ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72336— 2025/ IEC TR 63176:2019

Системы процессной аналитической технологии как часть инструментальных систем безопасности

(IEC TR 63176:2019, IDT)

Издание официальное

Москва
Российский институт стандартизации
2025

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 октября 2025 г. № 1238-ст

4 Настоящий стандарт идентичен международному документу IEC TR 63176:2019 «Системы процессной аналитической технологии как часть инструментальных систем безопасности» (IEC TR 63176:2019 «Process analysis technology systems as part of safety instrumented systems», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

Введение

Настоящий стандарт разработан в качестве рекомендации для пользователей анализаторов технологического процесса, которые устанавливают средства измерения как часть систем безопасности, и должен рассматриваться исключительно как рекомендация. Формулировки обязательного характера, встречающиеся в настоящем стандарте, обусловлены содержанием, связанным с безопасностью. Тем не менее, в целом сохраняется рекомендательный характер настоящего стандарта. Измерительное оборудование анализаторов технологического процесса используется, например, в обрабатывающей промышленности в качестве сенсорных компонентов приборных систем безопасности. Во многих случаях они представляют собой единственный или наиболее эффективный метод мониторинга параметра процесса, который, со своей стороны, позволяет надежно оценить целевое использование защищаемой системы. Из-за непосредственного взаимодействия материала с технологической средой измерительное оборудование анализаторов технологического процесса в целом более подвержено отказам и требует дополнительного обслуживания по сравнению с широко используемыми датчиками для измерения давления, температуры, уровня заполнения и расхода. Вследствие этого взаимодействия невозможно полностью избежать систематических отказов. Данная проблема обычно устраняется путем проверки измерительного оборудования через короткие регулярные интервалы.

Разнообразие переменных и методов аналитического измерения процесса и следовательно сравнительно ограниченное количество измерительных устройств для анализа технологического процесса, используемых в каждом случае для одного, строго ограниченного приложения, в большинстве случаев затрудняет количественную оценку функциональной безопасности в соответствии с МЭК 61511. Помимо часто некорректных спецификаций производителей для оценки компонентов как систем безопасности количество существующих сопоставимых применений недостаточно. Тем не менее специалистами по анализу процессов за последние 30 лет были успешно реализованы несколько сотен приборных систем безопасности на основе анализаторов технологического процесса с использованием измерительного оборудования анализаторов технологического процесса.

В настоящем стандарте предлагаются меры в тех областях, где нормативные требования не могут быть выполнены или выполняются ненадлежащим образом. Эти меры при их аккуратном применении приводят к эквивалентному уровню безопасности.

Требования, касающиеся функциональной безопасности электрических и электронных систем, описаны в МЭК 61508 и конкретизированы для приборных систем безопасности для сектора перерабатывающей промышленности в МЭК 61511. Целью настоящего стандарта является описание процедуры использования измерительных устройств анализаторов технологического процесса как части приборной системы безопасности в форме руководства.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системы процессной аналитической технологии как часть инструментальных систем безопасности

Process analysis technology systems as part of safety instrumented systems

Дата введения — 2026—01—01

1 Область применения

Настоящий стандарт содержит рекомендации по планированию, установке и эксплуатации (включая техническое обслуживание) измерительного оборудования анализаторов технологического процесса в приборных системах безопасности обрабатывающей промышленности. Он охватывает все необходимые этапы для квалификации оборудования безопасности и развивает менеджмент безопасности оборудования приборных систем безопасности посредством добавления специальных требований к оборудованию для анализаторов технологического процесса. Настоящий стандарт не рассматривает в полном объеме менеджмент безопасности для оборудования приборных систем безопасности.

Термин «квалификация», используемый в настоящем стандарте, относится исключительно к проверке соответствия систем анализа технологического процесса для использования в устройствах приборных систем безопасности. Этот термин отличается от термина «квалификация», используемого в фармацевтической среде.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения к нему)]:

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью)

IEC 61508-6:2010, Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3)

IEC 61511 (all parts), Functional safety — Safety instrumented systems for the process industry sector (Безопасность функциональная. Системы безопасности приборные для промышленных процессов)

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

IEC 61326-3-1:2017, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — General industrial applications [Электрическое оборудование для измерения, управления и лабораторного применения. Требования ЭМС. Часть 3-1. Требования помехоустойчивости для систем, связанных с безопасностью, и оборудования, предназначенного

Издание официальное

для выполнения функций, связанных с безопасностью (функциональная безопасность). Общие промышленные применения]

IEC 61326-3-2:2017, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) — Industrial applications with specified electromagnetic environment [Электрическое оборудование для измерения, управления и лабораторного применения. Требования ЭМС. Часть 3-2. Требования помехоустойчивости для систем, связанных с безопасностью, и оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональная безопасность). Промышленные применения с учетом определенной электромагнитной обстановки]

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

ИСО и МЭК для применения в стандартизации поддерживают терминологические базы данных:

- платформа онлайн-просмотра ИСО, доступная на https://www.iso.org/obp;
- Электропедия МЭК, доступная на http://www.electropedia.org/.

3.1.1 **измерительное оборудование PAT** (PAT measuring equipment): Системы анализа технологического процесса как совокупность всего оборудования и среды, необходимые для реализации функции измерения определенной субстанции.

Примечание — Примерный, но не обязательно полный, список включает в себя оборудование для отбора проб, оборудование для транспортировки проб, оборудование для предварительной подготовки проб, оборудование для рециркуляции проб, анализатор, блоки управления PAT и инфраструктурное оборудование, а также их поставку, эталонные и калибровочные среды и необходимое электропитание. В каждом конкретном случае в помещении или комнате следует предусмотреть необходимый шкаф или место для размещения анализатора.

3.1.2 **базовое испытание** (basic testing): Возможный предварительный выбор подходящего аналитического оборудования для приборных систем безопасности без какой-либо ссылки на конкретную измерительную задачу.

Примечание — Это относится исключительно к испытанию аналитического оборудования в соответствии с критериями, указанными в приложении А.

3.1.3 **прикладное тестирование** (application testing): Тест, который гарантирует, что измерительная задача может быть успешно реализована с помощью системы PAT.

Примечание — Оно включает проверку конфигурации и иногда программного обеспечения измерительного оборудования на соответствие задаче измерения, с учетом влияния обработки образца, особенно его точности, определения влияния матрицы и переменных состояния (давления, температуры, расхода) как для внутренней, так и для внешней среды измерительного оборудования, а также знания о стабильности во времени.

3.1.4 **опыт эксплуатации** (operational experience): Знания, имеющиеся до использования анализатора, включая информацию о необходимых комплектующих для сопоставимых измерительных задач.

Примечание — Следовательно, это включает исключительно опыт, полученный в ходе фактического использования сопоставимого измерительного оборудования для аналогичных задач измерения.

3.1.5 **эксплуатационное испытание** (in-service testing): Контролируемый режим системы PAT как части приборной системы безопасности в процессе производственной эксплуатации.

Примечание 1 — Существует явно выраженное отличие процедуры доказательства эксплуатационных характеристик систем PAT от соответствующей процедуры для оборудования приборной системы безопасности.

Примечание 2 — Проведение испытаний, их график, спецификации для оценки результатов, дополнительные меры для выполнения функции безопасности, часто необходимые во время эксплуатационных испытаний, и ответственный персонал, выполняющий этот этап, должны быть документально оформлены.

3.1.6 **подтверждение эффективности защиты** (proven performance): Совокупность знаний, которая является частью окончательного решения за или против пригодности предлагаемой установки анализатора процесса в качестве части приборной системы безопасности.

Примечание 1 — Подтверждение эффективности защиты будет достигнуто при достаточном опыте эксплуатации, включая подтверждение соответствия задаче измерения. Если это невозможно, то подтверждение эффективности защиты может быть достигнуто посредством эксплуатационных испытаний.

Примечание 2 — Подтверждение эффективности защиты PAT окончательно определяется группой экспертов и по способу определения отличается от метода, обычно используемого для полевых устройств и программируемых логических контроллеров (ПЛК).

3.1.7 **калибровка** (calibration): Задача проверки, целью которой является подтверждение целевого состояния.

Примечание 1 — «Калибровка» означает определение и документальное оформление отклонения значения измерения прибора от корректного измеряемого значения.

Примечание 2 — При калибровке анализатора процесса соотношение между входом и выходом определяется при заданных условиях и документально оформляется. Входное значение — это измеряемая физическая величина. Выходное значение — это электрический выходной сигнал измерительного прибора.

3.1.8 **регулировка** (adjustment): Настройка или модификация прибора с целью устранения систематических ошибок, насколько это необходимо для предполагаемого применения.

Примечание — Регулировка — это процесс, с помощью которого измерительный прибор настраивается или регулируется таким образом, чтобы ошибки измерения были минимальными относительно номинального значения и находились в пределах спецификаций на этот прибор. Данная регулировка — это процесс, который изменяет прибор постоянно.

3.1.9 **интервал испытания** (test interval): Контрольная проверка с различными интервалами для выполнения разных задач испытаний системы PAT как части системы безопасности.

Примечание — Примерами являются следующие:

- интервал испытания для внутреннего диагностического датчика системы PAT (например, расходомера);
- интервал испытания для внутреннего канала системы PAT (например, автоматической калибровки);
- интервал испытания для внутреннего канала системы PAT (например, осмотра и обслуживания, включая ручную настройку);
- интервал испытания для всей системы (ручное тестирование, PAT + остальные приборные системы безопасности).

3.1.10 **контрольная проверка** (proof test): Тест для обнаружения ошибок в технической системе безопасности, чтобы система при необходимости могла быть возвращена в состояние, в котором она выполняет свою предполагаемую функцию.

3.1.11 **охват контрольными проверками** (proof test coverage): Охват тестами для обнаружения ошибок в технической системе безопасности.

Примечание — Первоначально этот термин относился к контрольным проверкам. Однако любой тест (см. интервал испытаний) может достичь охвата ≤1. Для датчиков это означает, что интенсивность DU отказов канала увеличивается из-за его неработоспоспособности, в то время как интенсивность DD отказов уменьшается. Автоматическая калибровка обычно может только проверить некоторую интенсивность DU отказов за достаточно короткие промежутки времени. Также нельзя исключать, что отказы каналов останутся необнаруженными во время проверки и обслуживания. Тщательное планирование процессов тестирования должно гарантировать, что вероятность этого будет низкой.

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

DC — охват диагностикой (diagnostic coverage);
DD — опасный обнаруженный (dangerous detected);
DU — опасный необнаруженный (dangerous undetected);
FAT — заводские приемо-сдаточные испытания (factory acceptance test);
FMEA — анализ видов и последствий отказов (failure mode and effects analysis);
FMEDA — анализ видов, последствий и диагностики отказов (failure mode, effects and diagnostic analysis);
HazOp — исследование опасности и работоспособности (hazard and operability study);
HFT — отказоустойчивость аппаратных средств (hardware fault tolerance);
PAT — анализатор технологического процесса (process analyser technology);

PFD — вероятность опасного отказа по запросу (probability of failure on demand);
PID — монтажно-технологическая схема (piping and instrumentation diagram);
SAT — приемочные испытания на объекте (site acceptance test);
SIF — приборная функция безопасности (safety instrumented function);
SIL — уровень полноты безопасности (safety integrity level);
SIS — приборная система безопасности (safety instrumented system);
SFF — доля безопасных отказов (safe failure fraction);
PTC — охват контрольными проверками (proof test coverage);
λ_i — интенсивность отказов *i*-го компонента (failure rate of *i* component);
μ_i — интенсивность восстановления *i*-го компонента (repair rate of *i* component);
$U_{DD,\,i}$ — неготовность *i*-го компонента из-за его DD отказа (unavailability through DD failure of *i* component);
$U_{DU,\,i}$ — неготовность *i*-го компонента из-за его DU отказа (unavailability through DU failure of *i* component);
U_{ch1} — неготовность 1-го канала (unavailability of channel 1);
U_{MooN} — неготовность всей системы с конфигурацией MooN (unavailability of entire system in the MooN configuration);
β — доля отказов по общей причине (proportion of common cause failures);
T_{max} — максимальный интервал испытаний (maximum test interval);
PFD_{beta} — часть *PFD*, составляющая отказы по общей причине (proportion of *PFD* value due to common cause);
PFD_{MooN} — значение *PFD* всей системы без учета отказов по общей причине (*PFD* value of entire system without taking common cause into consideration);
PFD_{PAT} — значение *PFD* всей системы PAT (*PFD* value of the entire PAT system).

4 Процесс квалификации

4.1 Обзор

Измерительные устройства PAT, как правило, представляют собой сложные датчики SIS, индивидуально адаптированные под конкретные требования процесса технологического проектирования и описывающие состояние процесса посредством измерения концентрации одной или нескольких субстанций.

Особенности этих датчиков часто не позволяют в достаточной мере использовать опыт эксплуатации существующих SIS для нового измерительного оборудования PAT, которое планируется использовать. В этих случаях следует проводить эксплуатационное испытание готового функционального измерительного оборудования. Однако эти измерительные устройства требуют высокую степень технической компетентности от специалистов, участвующих на всех уровнях описанного на рисунке 1 процесса квалификации. Такими специалистами являются разработчики и операторы систем PAT (см. 4.2 и 4.3). Каждый этап квалификации должен быть документально оформлен.

Процесс квалификации должны выполнять эксперты PAT при участии инженеров по безопасности для управления процессом и инженеров по разработке технологического процесса. Все соответствующие данные о технологическом процессе, обеспечивающие эффективность системы PAT, должны быть подтверждены заслуживающим доверие инженером по безопасности.

Если технически реализуемы несколько методов измерения, то они должны быть изучены и оценены. С самого начала планирования квалификации следует учитывать дополнительные возможности по снижению/минимизации общей вероятности отказов системы PAT, включая:

- уровень резервирования/отказоустойчивости;
- однородность или разнообразие при резервировании;
- опыт эксплуатации/подтвержденную эффективность защиты в другом измерительном оборудовании;
- риск, связанный с метрологическим применением (например, поперечная чувствительность, процессы старения, отказ по общей причине).

Метрологическое соответствие может быть установлено на основе опыта предыдущих применений или доказано в процессе прикладного тестирования.

При использовании резервированных систем следует учитывать мониторинг отклонения (дельта) измеряемых величин.

Выбор метода измерения сопровождается проектированием системы предварительной обработки сигнала и определением компонентов для нее. Как проектирование, так и выбор компонентов должны быть обоснованы, если это имеет отношение к функциональности, а также документально оформлены. Для построения измерительной системы PAT следует использовать соответствующее и надежное оборудование и компоненты. Верификация надежности обычно основана на производственном опыте оператора, но также может быть реализована посредством оценки надежности, выполняемой производителем.

Предположения разработчика (специалиста по установке) и/или оператора на производстве, относящиеся к применению (например, частота отказов, интервалы контрольных испытаний и т. д.), всегда имеют приоритет над спецификациями производителя. Разработчик и/или оператор несут ответственность за классификацию SIL, соответствующую применению, независимо от любых возможных рекомендаций производителя. Хотя предпочтение следует отдавать использованию анализаторов с сертификатом SIL, это не означает, что обязательно использовать анализатор, сертифицированный производителем по SIL. Следовательно, анализатор без сертификата SIL может использоваться вместо анализатора с сертификатом SIL.

Также нет необходимости реализовывать конкретное приложение исключительно с анализатором, одобренным для этой цели конкретным производителем. Например, нет причин, по которым анализатор, сертифицированный производителем по SIL1 и с подтвержденной эффективностью защиты, не должен использоваться в 1-канальном приложении с SIL2, если выполнен процесс квалификации.

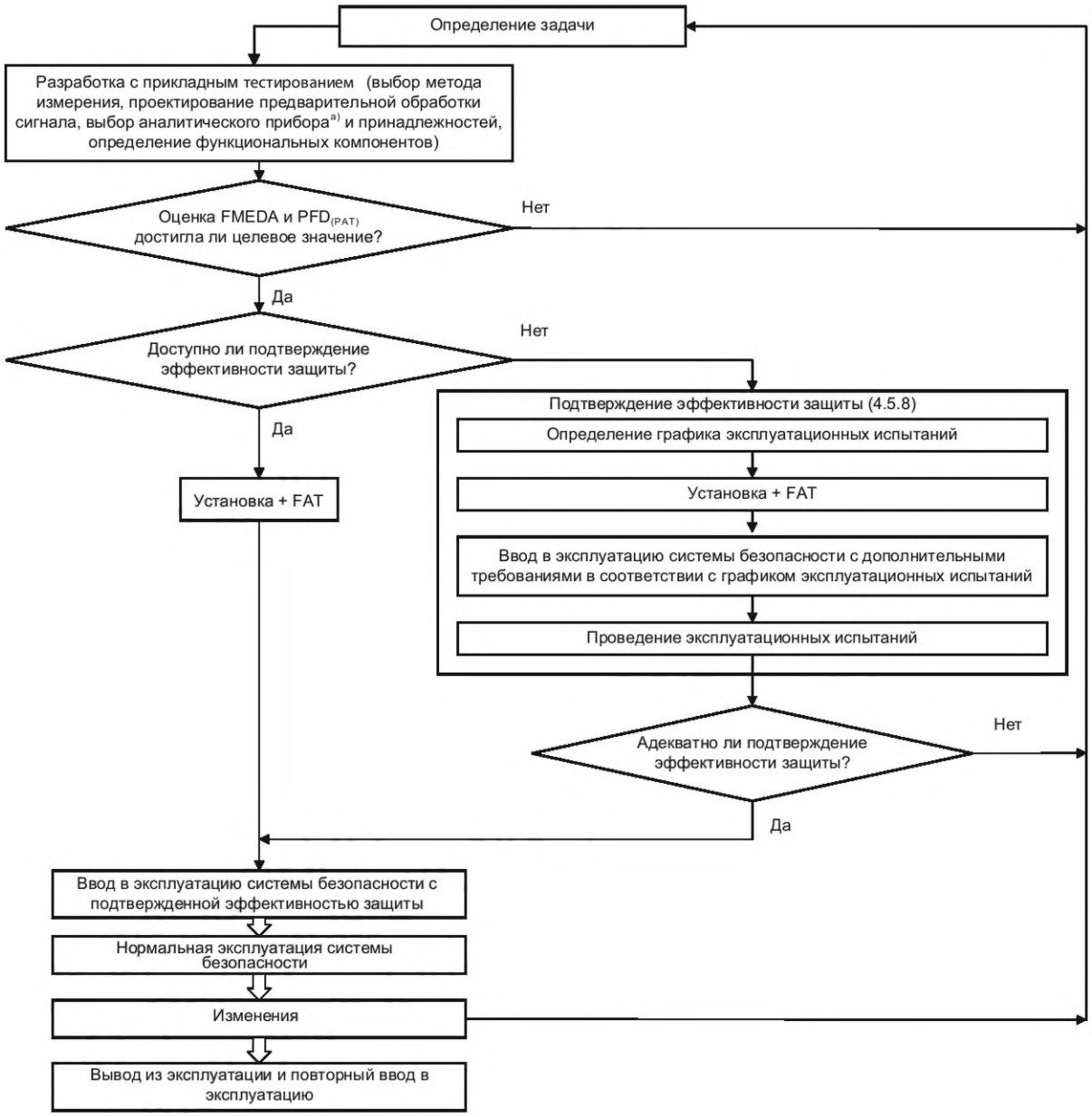
Для измерительного оборудования PAT следует выполнить детальное обследование всей системы PAT. Целью такого обследования является обнаружение возможных отказов с оценкой их с точки зрения влияния на функциональную безопасность. В результате можно вывести соответствующие меры по управлению отказами, предотвращению отказов, обнаружению отказов или снижению интенсивности отказов. Следует оценить значение PFD. Варианты оценки указаны в 4.5.6. Значение PFD_{PAT} учитывается в общем значении PFD для SIS.

Если имеются: подтверждение эффективности защиты, адекватное значение HFT (см. 4.5.5) и значение PFD (см. 4.5.7), то соответствие системы PAT для SIS следует оценить окончательно.

Из-за сложности оборудования анализатора процесса значения SFF недостаточно. По этой причине SFF не оценивается и не указывается для систем анализаторов технологического процесса.

Если для установления подтверждения эффективности защиты все еще нет адекватных данных, а методы измерения уже успешно используются в аналогичных средах, то соответствие системы PAT может быть частью средства обеспечения безопасности SIS и может быть определено во время активной эксплуатации на основе документально оформленного процесса эксплуатационных испытаний (см. 4.5.8).

В результате эксплуатационных испытаний оператор может столкнуться с требованиями, которые необходимо выполнить для поддержания функциональной безопасности. Наконец, жизненный цикл измерительного оборудования PAT должен быть документально оформлен от ввода в эксплуатацию до вывода из эксплуатации.



[a)] Рассматриваются аналитические приборы, прошедшие базовое тестирование.

Рисунок 1 — Уровни процесса квалификации для измерительной системы PAT

4.2 Рекомендации к требованиям для разработчика

Следующие требования получены из МЭК 61511-1:2016, 5.2 и конкретизированы для решения проблем анализаторов технологического процесса. Верификация квалификации установки PAT как части SIS требует всесторонних знаний и опыта в области анализаторов технологического процесса и их использования в химических и/или физических процессах. Эти знания и опыт могут быть собраны в экспертной группе, которая реализует верификацию квалификации. Лица, отделы или организации, участвующие в реализации различных мер обеспечения безопасности в жизненном цикле системы безопасности, должны быть компетентны для выполнения задач, за которые они несут ответственность. Лица, отвечающие за процесс квалификации, должны обладать адекватными управленческими и лидерскими качествами для соответствующей задачи и понимать последствия любого события, которое может произойти. Новые и сложные приложения или технологии должны использоваться только в том случае, если группа способна их понять и оценить их влияние на безопасность.

Экспертная группа должна обладать следующими знаниями и опытом:

- знание соответствующих химических или физических процессов в точке измерения.

Для определения соответствия анализатора химическому или физическому процессу (т. е. для оценки соответствия анализатора приложению) должны быть известны физические и/или химические параметры в точке измерения. Эти данные должны учитываться для всего диапазона нормальной эксплуатации (диапазон приемлемых значений и допустимый диапазон отказов) вплоть до границы некорректной эксплуатации. Запуск и останов должны учитываться так же, как и при обычной эксплуатации, если это явно не исключено из функции безопасности;

- опыт в подготовке применений анализатора.

Для подготовки применения в анализаторе метода измерения для использования в SIS необходимо понимание выбираемого метода и его ограничений с физической и химической точек зрения;

- опыт в проектировании процессов предварительной обработки сигнала.

Знания компонентов системы в процессе предварительной обработки сигнала, разработка процессов предварительной подготовки сигнала, физические и химические свойства измеряемой субстанции и процесс измерения необходимы для оценки соответствия процесса предварительной обработки сигнала;

- опыт работы с методами обеспечения безопасности.

Необходимы компетентность в проведении FMEDA, оценки значения PFD системы PAT и компетентность в последующем выполнении анализа рисков (например, метод HazOp для прогнозирования, определения причины, оценка последствий и контрмер);

- знание применяемых норм и стандартов.

Соответствующие нормы и стандарты при проектировании на момент разработки настоящего документа представлены в МЭК 61508 и МЭК 61511.

4.3 Рекомендации к требованиям для оператора на предприятии

Следующие требования вытекают из МЭК 61511-1:2016, 6.2 и конкретизированы для решения проблем анализаторов технологического процесса. Оператор установки PAT как части SIS должен гарантировать на протяжении всего жизненного цикла, что требуемый уровень полноты безопасности рассматриваемой функции безопасности поддерживается в процессе эксплуатации и технического обслуживания. Если SIS должна эксплуатироваться и обслуживаться таким образом, чтобы поддерживать требуемую функциональную безопасность, то следует обеспечить компетентность, необходимую для обслуживания такой системы на всех уровнях технического обслуживания, или поручить такое обслуживание поставщику таких услуг с соответствующей компетентностью. Организационная форма не имеет значения.

В дополнение к требованиям, описанным в МЭК 61511, эта компетентность охватывает следующие необходимые знания, навыки и опыт:

- знание функциональности системы PAT.

Знание о функционировании системы PAT, в частности предварительной обработки сигнала. Понимание принципов, лежащих в основе метода измерения. Знания функциональных ограничений измерительной системы, обычно получаемые из условий окружающей среды и взаимодействия со средой измерения;

- навыки и опыт в техническом обслуживании оборудования PAT.

Навыки механических и электрических работ с измерительной системой PAT. Они включают в себя как обслуживание, так и работы по технической поддержке. Опыт в выявлении отказов (т. е. случайных отказов измерительной системы).

4.4 Базовое испытание (только анализатор)

Каждый анализатор, используемый в системе безопасности, должен соответствовать основным требованиям к качеству. Базовое испытание может способствовать проверке этих требований к качеству (см. приложение А). Базовое испытание не заменяет прикладное тестирование анализатора, которое кроме того будет проводиться в отношении рассматриваемой системы предварительной обработки сигнала или подтверждения эффективности защиты.

Поскольку результаты базового испытания определяются состоянием аппаратного и программного обеспечения анализатора, то следует гарантировать, что производитель заранее и своевременно сообщает конечному пользователю об изменениях в аппаратном или программном обеспечении.

После этого оператор установки должен принять решение об обновлении базового испытания в каждом конкретном случае. Базовое испытание, как правило, не требует обновления, если производитель разработал анализатор в соответствии с требованиями к качеству, представленными в МЭК 61508.

4.5 Разработка

4.5.1 Общие положения

Разработку измерительной установки PAT как части SIS необходимо осуществлять с особой тщательностью, поскольку это существенно влияет на готовность SIS к дальнейшей эксплуатации.

По сути, проектирование системы PAT должно основываться на рабочих листах спецификаций, которые включают данные о процессе со всеми его физическими и химическими свойствами (давление, температура, состав, фаза, точка росы и т. д.).

Системы PAT, как правило, более сложны по своей структуре, чем другие измерительные системы (например, для измерения давления, температуры или расхода). Они относятся в частности к так называемым системам измерения в режиме реального времени, которые удаляют измеряемую часть смеси субстанций в процессе производства и очищают измерительную систему для последующего анализа. Это может повлиять на состав измеряемой смеси субстанций с помощью таких компонентов системы как клапаны, насосы, охладители, сепараторы и фильтры. Также может возникнуть ситуация, когда образец больше не может быть передан в анализатор или передается недостаточно быстро, а измеряемое значение больше не соответствует требованиям к своевременности данных. Таким образом, предварительная обработка сигнала является неотъемлемой частью системы безопасности SIS и следовательно должна учитываться при определении PFD.

Предварительная обработка сигнала может при определенных обстоятельствах существенно влиять на значение PFD сенсорных установок в системе PAT. По этой причине системы PAT по возможности оснащают дополнительными датчиками, которые могут определять ошибки предварительной обработки сигнала достаточно быстро. Доля имеющихся опасных необнаруженных сбоев может быть снижена в результате их преобразования в обнаруженные сбои.

Помимо контрольных проверок для обычных систем безопасности системы PAT подвергаются дополнительному ручному тестированию и калибровке с более короткими интервалами, включая настройку, когда это необходимо. Ручные или автоматические калибровки без настройки между вышеупомянутыми ручными испытаниями могут способствовать повышению достоверности тестирования системы PAT.

Поскольку корректное функционирование дополнительных датчиков имеет решающее значение для определения доли опасных необнаруженных и обнаруженных сбоев, они выполняют мониторинг с отдельными интервалами тестирования, где это необходимо.

4.5.2 Данные для разработки

Принципы, лежащие в основе разработки измерительной установки PAT как части SIS:

- определение SIF.

Уровень эффективности защиты системы функциональной безопасности (например, SIL). Он реализуется в процессе соответствующей оценки безопасности/анализе риска производственной линии и документально оформляется. Целью в этом случае является ограничение конкретного параметра состояния процесса. В PAT это, как правило, ограничение концентрации определенной субстанции сверху или снизу;

- максимально допустимое время отклика системы безопасности.

Его следует учитывать при разработке PAT, и оно зависит от времени «задержки» образца (т. е. периода сбора, транспортировки и анализа образца), продолжительности реакции исполнительных механизмов и логических компонентов;

- данные о технологическом процессе в точке отбора образца.

Эти данные включают в себя: состав анализируемого образца и физические/технические данные потока материала в точке отбора образца, включая токсичность и коррозионную активность. Следует также учитывать влияние особых условий системы (например, запуск, останов, изменение нагрузки, неисправность).

4.5.3 Анализатор и учет его применения

Выбор принципа измерения и анализатора может быть основан на данных для его разработки. При выборе анализаторов предпочтение следует отдавать тем, для которых их базовое соответствие определено в приложении А.

Конкретное метрологическое соответствие может быть установлено на основе опыта с сопоставимыми существующими применениями. Однако оно обычно верифицируется во время применения анализатора.

Причины выбора метода и анализатора должны быть документально оформлены.

4.5.4 Предварительная обработка сигнала

Требуемая в каждом конкретном случае предварительная обработка сигнала определяется данными для разработки и выбранным анализатором.

Предпочтительно предварительная обработка сигнала должна включать диагностические функции, чтобы отказы, влияющие на функцию безопасности, можно было идентифицировать и передать сигнал о них (предотвратить отказы DU и преобразовать отказы DU в отказы DD).

Периферия должна, где это возможно, охватывать компоненты с доказанной технической надежностью.

Полная система (измерительная установка PAT), состоящая из предварительной обработки сигнала и анализатора, должна быть проиллюстрирована на схеме P&I (технологическая схема анализатора) со списком комплектующих.

4.5.5 HFT

HFT предоставляет информацию об уровне резервирования системы. Согласно МЭК 61511-1, пункт 11.4, применяются следующие значения отказоустойчивости оборудования, указанные в таблице 1.

Таблица 1 — Минимальные требования к HFT согласно SIL

SIL	Минимальная отказоустойчивость оборудования SIL во время эксплуатационных испытаний	Минимальная отказоустойчивость оборудования в случае адекватно подтвержденной эффективности защиты
1	0	0
2	1	0
3	2	1

Для систем PAT в SIS всегда необходимо подтверждение эффективности защиты (см. раздел 4). Это соответствует выбору на основе более раннего применения МЭК 61511-1:2016, 11.5.

Минимальная отказоустойчивость аппаратных средств в случае адекватно подтвержденной эффективности защиты может применяться только в том случае, если в системе PAT можно настроить только параметры, связанные с процессом, и эта настройка защищена. Редактирование программного обеспечения системы PAT или анализатора во время подтверждения эффективности защиты должно быть обосновано, документально оформлено и завершено перезапуском контрольной проверки.

4.5.6 Анализ видов, последствий и диагностики отказов системы PAT (FMEDA)

Анализ вероятности и последствий отказов должен быть проведен для всей системы PAT, включая среду поставки, среду сравнения и вспомогательные среды (например, FMEDA — анализ видов, последствий и диагностики отказов). Отказы, выявленные в результате анализа, должны быть описаны и соответствующим образом классифицированы (например, DD — опасный обнаруженный, DU — опасный необнаруженный, S — безопасный), а также перечислены интенсивности отказов (включая отказы по общей причине, общего вида), включая источник их происхождения (например, спецификация производителя, собственная статистика). Возможные отказы идентифицирует экспертная группа и определяет их интенсивности. Выявленные отказы должны быть далее классифицированы как случайные и систематические. Систематические отказы должны быть устранены, где это возможно. Если это невозможно, то систематические отказы должны быть идентифицированы диагностическими средствами. Должны быть предприняты усилия для достижения уровня охвата контрольными проверками, равного 100 %, при регулярной проверке системы PAT (контрольными проверками). Если уровень охвата контрольными проверками оценивается ниже, то такое консервативно оцененное значение должно быть обосновано и документально оформлено. Статистическая обработка отдельных интенсивностей отказов не представляется возможной из-за неточности оценки. Все соответствующие реальные условия эксплуатации должны быть учтены.

Область применения FMEDA зависит от сложности системы PAT. Пример документации узких мест такого анализа проиллюстрирован в приложении В.

С другой стороны, ошибка человека (например, использование неподходящих вспомогательных сред) не принимается во внимание. Этот отказ должен быть исключен с помощью организационных

мер. Аналогичным образом отказы, возникающие, например, из-за систематической неточности концентрации испытательных газов, в FMEDA не учитываются, но должны рассматриваться другим подходящим способом, например путем настройки положения точки переключения.

4.5.7 Оценка значения PFD_{PAT}

Значение PFD_{PAT} используется для оценки вероятности отказа по запросу измерительной системы PAT. Значение PFD_{PAT} представляет собой только часть PFD системы безопасности. В любом случае при общей оценке следует учитывать дополнительные показатели PFD (например, связанные с логикой или исполнительным механизмом). В некоторых случаях значение PFD_{PAT} можно минимизировать с помощью дополнительных сигналов состояния (преобразование отказов DU в отказы DD) и/или сокращения интервалов технического обслуживания. Если это невозможно, то следует заменить измерительную систему при необходимости или увеличить количество каналов. И если окончательное значение PFD_{PAT} превышает норму, то рассматриваемую измерительную установку исключают из состава SIS.

Значение PFD_{PAT} следует определять с помощью соответствующего процесса. Одним из методов является численный дискретный метод, представленный далее в качестве примера.

Численный дискретный метод определения значения PFD с использованием анализа электронных таблиц реализуется на основе неготовности подкомпонентов системы в зависимости от времени *t*. Случаи неготовности, связанные с компонентами, могут быть соответствующим образом совмещены для формирования общей неготовности системы. Значение PFD определяется путем усреднения этой неготовности $U(t)$ за весь срок службы системы или за самый длинный период роста кривой $U(t)$.

Возможные неисправности сначала регистрируют с помощью анализа видов, последствий и диагностики отказов (FMEDA) и классифицируют как безопасные, опасные обнаруженные и опасные необнаруженные. Эти неисправности составляют основу для случаев неготовности.

Формулы для неготовности $U(t)$ компонентов являются универсально общезначимыми и составляют основу для формул, используемых для расчета значения PFD, содержащихся в МЭК 61508-6.

Метод описан в приложении С.

4.5.8 Подтверждение эффективности защиты, которое всегда выполняется после предварительного эксплуатационного испытания системы PAT

Подтверждение эффективности защиты достигается за счет достаточного опыта эксплуатации, включая подтверждение пригодности измерительной задаче. Если это неосуществимо, то подтверждение эффективности защиты может быть достигнуто путем эксплуатационного испытания.

После выполнения схемы технологического процесса, подготовки набора изготовленных деталей и оценки значения PFD_{PAT} как приемлемого следует принять решение о наличии достаточного опыта эксплуатации с сопоставимой измерительной системой PAT. Вышеупомянутая группа экспертов должна определить, является ли эксплуатационный опыт достаточным, или при необходимости запросить эксплуатационные испытания измерительной системы PAT. Они реализуются в предназначенном для измерения месте для всех режимов эксплуатации. Эксплуатационные испытания необходимо проводить в следующих условиях:

- предполагается, что эксплуатационное испытание может быть выполнено с положительным результатом;
- оцененное значение PFD_{PAT} достаточно низкое (т. е. остается значительный резерв неиспользованной вероятности отказов для применяемых логических и исполнительных систем). Подтверждение эффективности защиты посредством эксплуатационных испытаний не выполняется, если предполагается, что максимально возможное значение PFD уже практически достигнуто в процессе планирования;
- компоненты рассматриваемого анализатора технологических процессов уже должны успешно применяться в сопоставимой позиции;
- функция безопасности должна всегда дополняться необходимыми мерами на этапе эксплуатационных испытаний;
- процесс эксплуатационных испытаний и критерии оценки для последующего подтверждения эффективности защиты должны быть документально оформлены до начала установки системы;
- если выполнить подтверждение эффективности защиты невозможно, то соответствующее выполнение функции безопасности должно быть гарантировано другим способом, а также с помощью методов, отличных от методов, необходимых для анализа технологических процессов. Это означает, что PAT является неподходящим в этом случае.

С помощью эксплуатационных испытаний (4.5.8) для реализации функции безопасности может быть установлен новый анализатор или новая предварительная обработка сигнала.

4.5.9 Логика безопасности в системе PAT

Системы PAT как часть SIS, рассматриваемые в настоящем стандарте, могут иметь свои собственные логические блоки, которые, например, облегчают переключение точек измерения или связывают сигналы заранее.

Логический компонент может быть реализован в главной системе управления или в связанном с безопасностью ПЛК, или логическом решателе вышестоящего уровня, или в отдельном контроллере PAT (ПЛК; ПЛК, связанный с безопасностью, или логический решатель), или может быть полностью включен в анализатор. Возможны также смешанные формы.

Если информация, связанная с безопасностью, обрабатывается отдельно, важно действовать в соответствии со стандартами и рекомендациями функциональной безопасности (например, использовать ПЛК, связанный с безопасностью).

4.5.10 Переключение точек измерения

С переключением точки измерения связаны дополнительные риски, и это всегда следует рассматривать как источник ошибок. Возможные DU отказы из-за неисправных клапанов можно, как правило, свести к DD отказам с помощью датчиков положения. Также следует учитывать вызванное переключением увеличение предельного значения времени срабатывания системы безопасности.

4.5.11 Составление плана периодических проверок во время эксплуатации

Частота периодических испытаний всей измерительной системы должна определяться в контексте оценки значения PFD. В идеале эти периодические испытания должны выявлять все возможные возникающие DU отказы, также неработающую регистрирующую аппаратуру, ограничительные датчики уровня, расхода, давления или температуры.

Необходимо оценить уровень охвата периодическими испытаниями для обнаружения описанных отказов. Этот охват контрольными проверками следует учитывать при оценке значения PFD.

Определенные интервалы испытаний оказывают значительное влияние на значение PFD.

4.6 Ввод в эксплуатацию системы безопасности

Ввод в эксплуатацию осуществляется после установки и SAT в случае документально подтвержденной эффективности защиты. При отсутствии подтвержденной эффективности защиты ввод в эксплуатацию может осуществляться совместно с эксплуатационным испытанием. Персонал по эксплуатации и техническому обслуживанию должен быть обучен.

4.7 Документирование процесса квалификации

Документирование процесса квалификации должно охватывать следующее:

- выдержки из оценки безопасности эксплуатации/HazOp;
- данные технологического процесса для рабочего журнала выполнения анализа;
- анализатор, лист спецификации;
- технологическую схему (PAT P&I, PAT P&ID) со списком комплектующих;
- документацию на анализаторы/детали (например, сертификаты SIL);
- оценку PFD, включая протокол FMEDA;
- принципиальную схему контура SIS;
- функциональную схему;
- вопросы безопасности, связанные с функцией измерения;
- спецификацию тестирования;
- информацию для оператора по функциональной безопасности;
- график технического обслуживания;
- лицо, ответственное за верификацию знаков сертификации;
- имена участников экспертной группы;
- программу каждого эксплуатационного испытания и записи его результатов.

5 Регулярная эксплуатация

5.1 Общие положения

Все задачи, упомянутые в настоящем разделе, должны инициироваться оператором системы безопасности.

5.2 Периодические испытания во время эксплуатации

Значение PFD, определенное в 4.5.7, непосредственно зависит от определенных интервалов испытания. Поэтому интервалы испытания должны соблюдаться и документироваться в графике технического обслуживания.

Проверка должна быть записана в отчете об испытаниях. Рекомендуется подробный план процедур для проведения проверки. Он может зависеть от различных стадий эксплуатации и видов деятельности (например, во время тестирования стадии запуска).

Проверка всей системы: датчики — логические системы — исполнительные механизмы — должна быть согласована и проведена, где это уместно, с другими выполняемыми задачами. Также применяют МЭК 61511-1:2016, 5.2.1—5.2.3.

Функция системы безопасности должна регулярно верифицироваться на основе выполняемых задач. В нее должна быть включена система PAT.

5.3 Документы и записи в процессе эксплуатации

5.3.1 Общие положения

Рекомендуется, чтобы оператор производства вел записи на основе определенных графиков и правил, которые указывают, что периодические испытания (см. 5.2) проводятся в порядке, установленном на стадии планирования. МЭК 61511 содержит структуру такой документации.

Эти записи должны содержать, как минимум, следующую информацию.

5.3.2 График технического обслуживания

График технического обслуживания и осмотра (график M+I) описывает, какие работы должны быть выполнены с каким интервалом. График M+I содержит, как минимум, следующую информацию:

- номер точки измерения, номер функции безопасности;
- интервал испытаний;
- условие применяемой спецификации испытаний.

Определенные продолжительности MTTR не должны превышаться, поскольку значение PFD, определенное в 4.5.7, непосредственно от них зависит.

5.3.3 Рабочие инструкции

Проведение проверок в соответствии со спецификацией испытаний (см. 4.7) должно быть определено в рабочих инструкциях.

5.3.4 Отчет о выполненных работах

Для отчета об испытаниях, упомянутого в 5.2, рекомендуется следующее минимальное содержание:

- дата выполненных работ по проверке и техническому обслуживанию;
- имена лиц, проводивших проверку и техническое обслуживание;
- описание устраненных неисправностей (тип);
- указание задействованных каналов в случае многоканальных систем безопасности;
- строгая маркировка протестированной системы (например, номер точки измерения, номер функции безопасности);
- отклонение от интервала испытания;
- указание применяемой спецификации испытания;
- результаты работы и верификацию того, что система после обслуживания была повторно введена в эксплуатацию без каких-либо неисправностей.

5.3.5 Регистрация данных о неисправностях

Каждая операция по техническому обслуживанию должна быть надлежащим образом документально оформлена. Вся система, включая предварительную обработку сигналов, должна быть зарегистрирована. Требования, представленные в 5.3.4, применяют к документации должным образом.

Каждая неисправность устройства будет классифицирована следующим образом:

- место неисправности (анализатор процесса, предварительная обработка сигналов);
- обнаружение неисправности (например, контрольной проверкой);
- вид неисправности (опасная, безопасная);
- тип неисправности (случайная, систематическая);
- причина неисправности (например, связанная с процессом, ошибка конструкции, неисправность устройства, неправильная калибровка);
- детали неисправности (например, тип устройства и производитель).

5.4 Оценка данных о неисправностях и обработка отклонений

В контексте процесса непрерывного совершенствования данные о неисправностях должны оцениваться оператором производственного предприятия и экспертами PAT, а отклонения от нормальной эксплуатации должны быть сведены к минимуму.

5.5 Изменения

5.5.1 Изменения в системе PAT

При изменении в системе безопасности существует риск того, что непреднамеренно или ошибочно могут быть реализованы систематические отказы, что ухудшит желаемое поведение этой системы безопасности в случае запроса. Значение PFD в этом случае изменяется, что означает, что критерии требуемого значения SIL могут больше не соблюдаться. Во время оценки изменения следует использовать ту же систему PAT, которая была запланирована и установлена в существующей системе безопасности. Персонал, ответственный за эксплуатацию и техническое обслуживание, должен быть проинформирован об изменении и при необходимости подготовлен к выполняемому изменению.

Если компоненты не могут быть заменены полностью идентичными запасными частями, то это считается изменением и оно будет проверено. Это относится к техническим средствам и программному обеспечению. Изменения программного обеспечения и аппаратных средств, предпринятые производителями в отношении компонентов системы безопасности, должны быть сообщены производителем.

Повторное тестирование программного обеспечения может быть отменено в случае, если программное обеспечение было разработано в соответствии с МЭК 61508.

5.5.2 Изменения процесса технологического проектирования

В случае изменений параметров технологического проектирования (химических и физических) или используемых материалов следует оценить и документально оформить влияние этих изменений на обеспечение безопасности. Следует использовать ту же систему PAT, которая была запланирована и установлена в существующей системе безопасности. Таким образом, оригинальная документация находится у оператора.

5.6 Вывод из эксплуатации и повторный ввод в эксплуатацию

5.6.1 Вывод из эксплуатации

Вывод из эксплуатации характеризуется отключением общего и вспомогательного питания. Отключение процесса само по себе не является выводом из эксплуатации системы PAT.

5.6.2 Повторный ввод в эксплуатацию

Повторный ввод в эксплуатацию соответствует первоначальному вводу в эксплуатацию. Однако стадия эксплуатационного испытания может быть пропущена, если нормальная работа не претерпела изменений (см. 5.5.2).

5.7 Сохранение существующих норм

Обычно применяются используемые правила существующих стандартов, регулирующие защиту. В случае внесения изменений следует учитывать конкретные технические требования к анализаторам процесса.

Приложение А
(справочное)

Базовое испытание анализаторов

Базовое испытание касается исключительно фундаментальных требований к качеству и эксплуатационным характеристикам анализаторов, предназначенных для дальнейшего использования в установках безопасности при условии их технического соответствия. Фактическое соответствие конкретной измерительной задаче обеспечивается посредством прикладного испытания, связанного с задачей.

Содержание базового испытания

1 Проверка организации
1.1 Тип/версия
1.2 Диапазон измерения, датчик
1.3 Серийный номер
1.4 Номер версии аппаратных средств
1.5 Номер версии программного обеспечения
1.6 Документация
1.6.1 Номер версии документации
1.6.2 Доступность для восприятия
1.6.3 Правильность
1.6.4 Полнота
1.6.5 Инструкции по эксплуатации и безопасности на родном языке
2 Технические характеристики анализатора от производителя
2.1 Разработка в соответствии с МЭК 61508 SIL2 или SIL3
2.2 ЭМС гарантирована в соответствии с МЭК 61326-3-1/МЭК 61326-3-2
2.3 Интенсивность DU отказов
2.4 Интенсивность DD отказов
2.5 Интенсивность SU отказов
2.6 Интенсивность SD отказов
2.7 Сертификат испытаний типового проектного решения ЕС для функции измерения
2.8 Допустимая влажность
2.9 Диапазон температур окружающей среды
2.10 Влияние температуры окружающей среды
2.11 Диапазон температур технологического процесса
2.12 Влияние температуры технологического процесса
2.13 Диапазон давлений технологического процесса
2.14 Влияние давления технологического процесса
2.15 Влияние вибраций
3 Оценка технического обслуживания
3.1 Конструкция
3.2 Техника безопасности на производстве
3.3 Эксплуатационные характеристики
3.4 Возможность сброса к настройкам по умолчанию
3.5 Блокировка параметризации
3.6 Сигнал отказа
3.7 Сигнал запроса на обслуживание
3.8 Сигнал на обслуживание
3.9 Расходы на техническое обслуживание
3.10 Удобство обслуживания
3.11 Экспериментальные данные об устройствах производителя, подлежащих данной оценке
4 Оценка взрывозащиты
4.1 Возможность взаимосвязи с другими взрывозащищенными устройствами
4.2 Требования в сертификатах проверки/руководствах по эксплуатации
4.3 Маркировка устройства
4.4 Сертификат испытаний типового проектного решения ЕС и декларация производителя о соответствии требованиям взрывозащиты
5 Оценка совместимости материалов
5.1 Датчик
5.2 Герметизация (кроме датчиков, эластомеров и «окон»)
5.3 Оптические окна
5.4 Уплотнения

6 Проверки

6.1 Испытание ЭМС в соответствии с МЭК 61326-3-1, МЭК 61326-3-2

Оценка неисправностей при срабатывании функции безопасности

6.2 Ошибка линейности — оценка для выбранной субстанции максимального отклонения и максимального гистерезиса

6.3 t_{90} — время отклика на ступенчатое воздействие

6.4 Затухание сигнала при максимальной нагрузке

На рисунке А.1 показан процесс базового испытания анализаторов в системах безопасности SIS.

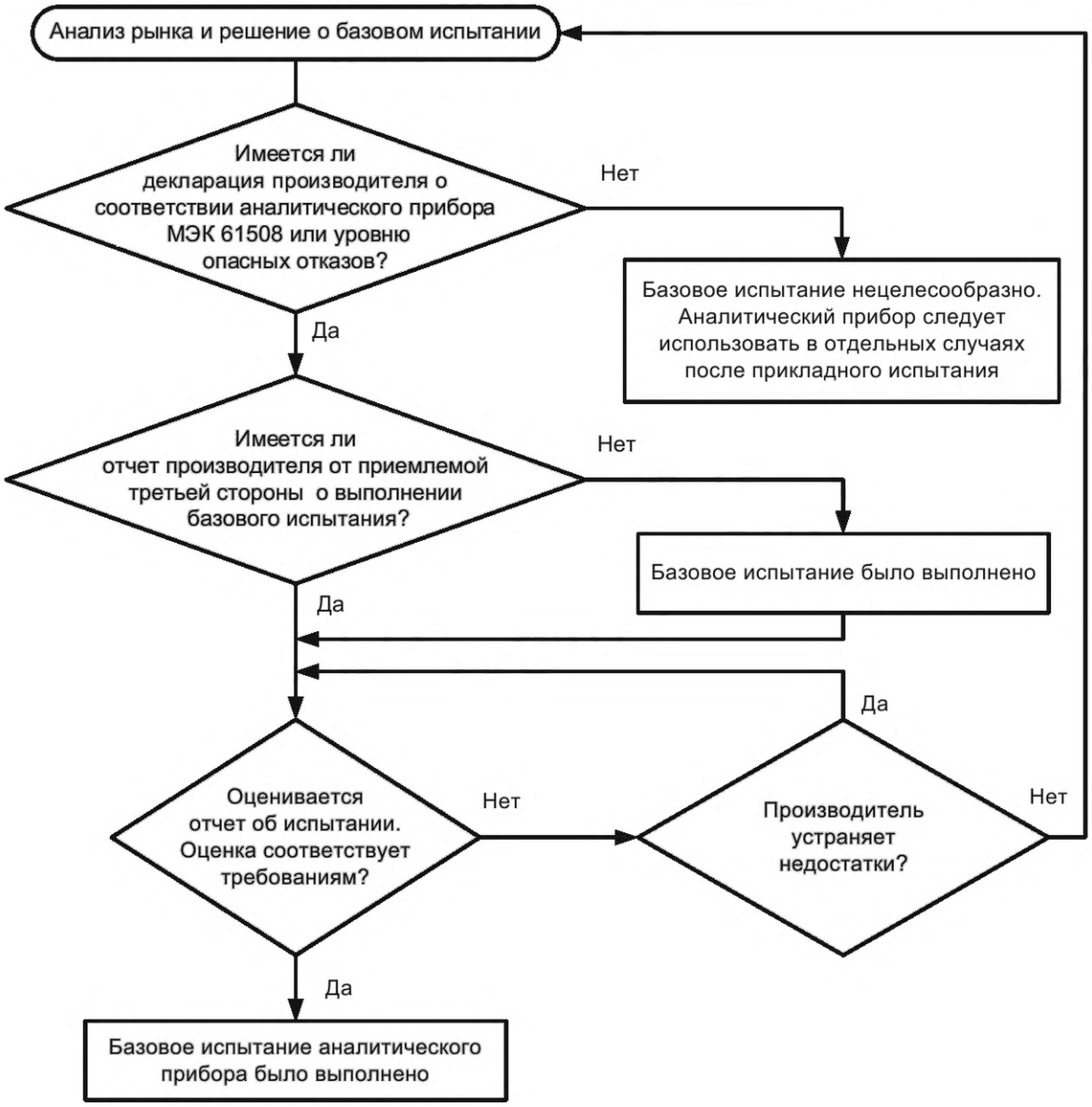


Рисунок А.1 — Процесс базового испытания анализаторов в SIS

Приложение В
(справочное)

FMEDA — документация для оценки безопасности (пример)

Представленная на рисунке В.1 форма может использоваться для систематической записи возможных отказов, сигналов состояния и интервалов технического обслуживания системы РАТ. В зависимости от конструкции системы РАТ для определения ее PFD могут быть необходимы дополнительные параметры.

Канал РАТ	Q 5551
Время ремонта (время восстановления после неисправности) для канала РАТ (ч)	72

Фактор общей причины	0,05

Параметры технического обслуживания	Интервал испытания, ч	Длительность испытаний, ч	Охват диагностикой, %	Дополнительные датчики	Автоматическое обнаружение неисправностей через № 1	№ 2	№ 3	№ 4
Общий интервал контрольной проверки SIS	8760	4	100	Имя	FIA.01 Образец	FIA.02 Бай-пас	TIA.02 Охладитель	Диагностика анализатора
Канал системы РАТ (интервал проверки и профилактического обслуживания, включая ручную регулировку)	168	0,5	90	Интенсивность отказов, $ч^{-1}$	$1{,}2 \cdot 10^{-4}$	$1{,}2 \cdot 10^{-4}$	$5{,}8 \cdot 10^{-5}$	$3{,}8 \cdot 10^{-5}$
Часть канала системы РАТ (интервал автоматической калибровки анализатора)	24	0,05	50	Интервал контрольной проверки датчика, ч	24	24	720	168

№ отказа	Описание и влияние отказа на функциональную безопасность канала РАТ[1)]	Классификация отказов, П, Э	Источник отказов	Интенсивность отказов, $ч^{-1}$	№ 1	№ 2	№ 3	№ 4
1	Неисправность источника света	П	Спецификация производителя	$1{,}2 \cdot 10^{-7}$				X
2	Высокое давление образца	Э	Опыт эксплуатации	$5{,}8 \cdot 10^{-4}$				
3	Неисправность охладителя	Э	Опыт эксплуатации	$1{,}2 \cdot 10^{-4}$			X	
4	Низкий поток образца	Э	Опыт эксплуатации	$2{,}3 \cdot 10^{-6}$		X		
5	Высокий поток образца	Э	Опыт эксплуатации	$2{,}3 \cdot 10^{-7}$	X			
6								
7								
8								

[1)] В настоящем примере влияние на функциональную безопасность канала РАТ не рассматривается.

Рисунок В.1 — FMEDA — документация, используемая для оценки безопасности (пример)

Приложение С
(справочное)

Численное определение PFD с учетом дискретных значений времени для компонентов

Интенсивность отказов для соответствующего компонента должна быть определена для каждого возможного отказа из FMEDA. При этом следует отличать опасный необнаруженный DU отказ от опасного обнаруженного DD отказа. Безопасные отказы не включены в определение значения PFD. С помощью этого метода можно исследовать несколько различных интервалов испытаний. DU отказы должны быть объединены в соответствии с интервалами испытаний (например, все отказы, обнаруженные во время еженедельной проверки). Отказы DD являются систематическими и могут быть объединены вместе.

В общем случае неготовность компонентов i, связанная с опасными обнаруженными отказами, на длительном интервале времени t определяется как [5]

$$U_{DD,i}(t) = \frac{\lambda_i}{\lambda_i + \mu_i}\left(1 - e^{-(\lambda_i + \mu_i)t}\right) \approx \frac{\lambda_i}{\lambda_i + \mu_i}.$$

Неготовность компонентов i, связанная с опасными необнаруженными отказами, равна

$$U_{DU,i}(t) = 1 - e^{-1\lambda_i t} \approx \lambda_i t.$$

При определении неготовности, связанной с компонентами, получаем разные дискретные значения времени.

Усреднение осуществляется последовательно по всему периоду проверки, который должен охватывать максимальный интервал испытаний T_{max}.

Неготовности DU отказов группируются и суммируются в соответствии с интервалами испытаний PTI.

Неготовности DD отказов объединяются все вместе, поскольку они не зависят от интервалов испытаний

$$U_{DD} = \sum_i U_{DD,i}.$$

Определение неготовности всей системы поясняется на примере с использованием электронных таблиц.

Предположения примера: имеются два различных интервала испытаний (PTI1 и PTI2, например, PTI1 = 1 неделя = 168 ч, PTI2 = 1 год = 8 760 ч), в которых могут возникнуть различные DU отказы.

Кроме того, существуют дополнительные DD отказы.

Суммарная частота отказов составляет $\lambda_{DU,\,PTI1} = 10^{-7}$ 1/ч, $\lambda_{DU,\,PTI2} = 10^{-8}$ 1/ч, $\lambda_{DD} = 10^{-7}$ 1/ч, $\mu = 1/5$ 1/ч.

Таблица С.1 — Интенсивность отказов для соответствующего компонента

Время, ч	$U_{DD} = \frac{\lambda_{DD}}{\lambda_{DD} + \mu}$	$U_{DU,\,PTI1}(t) = \lambda_{DU,\,PTI1} t$	$U_{DU,\,PTI2}(t) = \lambda_{DU,\,PTI2} t$	$U_{ch1}(t) = U_{DU,\,PTI1}(t) + U_{DU,\,PTI2}(t) + U_{DD}$
1	$5 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$1 \cdot 10^{-8}$	$6{,}1 \cdot 10^{-7}$
2	$5 \cdot 10^{-7}$	$2 \cdot 10^{-7}$	$2 \cdot 10^{-8}$	$7{,}2 \cdot 10^{-7}$
3	$5 \cdot 10^{-7}$	$3 \cdot 10^{-7}$	$3 \cdot 10^{-8}$	$8{,}3 \cdot 10^{-7}$
…	…			
168	$5 \cdot 10^{-7}$	0	$1{,}68 \cdot 10^{-6}$	1
169	$5 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$1{,}69 \cdot 10^{-6}$	$2{,}29 \cdot 10^{-6}$
170	$5 \cdot 10^{-7}$	$2 \cdot 10^{-7}$	$1{,}70 \cdot 10^{-6}$	$2{,}40 \cdot 10^{-6}$
…	…			
8759	$5 \cdot 10^{-7}$	$2{,}3 \cdot 10^{-6}$	$8{,}759 \cdot 10^{-5}$	$9{,}039 \cdot 10^{-5}$
8760	$5 \cdot 10^{-7}$	$2{,}4 \cdot 10^{-6}$	0	1

Неготовность всей рассматриваемой системы/канала устанавливают вручную для каждого часа во время теста (например, калибровки). Неготовность после теста равна нулю. Таким образом система снова доступна в этом отношении. Это достигается путем замены времени t в формулах для U_{DU} на T, где T представляет собой соответствующий интервал испытаний. Неготовность для U_{DD} является постоянной.

Если все отказы не могут быть обнаружены во время испытаний (РТС < 100 %), то это значение неготовности следует добавлять после испытания, проведенного после проверки неготовности, зависимой от времени.

В случае многоканальной структуры системы определение неготовности всей системы должно быть вычислено для конкретной конфигурации канала.

Для этого используют (согласно [6]):

$$U_{1oo1}(t) = U_{ch1}(t)$$

$$U_{1oo2}(t) = U_{ch1}(t) \cdot U_{ch2}(t)$$

$$U_{1oo3}(t) = U_{ch1}(t) \cdot U_{ch2}(t) \cdot U_{ch3}(t)$$

$$U_{2oo3}(t) = (U_{ch1}(t) \cdot U_{ch2}(t)) + (U_{ch2}(t) \cdot U_{ch3}(t)) + (U_{ch1}(t) \cdot U_{ch3}(t)) - 2\,(U_{ch1}(t) \cdot U_{ch2}(t) \cdot U_{ch3}(t)).$$

Значение PFD для конфигурации MooN будет

$$\mathrm{PFD}_{\mathrm{MooN}} = \frac{1}{T_{\max}} \sum_{T_{\max}} U_{\mathrm{MooN}}(t).$$

Если система состоит из более одного канала, то отказ по общей причине должен быть включен в значение PFD. Однако отказы по общей причине (обозначают как ß) всегда вычисляют для одного канала

$$\mathrm{PFD}_{\mathrm{beta}} = \beta \frac{1}{T_{\max}} \int_{0}^{T_{\max}} U_{1oo1}(t).$$

Тогда значение PFD для всей системы равно

$$\mathrm{PFD}_{\mathrm{PAT}} = \mathrm{PFD}_{\mathrm{MooN}} + \mathrm{PFD}_{\mathrm{beta}}.$$

Эта процедура для определения значения PFD достаточно точна и, как правило, может быть реализована с помощью обычных электронных таблиц.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным и национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 61508-1	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
IEC 61508-2	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
IEC 61508-3	IDT	ГОСТ IEC 61508-3—2018 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
IEC 61508-4	IDT	ГОСТ Р МЭК 61508-4—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
IEC 61508-5	IDT	ГОСТ Р МЭК 61508-5—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности»
IEC 61508-6:2010	IDT	ГОСТ Р МЭК 61508-6—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3»
IEC 61508-7	IDT	ГОСТ Р МЭК 61508-7—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
IEC/TS 61508-3-1	—	*
IEC/TS 61508-3-2	—	*
IEC 61511-1:2016	IDT	ГОСТ Р МЭК 61511-1—2018 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования»
IEC 61511-2	IDT	ГОСТ Р МЭК 61511-2—2018 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 2. Руководство по применению МЭК 61511-1»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 61511-3	IDT	ГОСТ Р МЭК 61511-3—2018 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 3. Руководство по определению требуемых уровней полноты безопасности»
IEC/TR 61511-4	—	*
IEC 61326-3-1:2017	IDT	ГОСТ IEC 61326-3-1—2015 «Электрическое оборудование для измерения, управления и лабораторного применения. Требования ЭМС. Часть 3-1. Требования помехоустойчивости для систем, связанных с безопасностью, и оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональная безопасность). Общие промышленные применения»
IEC 61326-3-2:2017	IDT	ГОСТ IEC 61326-3-2—2015 «Электрическое оборудование для измерения, управления и лабораторного применения. Требования ЭМС. Часть 3-2. Требования помехоустойчивости для систем, связанных с безопасностью, и оборудования, предназначенного для выполнения функций, связанных с безопасностью (функциональная безопасность). Промышленные применения с учетом определенной электромагнитной обстановки»

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] IEC TR 61831:2011 On-line analyser systems — Guide to design and installation

[2] IEC TR 61832:2015 Design and installation of on-line analyser systems — Guide to technical enquiry and bid evaluation

[3] IEC TR 62010:2016 Analyser systems — Maintenance management

[4] IEC 61285:2015 Industrial-process control — Safety of analyser houses

[5] Kumamoto H., Henley E., 1996: Probabilistic Risk Assessment and Management for Engineers and Scientists, IEEE Press

[6] Gabriel T., 2010: Generic Construction of Availability Calculation Models for Safety Loops in Process Industry, Dissertation Technische Universität Kaiserslautern (University of Kaiserslautern)

УДК 62-783:614.8:331.454.004.056.5:006.354 ОКС 13.110, 25.040.40

Ключевые слова: функциональная безопасность, анализатор технологического процесса, уровень эффективности защиты, оценка рисков, мониторинг параметров процесса, требования безопасности, параметры безопасности

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

Сдано в набор 22.10.2025. Подписано в печать 07.11.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,77.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru