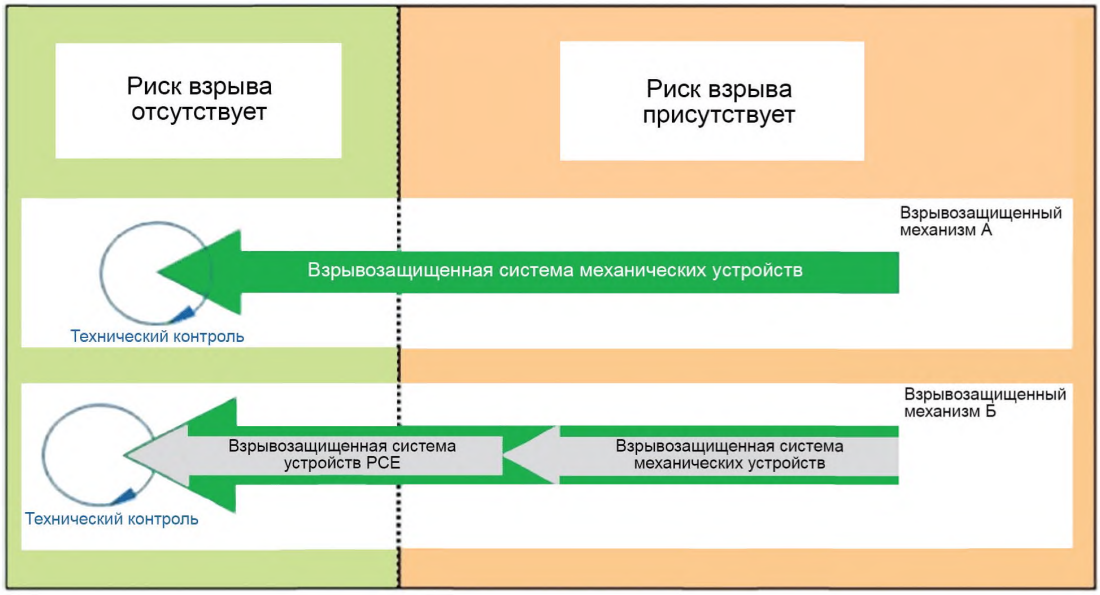

Рисунок 4 — Совместное действие взрывозащищенной системы и устройств технического контроля взрывозащищенного механизма

5 Оценка риска

Классификация производственных зон позволяет установить вероятность образования (в данной зоне) взрывоопасной среды. Данная вероятность может быть уменьшена с помощью технических (организационных мер). Например, с помощью вентиляции или инертизации (закачки инертного газа). В результате получается «зона с уменьшенным уровнем взрывоопасности».

Модули (технические устройства) данной зоны должны быть сертифицированы в соответствии с установленной процедурой. Если, в исключительном случае (после оценки риска), используются несертифицированные модули, то повышенный риск можно уменьшить до требуемого уровня с помощью дополнительных мер (например, путем обеспечения функциональной безопасности). Например, можно использовать имеющуюся систему устройств РСЕ для технического контроля источников искрообразования.

Требования к конструкции таких систем РСЕ зависят (в обоих случаях) от требуемой степени уменьшения риска, определенной его оценкой. Свойства рассматриваемых устройств и производственные условия играют здесь решающую роль.

При оценке риска приняты следующие допущения.

а) Качественные методы, используемые при взрывозащите модулей для классификации опасных зон, принципы конструирования взрывозащищенных модулей (определенные стандартами на их конструкцию), а также сама процедура оценки степени соответствия модулей установленным требованиям, доказали свою работоспособность в рамках имеющейся нормативно-правовой базы. Поэтому

никаких новых допущений (кроме имеющихся) не нужно, так как категория взрывозащитных устройств соответствует требованиям рассматриваемой зоны. Например, в зоне № 1 могут быть использованы устройства категории 2G. Принцип «обеспечения функциональной безопасности» начинает работать, когда рассматриваемая концепция взрывозащиты требует принятия дополнительных мер в отношении устройств РСЕ для уменьшения опасных зон, для предотвращения активации имеющихся операционных (технологических) источников искрообразования;

б) Количественная оценка риска (необходимое уменьшение реальных рисков на основе точных вычислительных алгоритмов) не представляется реалистичной. Этому могут служить следующие причины:

1) большой случайный разброс входных значений расчетных параметров (см. ПНСТ 366.4—2019);
2) наличие местных неоднородностей веществ в атмосфере зоны;
3) случайность совпадения во времени и пространстве событий, приводящих к активации взрывного механизма.

