ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН ООО «НИИ экономики связи и информатики «Интерэкомс» (ООО «НИИ «Интерэкомс») совместно с ООО «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. № 37-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 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 Термины и определения 2
2.1 Общие термины 2
2.2 Термины, связанные со сбоями, свойствами и характеристиками приборных систем безопасности 5
2.3 Термины, связанные с генерацией и обработкой сигналов 6
3 Разработка концепции безопасности 7
4 Классификация функций и систем автоматического управления производственными процессами . 8
4.1 Основные системы управления процессами (BPCS-системы) 8
4.2 Приборные системы безопасности (SIS-системы) 10
5 Процедура определения требований к приборным системам безопасности 12
6 Метод графов риска 13
6.1 Степень повреждения 14
6.2 Присутствие в опасной зоне 15
6.3 Предупреждение об опасности 15
6.4 Вероятность наступления нежелательного события 16
6.5 Прочие возможные параметры риска 16
7 Уровень полноты безопасности (SIL) 17
8 Определение требований 17
8.1 Требования пониженного уровня риска (уровни SIL 1 и SIL 2) 18
8.2 Требования повышенного уровня риска (SIL 3) 19
Приложение А (справочное) Цикл работ со сбоями 20

Введение

Комплекс 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 (настоящий стандарт);
- 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 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 1

Основные положения, принципы и понятия

Industrial automation systems and integration. Safety and security arrangements of industrial process plants by means of process control engineering. Part 1. Basic concepts, principles and terms

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 автоматического управления производственными процессами (PCE).

Также в настоящем стандарте определены общие принципы работы и возможности поддержки производственных установок, особенности их практической реализации и функционирования. Используемое оборудование в рамках рассматриваемого производственного процесса, как правило, защищается вспомогательными системами. Приборная система безопасности (SIS-система) используется, если другие меры оказываются неприменимыми, неадекватными или (при сравнительно меньшем риске) нерентабельными. Использование простых и понятных инструментов, дающих быстрый эффект, обеспечивает надежное и эффективное решение проблемы.

На рисунке 1 приводится процедура встраивания технологии управления производственными процессами в общую концепцию безопасности предприятий.

Издание официальное

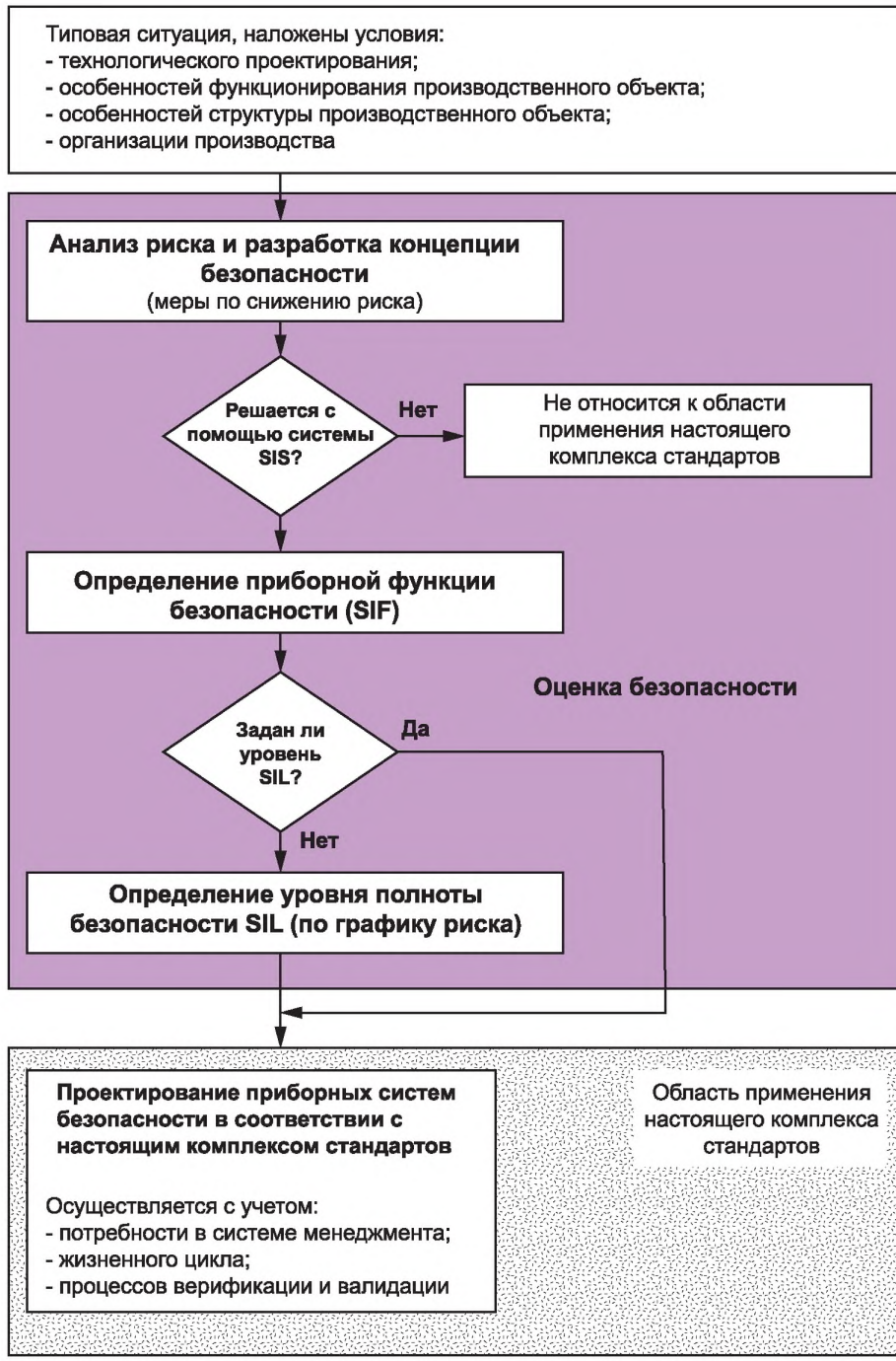


Рисунок 1 — Процедура встраивания технологии управления производственными процессами в общую концепцию безопасности

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

2.1 Общие термины

2.1.1 **опасность** (danger): Состояние системы, при котором возможно возникновение события (опасного), несущего вред (ущерб), и такого, что уровень риска (как количества опасности) нанесения

вреда или последствий превышает значения приемлемого риска; при этом возможно возникновение ситуации, при которой может возникнуть серьезный ущерб.

2.1.2 **безопасность** (safety): Отсутствие неприемлемого риска.

2.1.3 **требования безопасности** (safety requirement): Определенные необходимые условия, гарантирующие безопасность работы.

Примечание — Требования безопасности накладываются либо законами и техническими нормами (в дополнение к законодательству), либо другими руководящими документами. Указанные требования могут определяться общим мнением специалистов или утвержденными техническими документами.

2.1.4 **оценка безопасности** (safety assessment): Детальное исследование возможных опасностей, возникающих во время функционирования оборудования.

Примечание —Оценка безопасности включает в себя спецификацию мер безопасности. Данная оценка — это многостороннее мероприятие, задействующее специалистов по организации производства, инженеров-технологов, специалистов по охране труда, представителей контрольных технических служб, специалистов по автоматическому управлению производственными процессами, специалистов по другим прикладным дисциплинам.

2.1.5 **корректный диапазон** (correct range): Утвержденный диапазон, определяемый таким образом, чтобы качество и количество продуктов удовлетворяло установленным требованиям (см. рисунок 3).

2.1.6 **допустимый диапазон неисправностей** (permissible fault range): Диапазон между корректным диапазоном неисправностей и недопустимым диапазоном неисправностей.

Примечание — Если рассматриваемая установка находится внутри данного диапазона, то с точки зрения безопасности на дальнейшее функционирование указанной установки ограничений нет при условии, что значение соответствующего технологического параметра лежит внутри допустимого диапазона неисправностей.

2.1.7 **недопустимый диапазон неисправностей** (impermissible fault range): Диапазон, в котором возможно наступление нежелательного события.

2.1.8 **корректное состояние** (correct state): Рабочее состояние, в котором значения всех технологических параметров лежат внутри их корректных диапазонов, при этом, рассматриваемая установка не является источником опасности (например, вследствие протечек).

2.1.9 **допустимое состояние неисправности** (permissible fault state): Рабочее состояние, в котором значения одного или нескольких технологических параметров лежат внутри допустимого диапазона неисправностей, а технологические параметры, значения которых лежат в недопустимом диапазоне неисправностей, — отсутствуют, при этом, рассматриваемая установка не является источником опасности (например, вследствие протечек).

2.1.10 **недопустимое состояние неисправности** (impermissible fault state): Рабочее состояние, в котором значения одного или нескольких технологических параметров лежат внутри недопустимого диапазона неисправностей, при этом, рассматриваемая установка не является источником опасности (например, вследствие протечек).

2.1.11 **штатное использование** (normal use): Режим работы при котором оборудование используется по назначению, и его конструкция соответствует целям производства. Штатное использование включает:

- штатное функционирование;
- операции включения и отключения;
- ввод в эксплуатацию, вывод из эксплуатации;
- пробную эксплуатацию;
- визуальный осмотр, профилактическое и корректирующее техническое обслуживание.

Примечание — При использовании по назначению (штатное использование), рассматриваемая установка находится либо в корректном состоянии, либо в допустимом состоянии неисправности.

2.1.12 **нештатное использование** (non-normal use): Режим работы при котором, рассматриваемая установка находится в недопустимом состоянии неисправности.

2.1.13 **нежелательное событие** (unwanted event): Событие, непосредственно приводящее к травмам рабочих и экологическому ущербу, при этом, значение риска превышает максимально приемлемое значение.

2.1.14 **риск** (risk): Сочетание вероятности появления события причинения вреда и тяжести этого вреда.

Примечание 1 — Риск, ассоциируемый с конкретным техническим мероприятием и конкретным состоянием установки, оценивается по формуле теории вероятности, которая учитывает:

- ожидаемую частоту наступления события, приводящего к повреждению,
- ожидаемую степень повреждения в результате наступления события.

В большинстве случаев, риск (R) не выражается количественно. Определение количественных значений риска возможно, если есть комбинация (x) значений двух переменных: частоты наступления события (H) и степени повреждения (S). Тогда значение риска равно $R = H \times S$.

Если различные значения риска относятся к различным узлам одного конкретного производственного процесса, то данные узлы можно рассматривать как независимые. Это означает, что данному производственному процессу могут соответствовать различные уровни безопасности приборной системы безопасности.

Примечание 2 — Вероятность возникновения включает в себя подверженность влиянию опасной ситуации, возникновение опасного события и вероятность того, что вреда можно будет избежать или ограничить его.

2.1.15 **приемлемый риск** (acceptable risk): Риск, значение которого приемлемо для данного состояния общества в конкретном контексте.

Примечание — Наивысший уровень приемлемого риска — это максимально приемлемый риск.

2.1.16 **максимально приемлемый риск** (maximum acceptable risk): Наивысшее приемлемое значение риска, ассоциированное с конкретным техническим мероприятием или состоянием.

Примечание 1 — В большинстве случаев максимально приемлемый риск не выражается количественно. Обычно он выражается косвенно по спецификации безопасности.

Примечание 2 — Максимально приемлемый риск определяется объективными и субъективными действиями. Он может сильно отличаться для разных приложений. Субъективные действия могут включать:

- рабочее восприятие опасности, одни опасности являются видимыми, другие — нет. Важно учитывать, что люди, подвергающиеся опасности, в некоторых обстоятельствах сами могут оказывать действие на производственный процесс;
- социальное восприятие опасности;
- группу лиц, оказавшуюся под действием факторов опасности, выполнение требований по защите детей и больных.

2.1.17 **параметры риска** (risk parameters): Качественные выводы, касающиеся степени ущерба и частоты наступления событий, причиняющих ущерб (данные выводы определяют уровень полноты безопасности).

2.1.18 **меры безопасности** (safety measures): Комбинация мер принятых для уменьшения риска.

Примечание — В контексте настоящего стандарта, указанные меры могут быть как техническими, так и нетехническими (например, организационными).

2.1.19 **уровень полноты безопасности; УПБ** (safety integrity level; SIL): Дискретный уровень (принимающий одно из четырех возможных значений), назначаемый для функций безопасности приборной системы безопасности и определяющий требования к полноте безопасности, которая должна быть достигнута реализуемой приборной системой безопасности.

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.69]

2.1.20 **основная система управления процессом; ОСУП** (basic process control systems, BPCS): Система, которая реагирует на входные сигналы, поступающие от процесса, от его соответствующего оборудования, от программируемых систем и/или от оператора и вырабатывает выходные сигналы, заставляющие процесс и его соответствующее оборудование действовать желательным образом, но которая не выполняет никаких функций безопасности приборной системы безопасности.

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.3]

2.1.21 **системы контроля производственного процесса** (process supervision systems): Системы автоматического управления, работающие в пределах, установленных между корректным диапазоном и допустимым диапазоном неисправностей. Они также могут работать внутри допустимого диапазона неисправностей и обеспечивают выполнение таких функций, как выдача сигнала тревоги, переключение режима работы и т. п.

2.1.22 **приборная система безопасности;** ПСБ (safety instrumented system, SIS): Приборная система, которая используется для выполнения одной или нескольких функций безопасности (см. раздел 4, рисунок 2).

Примечания

1 Приборная система безопасности может состоять из одного или нескольких датчиков, из одного или нескольких логических устройств и из одного или нескольких исполнительных элементов. Она также включает в себя средства коммуникации и вспомогательное оборудование (например, кабели, кабельные каналы, источники электропитания, импульсные линии и линии обогрева).

2 Приборная система безопасности может содержать в себе программное обеспечение.

3 Приборная система безопасности может включать в себя действия человека как часть функции безопасности приборной системы безопасности.

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.67]

2.1.23 **функция безопасности приборной системы безопасности;** ФБ ПСБ (safety instrumented function, SIF)**:** Функция безопасности, которую будет реализовывать приборная система безопасности (см. раздел 4, рисунок 2).

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.66]

2.1.24 **надежность** (reliability): Способность узла выполнять указанную функцию в указанных пределах и в указанное время.

2.1.25 **коэффициент готовности** (availability): Вероятность того, что объект окажется работоспособным в произвольный момент времени, когда потребуется его применение по назначению.

2.1.26 **коэффициент отказа** (non-availability): Вероятность того, что объект окажется неработоспособным в произвольный момент времени, когда потребуется его применение по назначению (U = 1 — V).

2.2 Термины, связанные со сбоями, свойствами и характеристиками приборных систем безопасности

2.2.1 **сбой** (fault): Потеря способности выполнять требуемую функцию из-за внутреннего состояния.

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.19]

2.2.2 **систематический сбой** (systematic fault): Сбой, после которого детерминированным образом появляется отказ, который можно предотвратить только путем применения определенных мер к процессу производства или проектирования.

2.2.3 **случайный сбой** (random fault): Сбой с невоспроизводимыми причинами без возможности предсказания его наступления.

2.2.4 **контроль сбоев** (fault control): Защита приборной системы безопасности от случайных сбоев, возникающих при ее функционировании, а также от систематических сбоев, имеющих место при ее функционировании.

2.2.5 **предотвращение сбоя** (fault prevention): Использование методов и процедур, предназначенных для предотвращения возникновения сбоев во время любой стадии жизненного цикла приборной системы безопасности.

2.2.6 **активный сбой** (active fault): Неисправность, инициирующая функции безопасности, даже когда условия их выполнения неизвестны.

2.2.7 **пассивный сбой** (passive fault): Неисправность, блокирующая функции безопасности (или соответствующего канала), даже когда указаны все условия их выполнения.

2.2.8 **сбой с автоматической сигнализацией** (self-signaling fault): Неисправность, которая становится очевидной в момент ее возникновения.

2.2.9 **сбой программного обеспечения** (software faults): Расхождения между фактическими и целевыми функциями компьютерных программ.

Примечание — Сбой программного обеспечения относится к систематическим сбоям.

2.2.10 **время обнаружения сбоя** (fault detection time): Интервал времени между наступлением сбоя и его обнаружением.

2.2.11 **отказ** (failure): Потеря способности функционировать соответствующим образом.

Примечания

1 Отказ устройства — это событие, которое приводит к состоянию сбоя этого устройства.

2 Если потеря способности функционировать вызвана скрытым сбоем, то отказ происходит в условиях определенного набора обстоятельств.

3 Выполнение требуемых функций неизбежно исключает определенное поведение, а некоторые функции могут быть определены в терминах поведения, которого следует не допускать. Случаи такого поведения являются отказами.

4 Отказы могут быть случайными или систематическими.

5 На практике термины «сбой» и «отказ» часто считаются синонимами, несмотря на то, что они по-разному определяются в разных стандартах.

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.18]

2.2.12 **отказ по общей причине** (common-cause failure): Отказ, являющийся результатом одного или нескольких событий, вызывающих отказ двух или нескольких различных каналов мультиканальной системы, ведущий к отказу всей системы в целом.

2.2.13 **отказ общего характера** (common-mode failure): Генерация ошибочного результата, так как отказ в различных каналах может происходить одинаково.

2.2.14 **простой** (downtime): Интервал времени, в течение которого узел находится в неработоспособном состоянии.

Примечание — Продолжительность неработоспособного состояния включает все потери времени, связанные с восстановлением работоспособного состояния узла после отказа.

2.2.15 **частота отказов, интенсивность отказов** (failure rate): Количество отказов узла за единицу времени при заданных условиях его функционирования.

2.2.16 **интервал между отказами** (time between failures): Интервал времени между двумя отказами узла, вернувшегося в рабочее состояние после первого отказа.

Примечание — Значение среднего интервала между отказами используется для оценки степени доступности узла.

2.2.17 **периодическая проверка** (periodic inspection): Проверка, позволяющая обнаружить пассивные сбои приборной системы безопасности.

Примечание — В результате проверки узел восстанавливается, переходит к работе по назначению.

2.2.18 **интервал между проверками** (test interval): Интервал времени между двумя последовательными проверками узла.

2.2.19 **состояние «проверено в эксплуатации»** (proven in use): Демонстрация, основанная на анализе опыта работы определенной конфигурации компонента того, что вероятность опасных систематических отказов компонента настолько низка, что каждая функция безопасности, которую реализует этот компонент, достигает требуемого для нее уровня полноты безопасности.

2.3 Термины, связанные с генерацией и обработкой сигналов

2.3.1 **обработка сигнала** (signal processing): Действие, выполняемое устройствами обработки сигналов, в результате которого комбинируются и обрабатываются различные сигналы датчиков для возможности их использования приводными механизмами и генерации рабочих сообщений.

2.3.2 **датчик** (sensor): Часть BPCS- или SIS-системы, выполняющая измерение и выявление условий протекания процесса.

2.3.3 **приводной механизм** (actuator): Часть приборной системы безопасности, которая непосредственно выполняет операцию вмешательства в производственный процесс и гарантирует его безопасное состояние.

Примечание — Приводной механизм может изменять параметры потока материала (потока энергии) производственного процесса (например, греющего пара). Приводной механизм обеспечивает обработку сигнала. Примеры приводных механизмов: клапан, электромотор, вспомогательные агрегаты и т. п.

2.3.4 **передатчик предельного сигнала** (limit signal transmitter): Узел (программный модуль), который сравнивает текущее значение технологического параметра с его установленным фиксирован-

ным (переменным) предельным значением. Если текущее значение выше (ниже) предельного, то генерируется специальный выходной сигнал.

2.3.5 **предельное значение** (limit value): Значение, при котором инициируется рабочее сообщение и переключение рабочей функции.

2.3.6 **избыточность** (redundancy): Наличие более одного средства для выполнения требующейся функции или для представления информации.

Примечание 1 — Примерами избыточности являются дублирование устройств и добавление битов четности.

Примечание 2 — Избыточность используется в первую очередь для повышения безотказности или готовности.

[ГОСТ Р МЭК 61511-1—2018, статья 3.2.60]

2.3.7 **система с выбором *M* элементов из *N* возможных** (M-out-of-N system): Приборная система безопасности (или ее часть), включающая *N* независимых и соединенных в установленном порядке каналов, *M* из которых достаточно для выполнения требуемой функции.

Примечание — Системы с выбором *M* элементов из *N* возможных обозначаются как системы *M*-out-of-*N* или системы MooN (например, 2oo3, см. ниже).

2.3.8 **отказоустойчивость** (fault tolerance): Способность функционального элемента продолжать выполнять требуемую функцию при наличии сбоев, ошибок функций или отклонений от установленных условий (режимов) работы.

2.3.9 **самоконтроль** (self-monitoring): Регулярное и автоматическое определение того, что все выбранные части устройства безопасности в состоянии функционировать в соответствии с назначением.

2.3.10 **обесточивание по принципу отключения** (de-energize to trip principle): Используется при генерации сигнала, его обработке и передаче. Сигнал об обесточивании приравнивается к аварийному сигналу. Если выходит из строя вспомогательная энергетическая установка (происходит обрыв линии), то указанное действие гарантирует, что воспроизводится (сохраняется) «обесточенное состояние» выходного сигнала (т. е. производится электрическое обесточивание по принципу отключения).

2.3.11 **безопасное положение** (safety position): Состояние, в котором приводной механизм оказывается в отсутствие вспомогательных внешних источников энергии (например, состояние после перехода на внутренние источники энергии).

Примечание — В безопасное состояние можно перейти, его можно сохранить. Как правило, устойчивое состояние производственного процесса с низкими энергетическими затратами ассоциируется с безопасным режимом работы приводных механизмов (например, прерывание входного потока материалов / энергии, увеличение выходного потока материалов / энергии и т. п.).

3 Разработка концепции безопасности

Разработка (развитие) концепции безопасности является итерационным процессом и осуществляется в целях снижения риска функционирования производственной установки, характеризуемой высоким уровнем сложности и разнообразия. Задачами экспертов по безопасности являются:

- систематическая идентификация потенциальных опасностей и сбоев, приводящих к потенциальным опасностям; оценка (воспроизводимым способом) ассоциированного основного риска и его возможных последствий по установленной шкале;
- выделение функций безопасности, обусловленных результатами оценки риска, формулировка соответствующих требований надежности для снижения значений основного риска ниже максимально приемлемого уровня риска.

В добавление к результатам экспертизы свойств материалов, химических реакций и физических взаимодействий в технических системах, разработчику концепции безопасности необходимо владеть следующими эффективными методами поддержки текущей работы:

- метод анализа уязвимостей (идентификация потенциальной опасности);
- метод постадийной оценки риска;
- метод определения мер безопасности, соответствующих имеющемуся риску, постадийное определение степени надежности указанных мер.

В настоящем стандарте системы автоматического управления производственными процессами подразделяются на классы (с точки зрения обеспечения безопасности производственных установок). Приводятся рекомендации в части проектирования, практической реализации, организации работы и функционирования, а также контроль приборных систем безопасности.

В соответствии с принятой классификацией систем автоматического управления производственными процессами (см. раздел 4), процедура, рекомендуемая для обеспечения функционирования приборной системы безопасности, включает нижеследующие дополнительные шаги:

1) оценка существующего риска (см. раздел 5.1);
2) формулировка требований и назначение уровней полноты безопасности (SIL);
3) назначение специальных технических и организационных мер.

Вследствие большого разнообразия производственных установок и неуклонного технологического совершенствования оборудования для систем автоматического управления не представляется возможным раз и навсегда установить единые правила практической реализации и контроля в каждом конкретном случае. По этой причине, задачей исполнителей является отыскание наиболее приемлемых решений для конкретных проблем в зависимости от результатов проводимой экспертизы в соответствии с настоящим стандартом.

При применении настоящего стандарта предполагается, что в ходе этапов разработки, установки и функционирования систем автоматического управления производственными процессами соблюдаются все нормативно-технические документы, технические нормы по предотвращению происшествий, соответствующие национальные стандарты и прочие документы.

Концепция безопасности каждой конкретной установки должна быть задокументирована в форме правил и требований техники безопасности.

4 Классификация функций и систем автоматического управления производственными процессами

Практика обеспечения безопасности производственных установок с помощью технологий автоматического управления производственным процессами делает понятными различия между функциями безопасности и функциями управления. По данной причине, системы автоматического управления производственными процессами подразделяют на:

- системы, реализующие функции управления и функции контроля («основные системы управления процессами», BPCS-системы);
- приборные системы безопасности системы, реализующие функции безопасности («приборные системы безопасности», SIS-системы).

Цель данной классификации — обеспечить соответствие конструкции системы автоматического управления производственными процессами требованиям приложений при экономически приемлемых затратах. Это позволяет учесть очевидные ограничения в ходе разработки, установки и функционирования системы и обеспечить модификацию рассматриваемых систем автоматического управления производственными процессами в будущем. Решение по внедрению конкретных приборных систем безопасности, решение по практической реализации их рабочих функций и моделей принимается по результатам оценки безопасности. Необходимо различать:

- функции. Это производственные задачи, которые необходимо решать независимо от конкретной практической реализации. Например, снятие значения конкретной измеряемой переменной, отслеживание ее соответствующего предельного значения и т. п. («приборные функции безопасности», SIF-функции);
- производственные установки и системы. Они используются для практической реализации указанных функций с помощью соответствующего аппаратного обеспечения и, при необходимости, доступного программного обеспечения. Безопасная установка включает датчики, контроллеры, приводные механизмы, необходимое программное обеспечение и т. п.

4.1 Основные системы управления процессами (BPCS-системы)

4.1.1 BPCS-системы

BPCS-системы используются для обеспечения штатного функционирования производственной установки в ее корректном режиме работы. Указанный тип систем реализует функции автоматизации производства. Данные функции включают в себя измерения, управление и техническое нормирование

всех рабочих технологических параметров, включая регистрацию и запись в журнале. Реализуются продвинутые алгоритмы управления, внедряются сложные технологические контроллеры, автоматизированное рецептурное функционирование, эффективные стратегии оптимизации и т. п. Для выполнения указанных функций необходимо обработать большое количество бинарных, цифровых и аналоговых сигналов.

Функции BPCS-системы очень часто (или непрерывно) задействуются в ходе функционирования производственной установки. Персоналом, находящимся на рабочем месте, проводятся проверки достоверности получаемой информации. Отказы или нарушения функционирования должны быть обнаружены немедленно.

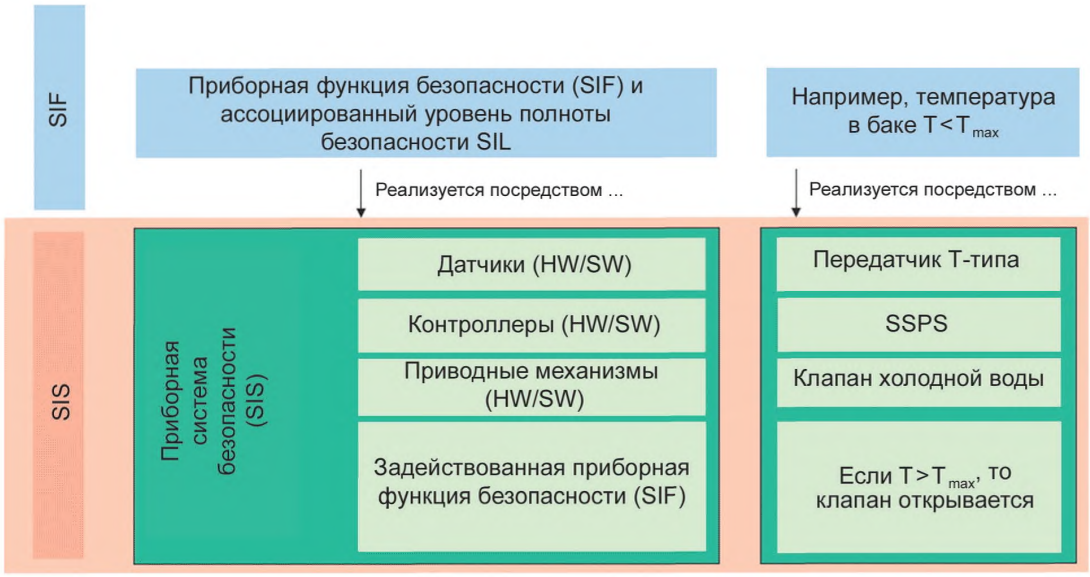


Рисунок 2 — Классификация терминов приборные функции безопасности (SIF) и приборные системы безопасности (SIS)

4.1.2 Системы мониторинга автоматического управления производственными процессами

Система мониторинга автоматического управления производственными процессами срабатывает в ситуации, где один или несколько технологических параметров вышли из корректного диапазона. При этом нет причин прерывать функционирование системы по соображениям безопасности. Система мониторинга срабатывает: 1) при пересечении границы (значений технологических параметров) корректного диапазона, границы допустимого диапазона неисправностей, 2) при попадании значений внутрь допустимого диапазона неисправностей (см. рисунок 3). В этом случае, системы мониторинга производственного процесса регистрируют состояния сбоя производственной установки, привлекают внимание рабочего персонала, инициируют ручное вмешательство оператора или вмешиваются в технологический процесс самостоятельно (автоматически). Значения технологических параметров возвращаются в корректный диапазон. Системы автоматического управления производственными процессами (приборные системы безопасности), занимающие более высокое положение по сравнению с системами ручного управления производственными процессами, определяются как системы мониторинга производственного процесса. Они регистрируют сбои и вмешиваются в технологический процесс автоматически до срабатывания аварийного предохранительного устройства.

Требования к базовым системам автоматического управления производственными процессами и к системам контроля производственных процессов с учетом их конструкции и особенностей функционирования в части обеспечения безопасности производственной установки — отсутствуют. По этой причине в настоящем стандарте они не обсуждаются.

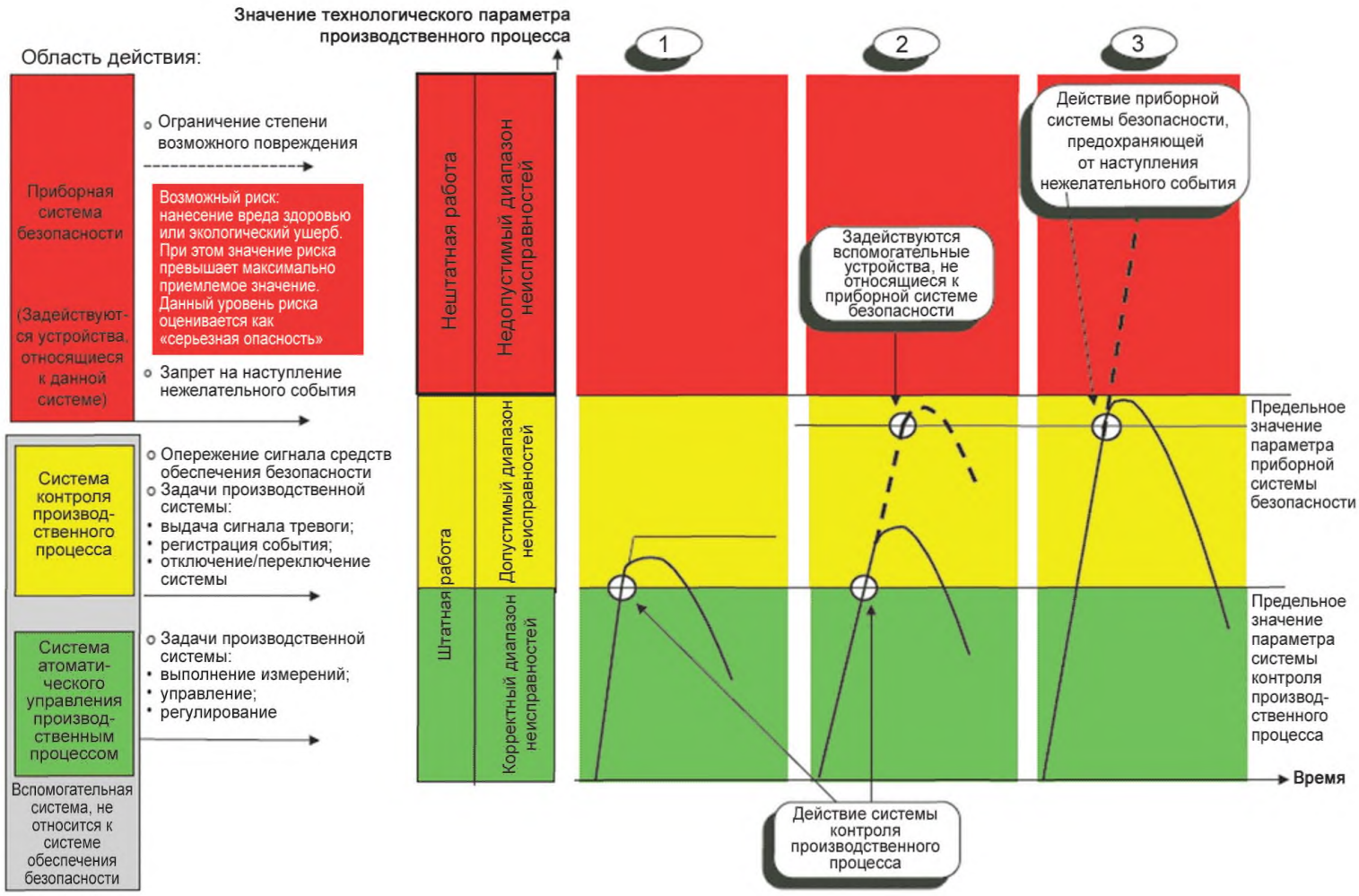


Рисунок 3 — Схематическое представление системы автоматического управления производственными процессами

На кривой 1 технологический параметр не достигает недопустимого диапазона неисправностей по причинам, связанным с особенностями конкретного производственного процесса. Достаточно одной системы контроля производственного процесса. Значение технологического параметра переводится в корректный диапазон автоматически или (после получения специального сигнала) вручную.

На кривой 2 значение технологического параметра пересекает границу недопустимого диапазона неисправностей. Задействуются вспомогательные устройства, не относящиеся к приборной системе безопасности (например, предохранительный клапан, разрывная мембрана, быстрооткрывающийся клапан, быстродействующий запорный клапан и т. п.). По этой причине система автоматического управления производственными процессами верхнего уровня, выдающая предупреждающий сигнал (просто ограничивающая рост значения технологического параметра), рассматривается как система контроля производственного процесса.

На кривой 3 система автоматического управления производственными процессами предотвращает попадание значения рассматриваемого технологического параметра в недопустимый диапазон неисправностей. По этой причине, данная система рассматривается как приборная система безопасности (предотвращающая наступление нежелательного события).

4.2 Приборные системы безопасности (SIS-системы)

SIS-системы уменьшают риски при функционировании производственной установки. SIS-системы задействуются, если:

1) оценка риска травмы рабочего (экологического ущерба) превышает уровень приемлемого риска (степень серьезности опасности);

2) риск не может быть обоснованно исключен из рассмотрения.

Приборная система безопасности уменьшает выявленный риск. Значение остаточного риска должно быть ниже приемлемого. Риск снижается двумя способами, а именно путем:

1) проведения профилактических мероприятий (предотвращения наступления опасного состояния производственной установки);

2) ослабления последствий уже наступившего опасного (критического) события.

Цель профилактических мероприятий приборной системы безопасности — предотвратить наступление недопустимого состояния неисправности производственной установки. Если приборная система безопасности не задействована (предполагается, что таковые всегда имеются в наличии для выполнения оценки безопасности), то:

1) возможно наступление опасного состояния производственной установки, приводящее к травмам рабочих (экологическому ущербу);

2) значение риска превышает приемлемый уровень, а также уровень «серьезная опасность».

Профилактические мероприятия, проводимые приборной системой безопасности, уменьшают значение параметра риска «частота наступления нежелательного события».

Режим «нанесение ограниченного ущерба» приборных систем безопасности — это режим нештатного функционирования. В случае наступления нежелательного события, данный режим работы уменьшает физическое воздействие на персонал и экологию. В данном, крайне редком случае, значение степени повреждения не выходит за установленные пределы.

Режим «нанесение ограниченного ущерба» приборной системы безопасности уменьшает значение параметра риска «степень повреждения», возникающего вследствие наступления нежелательного события. Режим «нанесение ограниченного ущерба» приборной системы безопасности крайне редко используется на практике, так как профилактические мероприятия приборных систем безопасности и меры контроля вспомогательного оборудования обычно уменьшают значение остаточного риска до приемлемой величины. По этой причине, какие-либо дополнительные меры (например, мониторинг состояния наружного воздуха с помощью датчиков и т. п.) по приборной системе безопасности, работающей в режиме «нанесение ограниченного ущерба», не принимаются. Эти меры целесообразны, скорее, для отслеживающего оборудования. Если же (в исключительных случаях) уровень приемлемого риска не достигнут, то 1) режим «нанесения ограниченного ущерба» приборной системы безопасности (во время безопасного цикла долговечности рассматриваемой установки) и 2) профилактические мероприятия данной системы могут использоваться в равной степени. По этой причине, в настоящем стандарте не проводится различие между указанными двумя различными типами приборных систем безопасности.

Важная задача приборной системы безопасности — проверить, в какой степени один или несколько параметров безопасности производственного процесса соответствуют допуску. Если соответствия нет, то:

1) инициируется операция автоматического переключения режима работы;

2) постоянно присутствующий рабочий персонал переводится в состояние готовности совершить необходимые предварительно продуманные действия.

Функции приборной системы безопасности всегда имеют приоритет перед функциями:

1) BPCS-системы;

2) системы контроля производственного процесса.

Данные функции должны выполняться «бок о бок» с технологическим процессом и с наименьшей возможной глубиной проникания в него. Функции приборных систем безопасности запрашиваются крайне редко по сравнению с функциями базовой системы автоматического управления производственными процессами. Это объясняется:

1) низкой вероятностью наступления нежелательного события;

2) «шахматной» компоновкой BPCS-систем, систем контроля производственного процесса и приборных систем безопасности (см. рисунок 3).

С учетом необходимости обеспечения доступности систем, необходимости регулярной проверки достоверности получаемой информации, это может оказаться хорошим решением. Отметим, что запросы на компоненты приборных систем безопасности приходят крайне редко. Такими компонентами, например, могут быть исполнительные элементы, используемые совместно с BPCS-системами. Если указанные компоненты используются совместно, то требования к их конструкции должны отвечать требованиям к приборным системам безопасности.

Системы автоматического управления производственными процессами, предотвращающие повреждение продукта (материала), оценка которых производится в интересах компании, и в которых получение травмы рабочим (экологический ущерб) исключаются, не относятся к приборным системам безопасности и не рассматриваются в настоящем стандарте.

5 Процедура определения требований к приборным системам безопасности

При оценке безопасности всегда необходимо проверять:

1) можно ли реализовать указанную функцию безопасности посредством имеющейся системы автоматического управления производственными процессами;

2) не лучше ли задействовать другие устройства, более целесообразные с практической точки зрения и более экономичные. Вышесказанное относится к конструкциям установок, безопасным по своей природе, и к механическим (структурным) мерам обеспечения безопасности. В нижеследующих разделах данный аспект рассматривается более детально.

Процедуру определения требований к приборным системам безопасности следует начинать с оценки существующего риска (оценки необходимого снижения риска).

Необходимое снижение риска в конкретной ситуации (выраженное качественно или количественно) — это снижение риска до приемлемого уровня (целевое значение безопасности установки) в конкретной ситуации. Концепция необходимого снижения риска имеет принципиальную важность при формулировке требований безопасности к приборным функциям безопасности (SIF). Особенно это касается части функциональной спецификации, определяющей требования полноты безопасности. Определение значения приемлемого риска для конкретных опасных событий позволяет понять, какое требование является обоснованным не только в терминах частоты (вероятности) наступления опасного (критического) события, но и в терминах его последствий. Меры безопасности выбираются из условия минимума частоты наступления опасного события, уменьшения степени серьезности его последствий.

Определяющими факторами оценки приемлемого риска являются также психология восприятия рабочих и мнения сотрудников, подвергающихся опасности. Чтобы определение приемлемого риска могло быть использовано в конкретном приложении, необходимо учесть:

- руководящие указания соответствующих руководящих органов (органов власти);
- результаты обсуждений и соглашения с различными исполнителями, связанные с конкретным приложением;
- промышленные стандарты и руководства;
- рекомендации руководителей промышленных предприятий, специалистов и научного сообщества;
- законодательно закрепленные и официальные технические нормы, относящиеся как в целом, так и в деталях к рассматриваемым приложениям.

Опыт показывает, чем строже технические требования безопасности (чем решительнее принимаемые меры), тем выше ожидаемый риск. Значение риска можно уменьшить, по крайней мере, до приемлемого уровня (до максимально приемлемого значения) за счет мер контроля вспомогательных систем управления, за счет мер обеспечения безопасности автоматического управления производством.

В большинстве случаев приемлемый риск, требования и выбранные меры определяются не только объективными критериями, но и субъективными аспектами.

Настоящий стандарт рассматривает преимущественно требования и меры, обусловленные объективной оценкой рисков.

При некоторых обстоятельствах, приборная система безопасности уменьшает только часть риска, исходящую от производственной установки. Риск, на котором основаны нижеследующие замечания, является парциальным. Он парируется приборной системой безопасности. Оставшаяся часть риска парируется вспомогательной системой управления. Предполагается, что меры включены в производственный процесс. Данная ситуация приведена на рисунке 4.

Меры, реализуемые внутри приборной системы безопасности, могут быть как техническими, так и нетехническими (организационными). Указанные меры взаимно дополняют (заменяют) друг друга. Это означает, что безопасность системы (парирующей парциальный риск автоматического управления производственными процессами, см. рисунок 4) может быть обеспечена различными эквивалентными методами. Например, одно решение с большим числом технических мер может быть эквивалентно другому решению с малым числом технических мер, но с большим числом нетехнических мер организационного характера (см. рисунок 5).

Нетехнические приборные меры безопасности включают, например, проверки производственных функций (регулярно выполняемые операторами), разрешение доступа в помещение только обученному персоналу и т. п.

Рассматриваемые требования определяются непосредственно целями обеспечения безопасности, указанными приложениями, и величиной парциального риска функционирования существующей приборной системы безопасности. Парциальный риск (см. последующие разделы настоящего стандарта) оценивается качественно специальными параметрами риска. Требования определяются SIL-уровнем. Рассматриваемые технические и нетехнические меры, соответствующие указанным требованиям, могут варьироваться. Четкой привязки одного к другому не существует.

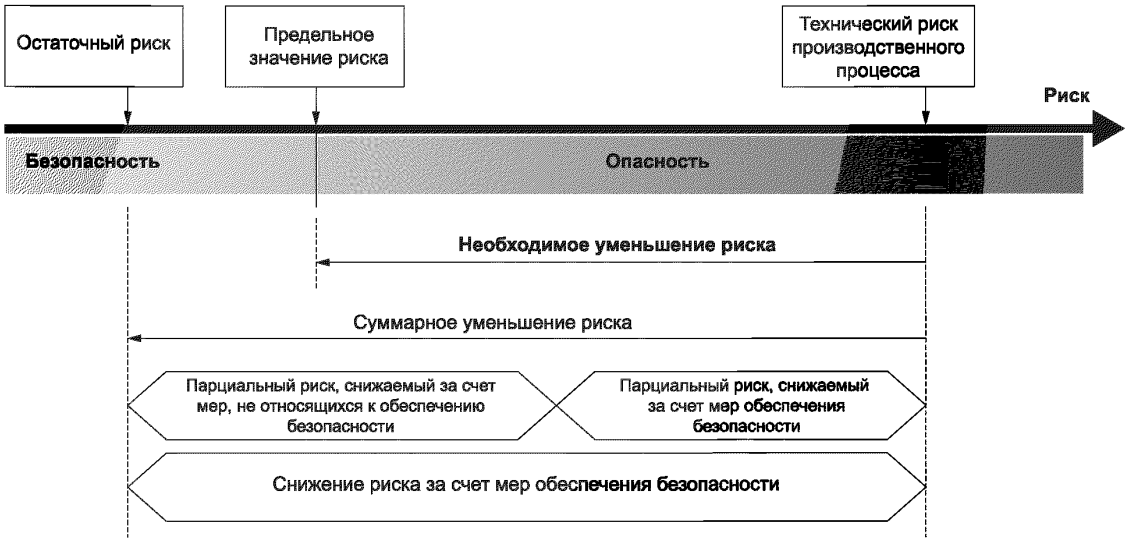


Рисунок 4 — Снижение риска за счет мер безопасности, принимаемых системой автоматического управления производством и вспомогательной системой управления

Существует несколько способов определения необходимого уровня полноты безопасности конкретного приложения. Выбор конкретного способа для конкретного приложения зависит от многих факторов:

- сложности приложения;
- наличия руководящих указаний;
- типа риска, степени необходимого снижения риска;
- опыта и возможностей исполнителя работы;
- наличия информации о параметрах рассматриваемого риска.

Опасности могут быть идентифицированы, например, путем HAZOP-анализа (известен как PAAG-метод).

Риск можно оценивать различными методами. Допускается использование*:

- метода графов риска (качественный, частично количественный);
- ALARP метода (минимальный практически возможный предел риска);
- метода составления матрицы рисков;
- LOPA метода (анализ уровней надежности средств защиты).

Далее подробно рассмотрен качественный метод графов риска.

6 Метод графов риска

В основе метода графов риска лежит допущение, что значение риска пропорционально последствиям и частоте наступления опасного события. Принято, что приборная система безопасности отсутствует. Выполнена установка типовой системы, не связанной с обеспечением безопасности (например, BPCS-системы или системы контроля производственного процесса).

Под последствиями понимаются травмы персонала и экологический ущерб.

* См. ГОСТ Р МЭК 61511-3—2018 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности».

Под частотой наступления события понимается:

- частота попадания в опасную зону, возможная продолжительность воздействия;
- возможность предотвращения опасного события;
- вероятность, с которой наступит опасное событие при условии, что приборная система безопасности отсутствует, но приняты все доступные меры снижения риска. Данная величина называется вероятностью наступления нежелательного события.

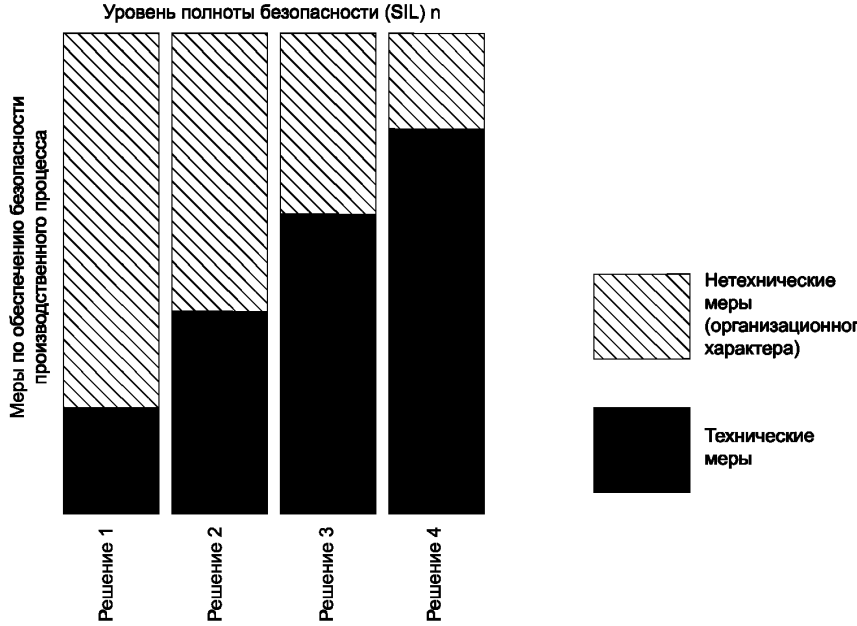


Рисунок 5 — Пропорции парциального риска, парируемого мерами по обеспечению безопасности производственного процесса с помощью технических (нетехнических) средств

Точное определение количественных значений полного риска и парциального риска, как правило, затруднительно. По данной причине, для упрощения в рассмотрение вводятся технологические переменные (параметры). Они дают возможность описать природу и степень серьезности конкретной опасной ситуации в случае отказа приборной системы безопасности или ее отсутствия.

При оценке риска, парируемого приборной системой безопасности, за основу принимается значение риска как при отсутствии приборной системы безопасности. Основными аспектами данного подхода являются анализ природы риска, оценка степени серьезности последствий, оценка ожидаемой частоты наступления недопустимого состояния неисправности производственной установки.

Из широкого перечня параметров, оказывающих влияние на требования безопасности и на выбор мер безопасности, рекомендуется выбрать 4 наиболее важных (смотри ниже). Данные параметры позволяют классифицировать риски и выделить наиболее важные аспекты оценки:

- последствия опасного события;
- частота попадания в опасную зону, умноженная на возможную продолжительность вредного воздействия;
- возможность предотвращения последствий опасного события;
- вероятность наступления нежелательного события.

6.1 Степень повреждения

Данный параметр используется для построения нижеследующих критериев:

а) характер воздействия:
   - штатный персонал (люди);
   - окружающая среда;

б) масштаб воздействия (на людей):
   - один человек;

- несколько человек;
- большое количество людей (катастрофа);

в) серьезность воздействия:
- легкая (обычно излечимая) травма;
- серьезная (обычно неизлечимая) травма;
- смерть.

С учетом вышесказанного в рассмотрение вводится параметр S «Степень повреждения». Параметр S принимает значения:

S1: Легкая травма одного человека, негативное экологическое воздействие;

S2: Серьезная неизлечимая травма одного человека, нескольких человек, смерть одного человека, временное серьезное негативное экологическое воздействие;

S3: Смерть нескольких человек, продолжительное серьезное негативное экологическое воздействие;

S4: Катастрофические последствия, очень много жертв.

Примечание 1 — Если параметр S принимает значения S1-S4, то последствия происшествий являются ожидаемыми. Процедуры медицинского обслуживания производственного процесса являются штатными.

Примечание 2 — При оценке экологического ущерба оцениваются значения параметра A «Продолжительность воздействия» и параметра G «Предупреждение опасности».

6.2 Присутствие в опасной зоне

Использование данного параметра позволяет ввести в рассмотрение нижеследующие критерии: присутствие в опасной зоне (продолжительность воздействия, частота попадания в опасную зону):
- редко;
- часто;
- очень часто, постоянно.

С учетом вышесказанного, параметр A «Продолжительность воздействия» принимает значения:

A1: редкое, нечастое присутствие в опасной зоне;

A2: очень частое, постоянное присутствие в опасной зоне.

6.3 Предупреждение об опасности

Использование данного параметра позволяет ввести в рассмотрение нижеследующие критерии:

а) функционирование производственного процесса:
- функционирование под контролем (контроль может выполняться экспертом или не экспертом);
- функционирование без обеспечения контроля;

б) появление или нарастание опасности (во времени):
- внезапно, быстро;
- медленно;

в) обнаружение опасности:
- прямым наблюдением;
- с помощью технических средств (измерительными инструментами);
- без технических средств.

г) обнаружение опасности (например, оценка возможности необнаружения):
- возможно;
- возможно с ограничениями;
- невозможно.

д) практический опыт обеспечения безопасности (производственного процесса, оборудования и т. п.):
- один и тот же производственный процесс (производственный процесс, знакомый рабочему);
- сопоставимый производственный процесс;
- отсутствие опыта обеспечения безопасности производственного процесса.

Примечание — Критерии «Обнаружение опасности» и «Практический опыт обеспечения безопасности» имеют объективную природу. Они косвенно учитываются при определении рассматриваемого параметра.

С учетом вышесказанного, параметр G «Предупреждение опасности» принимает нижеследующие значения:

G1: Возможно при особых условиях;

G2: Практически невозможно.

6.4 Вероятность наступления нежелательного события

Данный параметр позволяет ввести в рассмотрение нижеследующие критерии.

Вероятность наступления нежелательного события в отсутствие приборной системы безопасности:

- очень низкая;
- низкая;
- относительно высокая.

С учетом вышесказанного, параметр W «Вероятность наступления события» принимает нижеследующие значения:

W1: Очень низкая вероятность наступления нежелательного события. Это означает, что в рассматриваемом производственном процессе (в сопоставимых производственных процессах без приборной системы безопасности) ожидаемо наступление очень небольшого количества нежелательных событий.

W2: Низкая вероятность наступления нежелательного события. Это означает, что в рассматриваемом производственном процессе (в сопоставимых производственных процессах без приборной системы безопасности) ожидаемо наступление нескольких нежелательных событий.

W3: Относительно высокая наступления нежелательного события. Это означает, что в рассматриваемом производственном процессе (в сопоставимых производственных процессах без приборной системы безопасности) нежелательные события наступают достаточно часто.

Если опыта работы с рассматриваемыми производственными процессами (с сопоставимыми производственными процессами) очень мало или опыт отсутствует, то оценка вероятности наступления нежелательного события приводится с расчетом. Рекомендуется выбирать значение параметра W с запасом.

6.5 Прочие возможные параметры риска

Параметры риска, введенные в разделах 6.1—6.4, берут свое начало из рассмотрения большого количества аспектов, оказывающих существенное влияние на оценку ситуаций с риском. Кроме того, существуют аспекты, обосновывающие введение дополнительных параметров риска. Это, например, использование новых технологий в приборных системах безопасности в производственном процессе. Указанные дополнительные параметры риска могут усилить или ослабить установленные требования.

Каждая комбинация параметров риска — это «пакет оценок риска». В соответствии с имеющейся классификацией, существуют 48 комбинаций параметров риска. Вместе с тем, анализ большого числа различных моделей показал, что, вследствие преобладания некоторых параметров риска, количество практически значимых комбинаций значительно меньше 48.

Известно, что для первых трех параметров S, A и G практическую значимость имеют только 8 комбинаций. Данные комбинации (классы требований) и их соответствующие уровни SIL приведены на рисунке 6. Из данного рисунка следует, что для параметров риска S1, например, практически значимыми требованиями к приборной системе безопасности являются требования относительно низкого уровня. Соответствующая настройка системы, теоретически связанная с изменениями параметров риска G и A, не имеет практической значимости.

Для происшествий с серьезными последствиями, особенно событий со значением параметра риска S4, параметры G и A играют подчиненную роль. При формулировке требований безопасности они практически не учитываются.

Пример — Если от производственной единицы исходит крайняя опасность, и если приборная система безопасности вышла из строя, то рабочий постоянно находится в опасной зоне. Поэтому параметр A можно не учитывать. Кроме того, возможность устранить опасность в некоторых обстоятельствах, как правило, не является серьезным аргументом за ослабление требований безопасности на производстве.

Изменение параметра W приводит к снижению SIL-уровня вследствие уменьшения вероятности наступления нежелательного события.

7 Уровень полноты безопасности (SIL)

В целях обеспечения безопасности, параметры риска должны соответствовать установленным требованиям.

Уровень полноты безопасности (от 1 до 4) можно определить по достоверным значениям технологических параметров.

Чем выше SIL-уровень, тем 1) больше парциальный риск, парируемый приборной системой безопасности, 2) тем строже требования и принимаемые меры обеспечения безопасности.

Из графа рисков (для высоких рисков) следует:

- если приборная система безопасности имеет SIL-уровень равный 4, то должны быть установлены дополнительные требования безопасности. По этой причине в настоящем стандарте рекомендуется парировать соответствующий риск мерами безопасности вспомогательной системы управления;
- в настоящее время пока не представляется возможным предотвращать события с катастрофическими последствиями (S4) и относительно высокой вероятностью наступления нежелательных событий (W3) только за счет приборной системы безопасности. Системы автоматического управления производственными процессами, в лучшем случае, играют только вторичную роль.

8 Определение требований

Приборная система безопасности (работающая как в режиме профилактики, так и в режиме ограничения ущерба) всегда имеет, по крайней мере, уровень SIL 1.

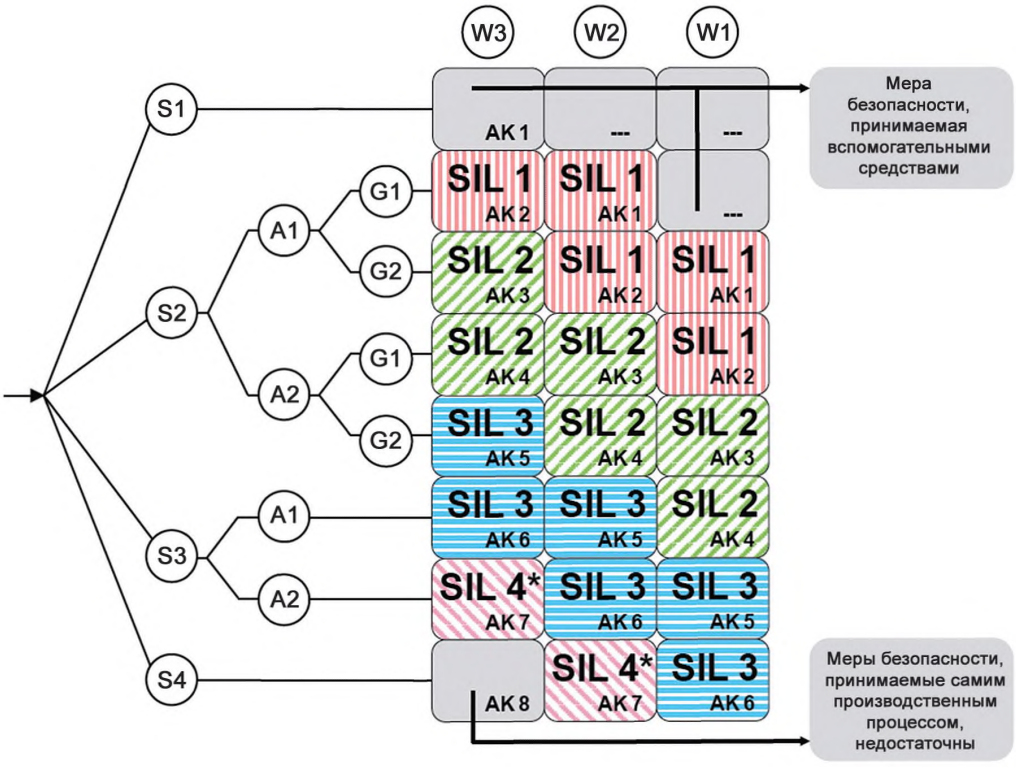


Рисунок 6 — Граф риска ассоциирует значения параметров риска с SIL-уровнями

На рисунке 6:

- S — степень повреждения:
  S1: легкая травма рабочего, слабое негативное экологическое воздействие;

S2: серьезная неизлечимая травма одного или нескольких рабочих, смерть одного рабочего, временные серьезные негативные воздействия на экологию;

S3: смерть нескольких рабочих, продолжительное негативное экологическое воздействие;

S4: катастрофические последствия, очень много жертв;

- A — продолжительность воздействия:

A1: от «редко» до «часто»;

A2: от «часто» до «постоянно»;

- G — предупреждение опасности:

G1: возможно при особых условиях;

G2: практически невозможно;

- W — вероятность наступления нежелательного события:

W1: очень низкая;

W2: низкая;

W3: относительно высокая.

- АК — класс требований.

Примечание — Обеспечение уровня безопасности SIL 4 требует чрезмерных затрат. По возможности его следует избегать. Требования к приборным системам безопасности (с учетом их поведения при наступлении сбоя) установлены в ГОСТ Р МЭК 61511.

В таблице 1 приведены оценки вероятности отсутствия сбоя в зависимости от значения SIL-уровня. Данные оценки основаны на результатах анализа частоты отказов компонентов системы автоматического управления производственными процессами.

Таблица 1 — SIL-уровни и соответствующие вероятности отсутствия сбоя

SIL	Вероятность опасного отказа (коэффициент отказа U)	Коэффициент готовности ($V = 1 — U$)
1	$= 10^{-2} < 10^{-1}$	0,9...0,99
2	$= 10^{-3} < 10^{-2}$	0,99...0,999
3	$= 10^{-4} < 10^{-3}$	0,999...0,9999
4	$= 10^{-5} < 10^{-4}$	0,9999...0,99999

В отраслях промышленности со сложными рабочими условиями (например, на прибрежных сооружениях, нефтехимических предприятиях, объектах атомной энергетики и т. п.), математическое обоснование вышеуказанных соотношений выполнить затруднительно. Очень сложно получить взаимозависимости между конкретными частотами отказов производственных единиц и многообразием условий функционирования.

По этой причине для данных условий далее приведена альтернативная процедура.

Приборные системы безопасности разрабатываются и используются так, чтобы гарантировать безопасность, несмотря на возможное наступление пассивных сбоев устройств безопасности. Для этого конкретного случая в нижеследующих двух разделах настоящего стандарта устанавливаются соответствующие требования.

Даже с учетом установленной процедуры, необходимо приводить доказательство соответствия вышеуказанному требованию отсутствия сбоя. Возможная процедура приведена далее:

- все приборные системы безопасности разрабатываются, изготавливаются и работают в соответствии с настоящим стандартом*;
- для всех приборных систем безопасности данные отказов должны регистрироваться;
- требования к SIL-уровню формулируются для коллективных систем.

Следование вышеуказанным требованиям подтверждает достоверность рассматриваемой концепции безопасности.

8.1 Требования пониженного уровня риска (уровни SIL 1 и SIL 2)

Пассивный сбой обнаруживается и корректируется в течение интервала времени, когда одновременные нарушения штатной работы оборудования не ожидаются.

* См. также комплекс стандартов ГОСТ Р МЭК 61511.

Это означает, что одноканальная конструкция приборной системы безопасности применяется тогда, когда в производственном процессе используется проверенное на практике оборудование.

Примечание 1 — Вышесказанное подтверждает требования отказоустойчивости к сбоям аппаратных средств, установленные в ГОСТ Р МЭК 61511. Если аппаратура сложная или недостаточно проверена на практике, то степень ее избыточности устанавливается в соответствии с ГОСТ Р МЭК 61511.

Примечание 2 — В некоторых производственных установках, снижение уровня безопасности в результате нештатного использования оборудования обычно не зависит от возможного пассивного сбоя приборной системы безопасности. Вероятность одновременного наступления сразу двух указанных событий достаточно низка. Поэтому интервал времени между двумя регулярными проверками должен быть достаточно коротким, чтобы максимально уменьшить вероятность наступления пассивного сбоя приборной системы безопасности.

8.2 Требования повышенного уровня риска (SIL 3)

Пассивный сбой не должен уменьшать способность приборной системы безопасности выполнять свои функции по назначению. Сбой обнаруживается и устраняется в ходе производственного процесса. Время устранения сбоя должно быть малым настолько, чтобы вероятность наступления (в это время) второго независимого сбоя была достаточно малой.

Чтобы оборудование имело состояние «проверено на практике», приборная система безопасности проектируется с запасом (по показателям 1oo2, 2oo3).

Примечание — Вышесказанное иллюстрирует требование отказоустойчивости к сбоям аппаратных средств, установленное ГОСТ Р МЭК 61511. Если аппаратура сложная или недостаточно «проверена на практике», то повышенная степень ее избыточности (дублирования) обеспечивается в соответствии с ГОСТ Р МЭК 61511.

Приложение А
(справочное)

Цикл работ со сбоями

А.1 Анализ и типы сбоев

Если приборная система безопасности уменьшает риск до приемлемого уровня, то, соответственно, вероятность наступления нежелательного события уменьшается. На практике не бывает оборудования, работающего без отказов. Поэтому должна быть выявлена связь между возможными сбоями приборной системы безопасности и вероятностью наступления соответствующих нежелательных событий. Следует изучить возможные сбои приборной системы безопасности, и оценить их влияние на функции безопасности.

Все возможные сбои (все сбои, которые нельзя исключить из рассмотрения) подразделяются на сбои:

- не оказывающие влияние на функции безопасности;
- оказывающие влияние на функции безопасности.

Сбои, не оказывающие влияние на функции безопасности, в настоящем стандарте не рассматриваются.

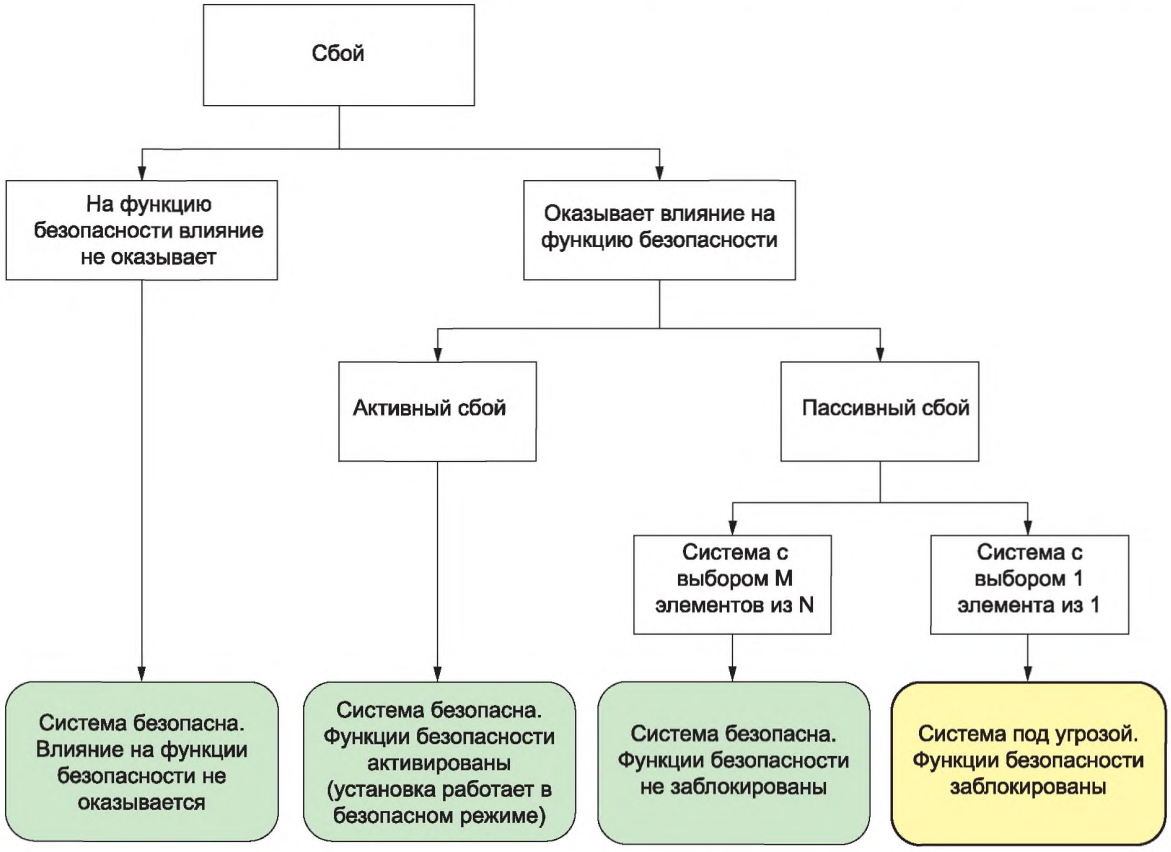


Рисунок А.1 — Типы сбоев и их влияние на функции безопасности

В соответствии с их спецификацией (с учетом одноканальной структуры) сбои, оказывающие влияние на функции безопасности, подразделяются на «активные сбои» (см. 2.2.6) и «пассивные сбои» (см. 2.2.7).

Из приведенных определений сбоев следует, что действующие сбои одноканальных приборных систем безопасности снижают вероятность отсутствия сбоя технического оборудования (производственного процесса), но не саму безопасность. Пассивные сбои влекут наступление опасного рабочего состояния. Требуемой реакции оборудования, при необходимости, можно и не получить.

Указанные утверждения допускают, что рассматриваемое техническое оборудование и установки всегда имеют стационарное безопасное состояние, в которое можно мгновенно перейти.

Сбои, последствия которых плохо поддаются определению, следует считать пассивными. Вероятность наступления пассивных сбоев приборных систем безопасности в значительной степени определяет уровень остаточного риска в технических системах.

В следующем разделе пассивные сбои подразделяются на различные типы, соответствующие причинам их наступления. Данная классификация позволяет назначить количественные меры указанным типам сбоев.

Рабочие сбои — это сбои, возникающие вследствие некорректного применения (нарушения правил функционирования) приборной системы безопасности;

- систематические сбои аппаратуры, возникающие вследствие:
- ошибок в спецификациях и дефектов изготовления;
- недостатков конструкции и некорректной организации производства;
- неправильной установки аппаратуры;
- сбои при техническом обслуживании;
- сбои, обусловленные модификацией предохранительного устройства;
- случайные сбои аппаратуры, а именно:
- случайные сбои, возникающие без внешнего воздействия (например, отказы компонентов);
- случайные сбои, возникающие в результате внешнего воздействия (например, электромагнитного возмущения, нагрева, влажности, приложенной силы и т. п.);
- ошибки программного обеспечения:
- ошибки спецификации;
- ошибки компьютерных программ;
- ошибки пользователя.

А.2 Предотвращение и контроль сбоев

А.2.1 Общая информация

Число пассивных сбоев должно быть сведено к минимуму. Необходимо задействовать все возможные средства предотвращения сбоев. Если сбои неизбежны, то необходимо заранее планировать работу по их устранению.

А.2.2 Предотвращение сбоев

Главной целью мер по предотвращению сбоев является предотвращение наступления неизбежных сбоев во время функционирования приборной системы безопасности. Меры предотвращения сбоев, принятые для одной приборной системы безопасности, могут быть приняты и для других приборных систем безопасности аналогичного типа. Соответственно, заранее должны быть предусмотрены особые затраты на функционирование конкретной приборной системы безопасности.

Все факторы, приводящие к наступлению сбоев, учитываются техническими и нетехническими мерами предотвращения сбоев с начала разработки приборной системы безопасности и до момента ввода ее в эксплуатацию.

Технические меры предотвращения сбоев включают, например, все меры, снижающие риск наступления сбоя, обусловленной внешними воздействиями. Данные меры (превышение размеров деталей и т. п.) уменьшают частоту наступления случайного сбоя во время функционирования.

Такие меры, как проверки в ручном режиме, позволяющие обнаружить и устранить сбой, относятся, главным образом, к систематическим сбоям и мерам нетехнического характера.

А.2.3 Контроль сбоев

Все сбои, возникающие во время функционирования приборной системы безопасности, работавшей ранее безотказно (обычно это сбои компонентов), могут быть выявлены только путем специальных контрольных процедур. Контрольные процедуры выявляют, главным образом, случайные сбои.

Цель контроля сбоев — устранить их возможные неблагоприятные последствия на производстве, не допустить снижения уровня безопасности. Основная характеристика мер контроля сбоев — уровень необходимых затрат на обеспечение функционирования приборной системы безопасности.

Технические меры контроля сбоев включают, например, использование дублирующих структур, проведение специальных проверок в режиме работы оборудования и т. п. Нетехнические меры контроля сбоев включают, например, периодические проверки приборных функций безопасности в ручном режиме.

А.2.4 Комбинации мер безопасности

Если одной конкретной меры недостаточно для уменьшения вероятности наступления пассивного сбоя до приемлемо низкого уровня, то принимается заранее подготовленная комбинация мер (пакет мер безопасности).

Если, например, принята только одна мера «дублирование», то после достаточно продолжительного времени все (в том числе и задублированные) каналы могут оказаться заблокированы пассивными сбоями. По этой причине, может оказаться необходимой дополнительная мера «обнаружение сбоев».

А.2.5 Оценка конкретных мер

В таблице А.1 представлены: 1) меры предотвращения сбоев, 2) меры контроля сбоев. Это функции различных типов сбоев и их причин.

При рассмотрении мер предотвращения сбоев необходимо различать меры штатные, простые, средней сложности и высокотехнологичные. Штатные меры принимаются по стандартам качества для технологий автоматического управления производственными процессами в приложениях, не связанных с обеспечением безопасности. По данной причине, штатные меры не ставятся в соответствие каждому конкретному типу сбоев. Они указываются только в случаях, когда обеспечение соответствия стандартам качества не является общей практикой.

Простые и высокотехнологичные меры — это чаще всего меры контроля сбоев. В настоящем стандарте принято, что меры контроля сбоев не принимаются по стандартам качества для технологий автоматического управления производственными процессами в приложениях, не связанных с обеспечением безопасности.

А.3 Своевременность принятия мер контроля сбоев

Эффективность мер контроля сбоев зависит от своевременности обнаружения пассивного сбоя, своевременности ее устранения, своевременности перевода производственного процесса в безопасное состояние.

Максимально допустимое время обнаружения и устранения указанной пассивного сбоя зависит, с одной стороны, от требований к производственному процессу, а, с другой стороны, от его структуры (степени избыточности) и принятии мер обнаружения сбоя приборной системы безопасности.

А.3.1 Время отказоустойчивости производственного процесса

Требования своевременности принятия мер для производственного процесса определяются его динамикой и временем отказоустойчивости к сбоям. Данные требования зависят от частоты наступления состояний производственного процесса, требующих вмешательства приборной системы безопасности. На временной диаграмме, представленной на рисунке А.2, принято, что возникшая проблема (сбой системы автоматического управления производственными процессами, вызванная отказом приборной системы безопасности) после истечения времени отказоустойчивости производственного процесса к сбою влечет опасные последствия.

Таблица А.1 — Оценка конкретных мер как функция типа сбоя (примеры)

1 Сбой функционирования	Штатные: определение указанной операции, стандартная конструкция с руководством пользователя	
	Простые: обеспечение безопасности путем ограничения доступа, разрешение доступа только специально обученному персоналу	Простые: проверка достоверности рабочего состояния, проверка разрешения на доступ, вывешивание предупреждений
	Высокотехнологичные: профилактика неправильного использования, исключение постороннего вмешательства (не саботаж), работа пользователей запрещается	Высокотехнологичные: проверка достоверности рабочего состояния, проверка разрешения на доступ, задействование функции блокировки
2 Систематические сбои аппаратных средств		
2.1 Несовершенства конструкции	Штатные: использование оборудования, прошедшего типовые испытания	
	Простые: периферийные устройства — устройства «проверенные в эксплуатации», устройства с сертификатом уровня безопасности SIL, с сертификатом безопасности SSPS	
		Высокотехнологичные: разнотипное дублирование
2.2 Ошибки планирования	Простые: проверка рабочих функций при вводе в эксплуатацию, при приемке	

Продолжение таблицы А.1

Тип сбоя	Классификация мер	
	Предотвращение сбоя	Контроль сбоя
	Высокотехнологичные: проверка уровня безопасности лицами, не связанными с планированием производственного процесса	Высокотехнологичные: регулярные проверки в ручном режиме
2.3 Ошибки при установке	Простые: проверка уровня безопасности по окончании установки	
	Высокотехнологичные: проверка уровня безопасности лицами, не связанными с установкой	
3 Сбои технического обслуживания	Простые: проверка соответствия защитной функции оборудования требованиям специальной инструкции. Проводится специалистом по техническому обслуживанию данного оборудования	
	Высокотехнологичные: проверка соответствия защитной функции оборудования требованиям специальной инструкции. Проводится лицами, не связанными с техническим обслуживанием данного оборудования	
4 Сбои, обусловленные модификацией устройства обеспечения безопасности	Совершенствование конструкции устройства обеспечения безопасности	
5 Случайные сбои периферийных устройств		
5.1 Случайные внутренние сбои	Штатные: общие меры по обеспечению качества работ	
	Простые: выбор компонентов, превышение размеров, предотвращение факторов напряжения и т. п.	Простые: одноканальные с проверкой
	Высокотехнологичные: выбор оборудования с надежностью, подтвержденной опытной эксплуатацией (аппаратура, проверенная в работе), использование оборудования с сертификатом уровня безопасности SIL	Высокотехнологичные: мультиканальные с проверкой, одноканальные с сертификатом уровня безопасности SIL
5.2 Случайные неисправности, обусловленные внешними причинами	Простые: меры, учитывающие маловероятные причины сбоев	Простые: одноканальные с проверкой
	Высокотехнологичные: меры, учитывающие маловероятные причины сбоев	Высокотехнологичные: мультиканальные с проверкой, разделение в пространстве

Окончание таблицы А.1

Тип сбоя	Классификация мер	
	Предотвращение сбоя	Контроль сбоя
6 Систематические сбои программного обеспечения		
6.1 Сбои спецификации	Штатные: грамотно структурированные и правильно оформленные спецификации, структурированный дизайн, модульная структура программ, наличие ограничений на диапазон решаемых задач по каждому модулю	
	Простые: дополнительно — проверка спецификации, разбиение задач на модули, обеспечение соответствия конструкции требованиям безопасности, отказ от «старья», использование только сертифицированных инструментов	Простые: логический мониторинг программ, мониторинг программ, привязанный ко времени
	Средней сложности: дополнительно — использование электронных спецификаций и документов, составление ведомости технического контроля и т. п.	
	Высокотехнологичные: дополнительно — методическое проектирование, например, с помощью специального языка, методов проектирования, признаков достоверности, проверки независимыми лицами	Высокотехнологичные: дополнительно — проверка доступа, проверка авторизации, проверка корректности данных, проверка достоверности
6.2 Ошибки программирования	Штатные: соответствие требованиям к разработке программного обеспечения, структурирование программы, использование модулей	
	Простые: дополнительно — инструменты программирования, проверка структуры, систематические тесты, обеспечение доступа с помощью специальных процедур	Простые: логический мониторинг программ, мониторинг программ, привязанный ко времени
	Средней сложности: дополнительно — проверки и тесты (например, пошаговый разбор программы), защитное программирование	
	Высокотехнологичные: дополнительно — пробное моделирование, специальные проверки	Высокотехнологичные: дополнительно — проверка доступа, проверка авторизации, проверка корректности данных, проверка достоверности, проверка разновидности ПО
6.3 Сбои практической реализации	Штатные: ограничение области применения компьютерной программы, устранение опасных команд, тесты программ	
	Простые: дополнительно: использование специальных операционных систем для конкретных приложений, проверка кодов, систематическое тестирование ПО, проверка соответствия установленным требованиям практической реализации	Простые: логический мониторинг программ, мониторинг программ, привязанный ко времени

А.3.2 Своевременность регулярных проверок приборной системы безопасности

Пассивные сбои установок, обеспечивающих безопасность, можно обнаружить путем проверок.

Сбои установок, обеспечивающих безопасность, обнаруживаются периодическими проверками. Интервалы

между проверками должны быть достаточно короткими: отказ установки, обеспечивающей безопасность, и запрос на вмешательство в производственный процесс не должны происходить одновременно в интервале времени между проверками (типовой интервал времени между испытаниями — один год).

Если рассматриваемая установка, обеспечивающая безопасность, имеет автоматическую диагностику, то время обнаружения сбоя значительно сокращается (обычно несколько секунд). К сожалению, область применения автоматической диагностики меньше области применения периодических испытаний.

При активном сбое время реакции системы на сбой — это время между моментом наступления сбоя и моментом перевода производственного процесса в безопасное состояние. В идеале, время обнаружения сбоя не должно превышать время обработки результата измерения (см. рисунок А.2). Рисунок А.2 рекомендуется принимать во внимание при настройке времени реакции системы на сообщение о наступлении сбоя.

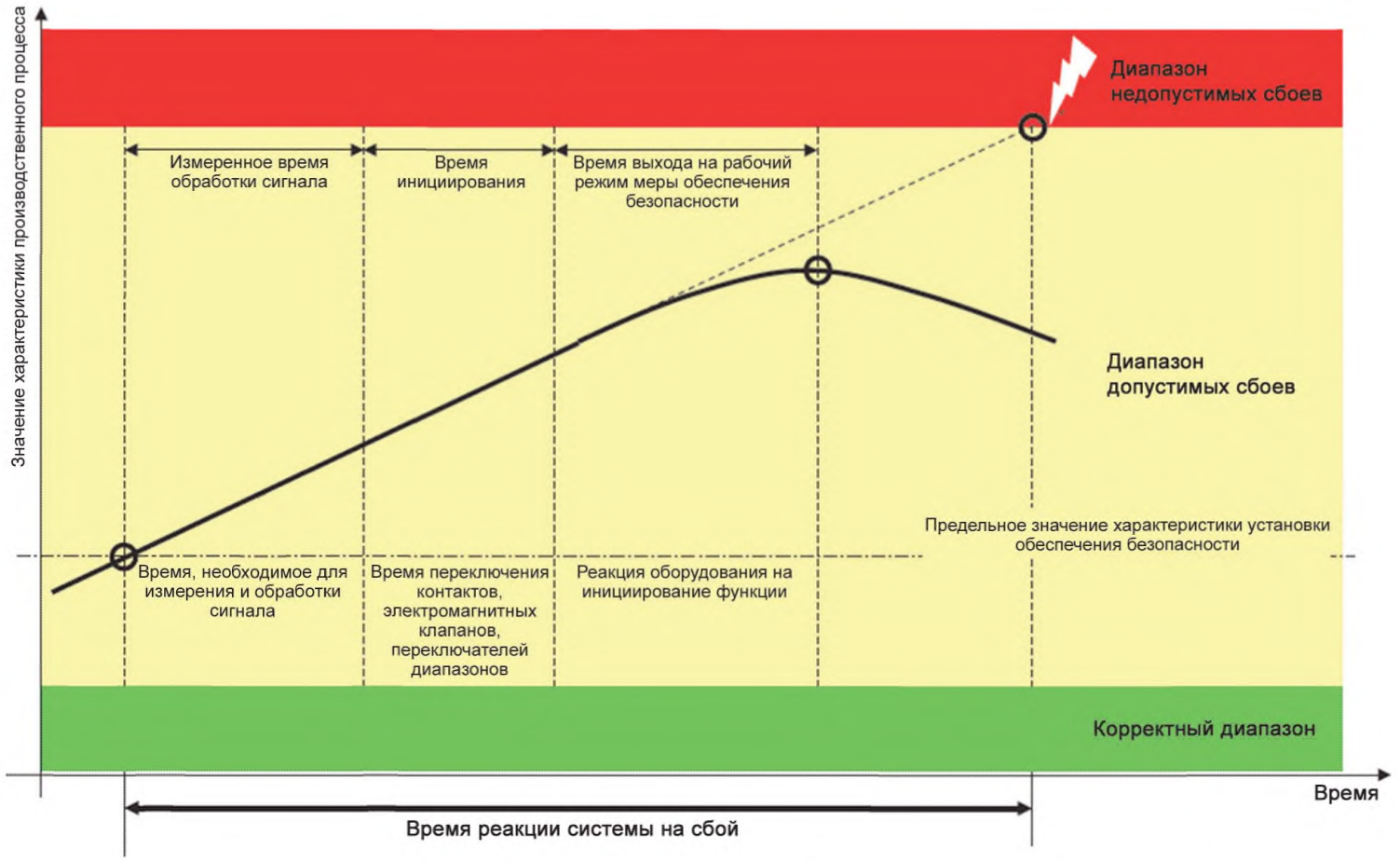


Рисунок А.2 — Отказоустойчивость производственного процесса. Производственный процесс переводится в безопасное состояние с помощью (активированной) приборной системы безопасности



Рисунок А.3 — Время обнаружения и устранения сбоев при последовательных регулярных проверках

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; планирование функциональной безопасности; уровень полноты безопасности

БЗ 10—2019/146

Редактор *Г.Н. Симонова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 24.09.2019. Подписано в печать 04.10.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,36.
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