Численная оценка уменьшения риска — основной рассматриваемый параметр. Обычно при обеспечении функциональной безопасности для оценки уменьшения риска рассматривают 3 уровня: *низкий*, *высокий*, *очень высокий*. Значение нижнего уровня уменьшения риска равно 10. Значения указанных уровней уменьшения риска отличаются друг от друга примерно в 10 раз. Данная оценка очень грубая. Поэтому в ряде случаев для рассматриваемых систем устройств РСЕ целесообразно введение специально градуированных мер уменьшения риска.

Примечание — Указанные численные оценки рассматриваемых величин — очень грубые. С другой стороны, практический опыт показывает: точные количественные оценки либо невозможны, либо не нужны.

При учете влияния производственного процесса на оценку риска при проведении цеховых мероприятий по уменьшению рисков предпочтение следует отдавать мерам, не связанным с непосредственным использованием рабочих устройств РСЕ, например механических устройств, устройств управления установкой и т. п.

Необходимо учитывать, что результат оценки риска существенно зависит от стадии рассматриваемого технологического процесса. На стадии пуска установки (например, когда идет процесс формирования азотной «подушки» при затекании воздуха из окружающей атмосферы в бак) могут работать одни требования. При установившейся работе технологической установки работают другие требования. На стадии пуска технологического процесса особое внимание следует уделить организационным мерам (например, проверке герметичности установки, определению возможных протечек и т. п.). И наоборот, при установившейся работе установки важно бесперебойно обеспечивать требуемые расходы рабочих материалов с помощью специальных механических устройств (например, с помощью дырчатых пластин и т. п.).

Дополнительно необходимо учитывать:

- если в приложении риск взрыва уменьшается 1) путем уменьшения размеров взрывоопасных зон и 2) путем предотвращения активации источников искрообразования, то обе указанные меры могут рассматриваться независимо в соответствии с процедурой, определенной в настоящем стандарте. Опыт показывает, что, как правило, указанные два события (образование взрывоопасной зоны в атмосфере, активация источника искрообразования) не зависят друг от друга;
- требования таблицы 1 определяют процедуру необходимого уменьшения риска функционирования систем РСЕ (см. рисунки 1, 2);
- для принятия комплексных мер по снижению риска (уменьшение взрывоопасных зон, недопущение активации источников искрообразования) может оказаться необходимым задействовать несколько систем технического контроля. Это имеет смысл, если ожидается наступление нескольких неисправностей с различным механизмом, выявляемых различными методами.

Если оценка риска (повреждения) показывает, что ожидаемое значение риска равно соответствующему стандартному значению, то мероприятия по уменьшению риска проводятся в соответствии с таблицей 1.

Таблица 1 — Необходимое уменьшение риска в зависимости от начального и целевого состояний взрывоопасной зоны. Использование устройств PCE (взрывозащищенных устройств PCE и устройств технического контроля PCE)

Состояние зоны		Необходимое уменьшение риска с помощью устройств PCE
Начальное состояние[1)]	Целевое состояние[2)]	
0/20	1/21	Низкий
0/20	2/22	Высокий
0/20	nEx	Очень высокий[3)]
1/21	2/22	Низкий
1/21	nEx	Высокий
2/22	nEx	Низкий

[1)] Меры по уменьшению взрывоопасной зоны не принимались.
[2)] Приняты меры по уменьшению взрывоопасной зоны (преобладает вероятность активации источников искрообразования).
[3)] Специально для начальной зоны 0/20 и целевой зоны nEx (риск взрыва отсутствует). Постоянно присутствует источник искрообразования. При оценке риска данный случай является критическим.

6 Назначение принимаемых мер

Если устройства PCE используются в соответствии с рисунками 1, 2 и данные устройства имеют уровень полноты безопасности SIL2 или SIL3, то необходимо уменьшение рисков уровня высокий (очень высокий). Риск уровня низкий может соответствовать уровню полноты безопасности SIL1. Это обеспечивается путем использования высоконадежной системы контроля производственного процесса. При изменении уровня риска его значение изменяется примерно в 10 раз. Указанные обстоятельства учитываются рассматриваемой процедурой оценки риска (см. таблицу 2).

7 Выбор модуля и его эксплуатация

7.1 Полевые модули

а) Риск уровня высокий (очень высокий)

Требование уменьшения риска уровня высокий (очень высокий) — это типовое требование к полевым модулям с качеством «проверено-на-практике» (на основе предшествующего опыта). Данное требование определено в частях 1—5, для одноканальных конфигураций с функциями уровня SIL2, для многоканальных конфигураций с функциями уровня SIL3.

б) Риск уровня низкий

Требование уменьшения риска уровня низкий — это типовое требование к типовым полевым модулям качества «проверено-на-практике». Данное требование определено в частях 1—5 для одноканальных конфигураций.

В обоих случаях требования к испытаниям рабочих функций устанавливаются в рамках концепции эксплуатационных испытаний.

Таблица 2 — Функции PCE

Функции PCE	Уменьшение риска		Реализация
Функции обеспечения безопасности	Очень высокий	Примерно 1000	Уровень SIL3
	Высокий[1)]	Примерно 100	Уровень SIL2
	Низкий	Примерно 10	Уровень SIL1 или высоконадежная система контроля производственного процесса

Окончание таблицы 2

Функции PCE	Уменьшение риска	Реализация
Функция технического контроля/диагностика	—	Система контроля производственного процесса
[1] В обоснованных случаях уменьшение риска уровня высокий также можно обеспечить путем запараллеливания двух высоконадежных систем контроля производственного процесса. Важное условие: эти две системы должны работать независимо друг от друга. Тогда отказ одной из систем не приведет к возникновению опасной ситуации. Время реакции указанной системы на сбой (например, время инертизации бака с плоским днищем и т. п.) должно быть достаточно малым. Данная система не является приборной системой безопасности.		

Примечания

1 Взрывозащищенная система устройств PCE может работать в режиме «замкнутого контура» (как обычная операционная система управления). Тогда технический контроль — это отдельная функция безопасности уровня полноты безопасности SIL2.

2 Если для уменьшения риска принята комбинация мер, то требования к надежности взрывозащищенной системы устройств PCE могут быть снижены в соответствии с концепцией обеспечения взрывозащиты для заданной оценки риска.

7.2 Логические системы

7.2.1 Систематические сбои

а) Риск уровня высокий (очень высокий)

Программируемые логические контроллеры устройств обеспечения безопасности SPLC уровня полноты безопасности SIL3 должны соответствовать установленным требованиям по систематическим сбоям с риском уровня очень высокий. Следовательно, они удовлетворяют требованиям по сбоям с риском уровня высокий и низкий.

б) Риск уровня низкий

Программируемые логические контроллеры устройств обеспечения безопасности SPLC должны соответствовать установленным требованиям по сбоям с риском уровня низкий. Вследствие высокой адаптивности данных контроллеров к операционным модификациям, не связанным с обеспечением безопасности системой устройств PCE распределенной системы управления DCS, они имеют высокий потенциал в борьбе с систематическими сбоями (например, путем программирования приложений). Нижеследующие дополнительные меры являются минимальными даже при уменьшении риска уровня низкий:

- применение изготовителем системы управления DCS (в процессе производства) системы менеджмента качества для своих изделий (например, в соответствии с ГОСТ Р ИСО 9000);
- обеспечение соответствия системы управления DCS требованиям, установленным для промышленных предприятий с непрерывным циклом работы;
- задействование системы управления изменениями для всех модификаций системы управления DCS;
- периодическое тестирование высоконадежных систем контроля производственного процесса;
- надлежащее обучение персонала, связанного с техническим обслуживанием и модификациями оборудования;
- контроль независимости функционирования:
  1) системы операционного управления,
  2) систем технического контроля,
  3) высоконадежных систем контроля производственного процесса. Это достигается, например, путем использования раздельных модулей входа-выхода, путем реализации указанных функций в отдельных полевых системах управления FCS и т. п. [см. часть 3 (использование отдельных модулей, независимых функциональных блоков)];
- использование свойств отказоустойчивости (например, принципа «остановлен по отключению питания», свойства перехода в безопасное состояние при отказе системы энергообеспечения и т. п.).

7.2.2 Случайные сбои

а) Риск уровня высокий (очень высокий)

Интенсивность отказов программируемого логического контроллера устройства обеспечения безопасности SPLC должна соответствовать требованию обеспечения риска до уровня очень высокий.

б) Риск уровня низкий

Системы управления производственным процессом, используемые на предприятиях непрерывного цикла, а также сертифицированные программируемые логические контроллеры устройств обеспечения безопасности SPLC удовлетворяют требованию обеспечения риска уровня низкий с учетом случайных сбоев.

8 Дополнительные аспекты

а) Используемые модули должны быть разработаны и изготовлены в соответствии с требованиями комплекса национальных стандартов ГОСТ Р МЭК 61508.

Указание значения уровня полноты безопасности SIL в оценке риска — это общее требование к функции обеспечения безопасности (выбор надлежащего оборудования, системы безопасности, жизненный цикл устройства обеспечения безопасности и т. п.).

Указание значения уровня полноты безопасности SIL изготовителем модуля PCE подтверждает, что данный модуль удовлетворяет качественным требованиям комплекса национальных стандартов ГОСТ Р МЭК 61508 (например, в части процесса разработки модуля) и что указанная вероятность отказа при наличии запроса PFD данного модуля соответствует нормативному значению. Это частный аспект вышеуказанных общих требований.

Если указанные модули с заданным уровнем полноты безопасности SIL не связаны с функциями обеспечения безопасности, то соответствие вышеуказанным общим требованиям (например, к функционированию систем обеспечения безопасности, к жизненному циклу устройств обеспечения безопасности) не является необходимым. Более того, вышесказанное не требует организации периодического тестирования, задействования соответствующих логических функций сертифицированной системы безопасности.

Необходимо безусловное выполнение инструкций изготовителя в части обеспечения безопасного функционирования модуля.

б) Если работа некоторой приборной функции безопасности с заданным уровнем полноты безопасности SIL учитывается при оценке риска, то данную функцию следует разрабатывать и рассматривать как приборную систему безопасности. Замена приборной системы безопасности одной или несколькими высоконадежными системами контроля производственного процесса не разрешается.

в) Если изготовитель рекомендует использование модуля с заданным уровнем полноты безопасности SIL или функции обеспечения безопасности в руководстве пользователя (например, использование устройства контроля температуры насоса), то факт использования модуля уточняется при оценке риска (так как изготовитель может не охватывать конкретные условия производства).

Примечание — Если требуемый уровень полноты безопасности SIL рабочих модулей закладывается в оценку риска, то реальный уровень полноты безопасности SIL данных модулей (например, датчиков температуры), поставляемых изготовителем, должен быть не ниже требуемого.

УДК 658.52.011.56:006.354 ОКС 13.110; 25.040.01

Ключевые слова: системы автоматического управления производственными процессами; производственные процессы; приборные системы безопасности; уровень полноты безопасности; приложения для обеспечения безопасности промышленных предприятий с повышенным уровнем опасности

БЗ 10—2019/121

Редактор *В.Н. Шмельков*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 24.09.2019. Подписано в печать 09.10.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru