ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 366.5— 2019

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 5

Руководство по практическому применению

Издание официальное

Москва
Стандартинформ
2019

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 сентября 2019 г. № 41-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: info@interecoms.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 (www.gost.ru)

Содержание

Введение

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

- Часть 1. Основные положения, принципы и понятия;
- Часть 2. Системы менеджмента;
- Часть 3. Подготовка, запуск и эксплуатация устройств безопасности;
- Часть 4. Верификация полноты аппаратных средств автоматизированной системы безопасности;
- Часть 5. Руководство по практическому применению (настоящий стандарт);
- 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 5

Руководство по практическому применению

Industrial automation systems and integration.
Safety and security arrangements of industrial process plants by means of process control engineering.
Part 5. Recommendations for practical use

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).

Настоящий стандарт устанавливает практические рекомендации по инженерному обеспечению, эксплуатации и функционированию приборных систем безопасности (SIS). В настоящем стандарте акцент делается на рассмотрение:

- подсистемы датчиков;
- подсистемы пусковых устройств (исполнительные элементы), и
- логические системы.

Положения настоящего предварительного национального стандарта применяются совместно с:

- ПНСТ 366.1—2019, ПНСТ 366.2—2019, ПНСТ 366.3—2019.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р МЭК 61511-1—2018 Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования

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

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

ПНСТ 366.2—2019 Системы промышленной автоматизации и интеграция. Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами. Часть 2. Системы менеджмента

ПНСТ 366.3—2019 Системы промышленной автоматизации и интеграция. Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами. Часть 3. Подготовка, запуск и эксплуатация устройств безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесяч-

Издание официальное

ного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Сокращения и обозначения

В настоящем стандарте применены следующие сокращения и обозначения:

DC — охват диагностикой (diagnostic coverage);

HFT — отказоустойчивость аппаратных средств (hardware fault tolerance);

ОС — операционная система (operational system);

PFD — вероятность отказа при наличии запроса (probability of failure on demand);

PCE — управление производственными процессами (process control engineering);

SIF — приборная функция безопасности (safety instrumented function);

SIS — приборная система безопасности (safety instrumented system);

SIL — уровень полноты безопасности (safety integrity level);

SPLC — программируемый логический контроллер устройства обеспечения безопасности (safety related programmable logic controller);

λ_{DU} — интенсивность наступления опасных невыявленных пассивных сбоев (rate of detected passive faults (dangerous undetected);

β — доля невыявленных пассивных сбоев с общей причиной (part of undetected passive faults with common cause).

4 Основные положения

4.1 Выбор устройств приборной системы безопасности

Основным критерием выбора установки, обеспечивающей безопасность, должна быть устойчивость к отказам. В соответствии с положениями настоящего стандарта необходимо принять меры:

- в отношении систематических сбоев (см. ПНСТ 366.1—2019, пункт 2.2.2);
- мнимых (случайных) сбоев (см. ПНСТ 366.1—2019, пункт 2.2.3);
- по повышению отказоустойчивости (см. ПНСТ 366.1—2019, пункт 2.3.8).

Для каждой приборной системы безопасности (SIS) (каждой приборной функции безопасности (SIF)) всегда должны учитываться все три вышеуказанные меры. Недостаточно просто демонстрировать малую вероятность возникновения неисправности функции SIF, основанную на мнимых отказах. Меры против систематических сбоев и меры по повышению отказоустойчивости приводятся на рисунке 1.

В частных случаях должны:

- выполняться испытания типа рабочих устройств в соответствии с установленными нормативными требованиями;
- производиться рассмотрение и утверждение особых мер, принимаемых независимыми организациями.

Рисунок 1 — Меры, принимаемые при использовании устройства в системе обеспечения безопасности

4.2 Меры против систематических сбоев

К мерам против систематических сбоев систем обеспечения безопасности относятся:

- меры против систематических сбоев самих устройств;
- меры против систематических сбоев, обусловленных инсталляцией производственной установки.

4.2.1 Систематические сбои устройств

Типовые систематические сбои самих устройств — это следствие ошибок проектирования их компонентов, использование ненадлежащих материалов в производственном процессе, следствие ошибок программного обеспечения при использовании микропроцессорных управляющих устройств. Вероятность наступления систематических сбоев самих устройств зависит от особенностей разработки и изготовления указанных устройств, а также квалификации обслуживающего персонала.

Если изготовитель обеспечил выполнение требований комплекса стандартов ГОСТ Р МЭК 61508, то можно считать, что систематические сбои самого устройства невозможны.

Декларация изготовителя о работоспособности устройства, используемого в установке с уровнем обеспечения безопасности SIL 2, не может гарантировать безотказной работы указанной установки в целом. Работоспособность конкретного устройства, используемого по особому назначению, а также конкретной установки рассматривается и утверждается в соответствии с нижеуказанной процедурой.

4.2.2 Систематические сбои, обусловленные эксплуатацией производственной установки

Изготовитель предоставляет пользователю только паспортную информацию о систематических сбоях в интерфейсе производственного процесса. Текущие данные функциональной надежности — это информация о работоспособности, о возможных систематических сбоях в конкретной рабочей ситуации. Устройство, имеющее сертификат (декларацию) изготовителя, должно всегда проверяться дополнительно независимой организацией с помощью конечной, обычно короткой, процедуры верификации качества «проверено-на-практике» (с учетом предшествующего опыта). В результате пользователь устройства может быть уверен, что устройство защищено от систематических сбоев и соответствует реальным условиям эксплуатации в составе установки. Если условия эксплуатации отдельного устройства идентичны условиям эксплуатации всей установки, то пользователь может использовать данное устройство в своем производственном процессе. Если условия эксплуатации устройства и установки отличаются, то пользователь может оценить указанные условия и принять соответствующие решения (например, использовать устройства другого типа).

Рекомендуется сначала опробовать стандартные устройства для рабочих функций и функций контроля. И только потом следует использовать данные устройства для функций безопасности. Необходимо иметь в виду, что рабочие функции могут отличаться от функций безопасности, особенно в режиме управления. Использование «вслепую» новых, даже сертифицированных, устройств без качества «проверено-на-практике» не рекомендуется. Разработка специальных полевых устройств и их использование (в рамках специальных приложений) в установках обеспечения безопасности ограничены.

4.3 Меры против мнимых сбоев

Вероятность наступления отказа установки обеспечения безопасности должна быть меньше допустимой. В ГОСТ Р МЭК 61511-1 определены индивидуальные уровни безопасности SIL, соответствующие вероятности наступления отказа по запросу PFD. Указанные данные основаны исключительно на анализе мнимых сбоев.

Изготовители устройств должны гарантировать, что вероятность наступления отказа устройства (λ_{DU}) достаточно низка и что данное устройство разработано в соответствии с требованиями качества, ассоциированными с соответствующим уровнем SIL. Пользователь должен нести ответственность за надлежащее использование устройства. Он должен регулярно проверять корректность функционирования устройства и его соответствие рассматриваемому производственному процессу.

4.4 Меры по повышению отказоустойчивости

Запрос на отказоустойчивость основан на производственном опыте. Значение интенсивности отказов λ_{DU}, определенное изготовителем, в большинстве случаев является статистически недостоверным. Если риски отказа высоки, то следует отказаться от планирования и эксплуатации одноканальных приборных систем безопасности с соответствующими значениями интенсивности λ_{DU}. Необходимо учитывать следующие требования безопасности:

- функции обеспечения безопасности с низкими рисками (с уровнем полноты безопасности ≤ SIL 2) могут быть одноканальными;
- функции безопасности с высокими рисками (SIL 3) должны иметь параллельные структуры (см. ПНСТ 366.3—2019).

4.5 Функционирование приборной системы безопасности

Все собственники рассматриваемых установок должны понимать, что необходимое уменьшение риска наступления отказа каждой функции безопасности SIF обусловлено временем ее функционирования и техническим обслуживанием. В добавление к периодическим испытаниям функций и их документации, необходимы регистрация и анализ отказов компонентов, оценка необходимости задействования приборной системы безопасности. Накопленный таким образом производственный опыт позволяет:

- уточнить концепцию обеспечения работоспособности системы безопасности, и
- оптимизировать порядок ее применения.

Необходимые условия рассмотрения и утверждения качества «проверено-на-практике» (на основе предшествующего опыта) используемых устройств:

- непрерывная регистрация и анализ систематических и мнимых сбоев приборной системы безопасности в течение длительного времени;
- задействование статистически предсказуемого количества устройств в приложениях.

Примечание — Следует убедиться в том, что статистика отказов учитывает только мнимые сбои.

4.6 Техническая эксплуатация

Оптимальная конструкция приборной системы безопасности SIS (максимально исключающая наступление систематических сбоев) — это конструкция, удовлетворяющая следующим трем критериям:

- работоспособность компонентов (см. ПНСТ 366.3—2019);
- использование соответствующих систем менеджмента безопасности (см. ПНСТ 366.2—2019);
- высокая квалификация сотрудников (см. ПНСТ 366.3—2019).

В нижеследующих разделах настоящего стандарта рассмотрены различные компоненты и приведены практические рекомендации по их технической эксплуатации. Структура указанных разделов фокусируется на рассмотрении жизненного цикла обеспечения безопасности в целом и на его отдельных фазах.

4.7 Требования к составлению документации

Результаты всех принятых мер в части технического обслуживания, особенно результаты инспекций, должны быть задокументированы (результаты рассмотрения установки в целом, результаты проверки ее отдельных агрегатов, состояние агрегатов в начале проверки, объем работ в рамках выполненного технического обслуживания и т. п.).

Оформление документов может производиться автоматически (например, с помощью диаграмм тренда, путем регистрации состояний, с помощью другой диагностической информации, предоставляемой датчиками, и т. п.).

Полученные результаты рекомендуется верифицировать после нескольких циклов испытаний (см. ПНСТ 366.3—2019, пункт 3.3.4.2).

Результаты начального пуска и результаты периодических испытаний должны заноситься в ведомость технического контроля.

5 Рекомендации для подсистем датчиков

Подсистемы датчиков содержат большое количество различных систем сбора результатов измерений значений переменных. Сигналы обычно передаются по электрическим цепям. Рассматриваемые подсистемы датчиков содержат как сами датчики, так и устройства преобразования измерительных сигналов (например, устройства питания измерительных преобразователей). Если результаты измерения передаются по полевой шине, то данная шина должна удовлетворять требованиям обеспечения безопасности передачи данных.

5.1 Назначение подсистемы датчиков

Если рассматриваемая подсистема содержит множество датчиков, то появляется возможность параметризации. Параметризация упрощает доступ к устройствам, позволяет легко изменять настройки приборных функций безопасности SIF во время работы. Вместе с тем, настройки устройств обеспечения безопасности должны быть защищены от «дурака» и несанкционированного доступа (см. ПНСТ 366.3—2019, пункт 2.2.1).

Необходимо задействовать результаты внутренней диагностики. Данные результаты должны включать:

- информацию о сбоях устройств;
- диапазон сигналов;
- информацию о состоянии устройств.

Датчик обычно имеет один канал и его отказоустойчивость (отказоустойчивость аппаратных средств — HFT) равна 0. Следовательно, функционирование одноканального датчика возможно только при уровне полноты безопасности не выше SIL 2. Отказоустойчивость HFT = 1 и уровень полноты безопасности SIL 3 могут быть обеспечены путем запараллеливания устройств (например, использование нескольких датчиков с уровнем полноты безопасности SIL 2 и т. п.), или путем использования (в исключительных случаях) одного сертифицированного устройства. Если для нескольких датчиков задействуются ресурсы программного обеспечения и параметризации, то важно учесть данную возможность уже на этапе планирования работ. Важно с самого начала гарантировать, что задействованное программное обеспечение отвечает требованиям уровня полноты безопасности SIL 3 и отвечает качеству «проверено-на-практике» (см. ПНСТ 366.3—2019, пункт 2.2.2.2).

Контакты с внешней средой могут привести к систематическим сбоям датчиков, снизить надежность работы устройств приборной системы безопасности SIS. Влияние условий производственного процесса на работу оборудования необходимо изучать и принимать во внимание уже на этапе разработки данного оборудования и подготовке порядка его технического обслуживания.

Для уменьшения числа систематических сбоев может оказаться целесообразным разнообразить способы запараллеливания устройств (например, взять два различных устройства, использующих идентичные или различные методы измерений).

Примечания

1 Одни и те же устройства могут иметь различные названия у различных поставщиков. В данном случае, разнообразия способов запараллеливания нет.

2 Отказоустойчивость аппаратных средств — это способность устройства (подсистемы) выполнять требуемые функции, связанные с обеспечением безопасности, даже при наличии одного или нескольких опасных сбоев аппаратных средств. HFT=1 означает, что имеется, например, два устройства, и опасный отказ одного устройства не препятствует принятию мер обеспечения безопасности (см. ГОСТ Р МЭК 61511-1, подраздел 11.4).

5.2 Уменьшение числа систематических сбоев во время реализации

Для предотвращения систематических сбоев пользователь должен учитывать рекомендации изготовителя и нижеследующие существенные факторы:

- коррозия (разрушение преимущественно металлических материалов вследствие физико-химических реакций);
- усталость материала;
- износ (потеря вещества при частом контакте с твердыми материалами);
- внешние отложения;
- старение (разрушение органических материалов, таких как пластики и эластомеры на свету и при нагреве);
- химические реакции (вздутие, потеря массы и расслоение органических материалов, таких как пластики и эластомеры).

В соответствии с ГОСТ Р МЭК 61508-2, пункт 7.4.7.4, примечание 3, ожидаемый срок службы электронных датчиков SIS составляет 8-12 лет. Данный срок службы сокращается в результате действия ряда факторов. Типовые меры увеличения срока службы полевых устройств:

- использование устройств с качеством «проверено-на-практике»;
- периодическая диагностика;
- надлежащее техническое обслуживание.

В каждом конкретном случае необходимо оформление соответствующих сопроводительных документов, например:

- документов станций технического обслуживания;
- отчетов по результатам исследований и испытаний;
- статистики отказов.

Наличие листа технических данных SIS облегчает работу и позволяет существенно снизить количество систематических сбоев.

5.3 Оценка интенсивности мнимых сбоев

Интенсивность мнимых сбоев устройства должна оцениваться уже во время его разработки. Интенсивность мнимых сбоев допускается оценивать по сертификату (декларации) изготовителя, если рассматриваемый уровень полноты безопасности не превышает SIL 2.

5.4 Установка и запуск

Все датчики, входящие в состав SIS, должны соответствовать спецификации безопасности с учетом их конструкции, особенностей установки и процедуры инсталляции. Все отклонения должны быть выявлены, задокументированы и оценены. Все соответствующие руководства по безопасности, руководство пользователя, инструкции по инсталляции и т. п. должны быть в наличии и должны выполняться. Все решения, касающиеся системы обеспечения безопасности, должны рассматриваться и утверждаться.

Установка и запуск устройств производятся в соответствии с ПНСТ 366.3—2019, подраздел 2.3. Важную роль играет ведомость технического контроля (например, испытания подсистем датчиков и т. п.).

5.5 Функционирование и техническое обслуживание

При работе установки, приборная система безопасности SIS управляется и обслуживается так, что фактическая вероятность наступления отказа меньше нормативной вероятности наступления отказа по запросу, определяемой уровнем полноты безопасности SIL.

Для выполнения установленных требований к датчикам важно сначала выявить их систематические и мнимые сбои, а затем устранить их.

Для периодических испытаний может потребоваться значительный тестовый охват. Он должен быть обеспечен соответствующими средствами измерений. Необходимый тестовый охват определяется на стадии планирования технического обслуживания. На данной стадии определяется и необходимый интервал между испытаниями. К моменту пуска установки следует подготовить руководство (инструкцию) по проведению испытаний.

В основе данного руководства (инструкции) по проведению испытаний должен лежать перечень всех возможных сбоев (см. ПНСТ 366.3—2019, подраздел 2.4). Некоторые сбои можно выявить путем диагностики внутренних устройств. Дополнительная информация содержится в соответствующих руководствах по техническому обслуживанию установки. Прочие сбои выявляются и оцениваются путем принятия дополнительных мер и проведения дополнительных испытаний.

С учетом вышесказанного необходимо обязательно проверить нижеследующие аспекты:

- выполнение функции безопасности по запросу;

- наличие выходного сигнала при моделировании ситуации сбоя устройства (сбоя датчика);
- реакцию устройства при сбое одного канала в запараллеленной структуре;
- точность измерения набора данных;
- сравнение со спецификацией требований безопасности (см. ПНСТ 366.3—2019, приложение, пример 2);
- временная последовательность и время срабатывания;
- визуальный осмотр устройства (например, осмотр повреждений, осмотр меток и т. п.);
- электрические и механические соединения (герметичность соединений, прочность соединений и т. п.);
- коррозия, грязь, химическое воздействие и т. п.

Если имеются указания на возможный сбой во время функционирования установки, то данные указания требуют верификации. Причины сбоев немедленно должны устраняться и должны приниматься все необходимые защитные меры.

Таблица 1 — Типовые сбои подсистем датчиков и их выявление

Сбои (примеры)	Выявляемые сбои		Процедура выявления сбоя
	Электронные устройства	Аналоговые устройства	
Короткое замыкание линии, перекрестное замыкание	Выявляется частично	Выявляемый	Диапазон значений сигнала (3,8...20,5) мА. Проверка разности значений Δw в каналах
Обрыв линии, высокое сопротивление перехода	Невыявляемый, но неопасный (правило «тока холостого хода»)	Выявляемый	Диапазон значений сигнала (3,8...20,5) мА. Проверка разности значений Δw в каналах
Отделение от производственного процесса	Невыявляемый, но неопасный (правило «тока холостого хода»)	Выявляемый	Диапазон значений сигнала (3,8...20,5) мА. Проверка разности значений Δw в каналах
Сигнал вышел за границы диапазона измерения	Выявляемый	Выявляемый	Диапазон значений сигнала (3,8...20,5) мА
Дрейф сигнала, старение	Невыявляемый	Выявляемый (регистрация истории)	Проверка разности значений Δw в каналах, регистрация данных
Производственные шумы, шумы переговорного устройства, сбой передатчика	Невыявляемый	Выявляемый	Проверка разности значений Δw в каналах
«Замораживание» сигнала (на минимальном значении, на максимальном значении, внутри диапазона значений)	Невыявляемый	Выявляемый	Сигнал аналогового устройства обычно «дрейфует» (может изменяться в пределах нескольких мА). Чисто статистически — это сбой. Требует постоянного наблюдения
Значения лежат внутри диапазона, но это сбой	Невыявляемый	Выявляемый	Проверка ранее определенного диапазона, в котором должно лежать данное значение на рассматриваемой стадии производственного процесса
Сбой передатчика	Невыявляемый	Выявляемый	Проверка разности значений Δw в каналах. Проверка Δt при больших Δw

5.6 Автоматическая диагностика при функционировании

Сигналы аналоговых датчиков предоставляют больше возможностей для диагностики по сравнению с сигналами электронных датчиков. Использование измерительных сигналов со значениями в диапазоне 4-20 мА позволяет выявить большинство сбоев: обрыв провода, короткое замыкание, выход за границы диапазона измерений и т. п. При наличии программируемого логического контроллера устройства обеспечения безопасности (SPLC) открывается возможность выполнения расширенной автоматической диагностики.

Дополнительная диагностика ведет к увеличению охвата диагностикой (DC) (см. ГОСТ Р МЭК 61511-1—2018, пункт 3.2.15). При этом повышается коэффициент технического использования устройств обеспечения безопасности, увеличивается расчетный интервал между испытаниями.

По данной причине на практике часто предпочтение отдается комбинации: «измерительные сигналы аналоговых устройств» + «логический контроллер SPLC».

6 Рекомендации для подсистем пусковых устройств

В соответствии с настоящим стандартом, подсистемы пусковых устройств (исполнительных устройств) включают устройства позиционирования (в контурах устройств обеспечения безопасности) и приводные механизмы (например, электромагнитные клапаны). Типовые источники энергии — пружины, гидравлические (пневматические) агрегаты. Сюда относятся: механические установки, пневмоустройства, гидравлические агрегаты, силовые электрические машины, электропроводка сигнальных устройств. В данном разделе настоящего стандарта требования к приводным механизмам и особенности их энергообеспечения не рассматриваются.

6.1 Особенности подсистем пусковых устройств

Преимущества механических подсистем пусковых устройств перед электронными заключаются в:

- ограниченном числе компонентов;
- макроскопическом размере компонентов;
- понятном принципе действия;
- понятном диапазоне функциональных возможностей;
- малой вероятности сбоя (или даже полном исключении возможности сбоя) при надлежащей конструкции устройства.

Если пусковое устройство одноканальное, то его значение отказоустойчивости HFT = 0, и уровень полноты безопасности не более SIL 2. Уровень полноты безопасности SIL 3 достижим, если значение отказоустойчивости HFT = 1. Этого можно добиться путем запараллеливания каналов (например, использования нескольких пусковых устройств с уровнем полноты безопасности SIL 2). На уровне полноты безопасности SIL 3 одноканальные пусковые устройства допустимы только при выполнении дополнительных условий (например, обеспечение требуемого уровня диагностики и т. п.), определяемых конкретным приложением.

Постоянный контакт с окружающей средой ведет к систематическим сбоям, повышает коэффициент технического использования устройств обеспечения безопасности. Необходим мониторинг реальных производственных условий функционирования установки. Реальные производственные условия следует учитывать уже при конструировании установки, при планировании ее технического обслуживания. В ряде случаев, например, целесообразно повысить коэффициент запаса привода, сократить интервал между испытаниями.

Опыт показывает: число систематических сбоев можно уменьшить, если варьировать способы запараллеливания (например, использовать разные устройства позиционирования, разные шаровые клапаны и т. п.).

Если устройство позиционирования контура безопасности задействовано «в параллель» при управлении рабочим контуром, то (вследствие непрерывного движения устройства) увеличивается коэффициент технического использования устройств обеспечения безопасности, увеличивается охват диагностикой SIS. Однако работа «в параллель» несет дополнительный риск. Данный аспект необходимо учитывать при анализе рисков (см. ПНСТ 366.3—2019, пункт 2.2.1).

Надежность механических компонентов падает, если их конструкция не удовлетворяет установленным требованиям, если производственные условия неблагоприятны или если «происходят» систематические сбои. Накопленный опыт показывает, что мнимые сбои имеют второстепенное значение. Это также необходимо учитывать при пользовании базами данных.

6.2 Предотвращение систематических сбоев

Для предотвращения систематических сбоев пользователь (в добавление к рекомендациям изготовителя) должен учитывать нижеследующие факторы:

- наличие коррозии (разрушение преимущественно металлических материалов в результате физико-химических реакций);
- усталость материала;
- износ (унос материала взвешенными твердыми частицами потока жидкости);
- осадок (налет), обусловленный контактом с окружающей средой;
- старение (разрушение органических материалов, таких как пластики и эластомеры под действием света и температуры);
- химические воздействия (вздутие, унос массы и расслоения органических материалов, таких как пластики и эластомеры).

Срок службы пускового устройства существенно зависит от производственных условий. Накопленный опыт показывает, что такие меры, как:

- использование модулей с качеством «проверено-на-практике»;
- непрерывная диагностика;
- надлежащее техническое обслуживание могут существенно увеличить срок службы.

В каждом конкретном случае необходимо оформление соответствующих сопроводительных документов, например:

- документов станций технического обслуживания;
- отчетов с результатами исследований и результатами испытаний;
- статистики отказов.

Число систематических сбоев можно уменьшить, если пользоваться таким инструментом как лист технических данных приборной системы безопасности SIS.

6.3 Предотвращение мнимых сбоев

Интенсивность мнимых сбоев должна оцениваться уже на этапе разработки модулей. Интенсивность мнимых сбоев допускается оценивать по сертификату (декларации) изготовителя, если рассматриваемый уровень полноты безопасности не превышает SIL 2.

6.4 Установка и запуск

Все пусковые устройства приборной системы безопасности SIS должны удовлетворять требованиям спецификации устройства обеспечения безопасности в части этапов их проектирования, создания и установки. Возможные отклонения должны быть выявлены, задокументированы и оценены. Соответствующие руководства по безопасности, руководства пользователя, инструкции по установке должны быть доступны. Необходимо обеспечить их соответствие требованиям. Все решения по управлению системой обеспечения безопасности рассматриваются и утверждаются в установленном порядке.

Важным инструментом обеспечения требований является ведомость технического контроля.

6.5 Функционирование и техническое обслуживание

В ходе технологического процесса управление и техническое обслуживание приборной системы безопасности SIS производится так, чтобы реальная вероятность наступления отказа по запросу была меньше нормативной вероятности наступления отказа по запросу, соответствующей заданному уровню полноты безопасности SIL.

Для выполнения требований к подсистеме пусковых устройств важно выявить систематические и мнимые сбои модулей пусковых устройств и устранить их.

Во время периодических испытаний важно обеспечить значительный тестовый охват. Он гарантируется принятием соответствующих мер. Достаточный тестовый охват определяется на этапе планирования технического обслуживания (например, по методике FMEDA). При этом определяется достаточный интервал между испытаниями. Руководство по испытаниям должно быть в наличии при пуске оборудования.

Базовым элементом руководства по испытаниям является перечень всех возможных отказов установки.

6.5.1 Периодические контрольные испытания

Контрольные испытания включают функциональные испытания и визуальный осмотр установки в соответствии с указаниями изготовителя.

Функциональные испытания установки включают, например:

- перевод рукоятки клапана в безопасное положение;
- проверку достоверности указанного безопасного положения;
- «прозвон» и регулировку контактов конечного положения;
- верификацию атмосферной герметичности;
- измерение интенсивности протечек;
- разборку и тестирование устройств на специальной станции;
- измерение времени открытия/закрытия устройств (отслеживание сигнала монитора до момента перехода устройства в безопасное положение);
- измерение времени задержки (отслеживание сигнала монитора до момента начала движения устройства позиционирования);
- верификацию величины приводной силы, запаса мощности по силе, запаса мощности по крутящему моменту, а также начального пускового момента электродвигателя, рабочего крутящего момента, момента отвода рабочего органа в гнездо и т. п.;
- верификацию диаграммы «путь—время» для равномерного движения.

Визуальный осмотр установки включает проверку:

- повреждений устройства позиционирования, повреждений механических соединений;
- герметичности пневматических соединений;
- электрических соединений;
- наличия коррозии, грязи и химических воздействий;
- фактов необычных рабочих ситуаций (например, возникновение вибраций, посторонних звуков и т. п.).

Результаты всех испытаний должны быть задокументированы (общие результаты, степень соответствия установленным критериям, состояние объекта перед началом испытаний, принятые корректирующие меры и т. п.).

Документы, по возможности, должны оформляться автоматически. Это могут быть тренд изменения характеристики в виде диаграммы «путь—время», кривая (профиль) давления и т. п. Данные документы оформляются, например, с помощью диагностической коммуникационной системы (DCS) или с помощью соответствующих опций устройства позиционирования.

Тренды на основе результатов испытаний составляются на временном горизонте в несколько лет (см. ПНСТ 366.3—2019, пункт 3.3.4.2).

Если имеются указания на возможные неисправности технологической системы и системы обеспечения безопасности, то данные указания должны верифицироваться, немедленно выявляться причины неисправностей и приниматься соответствующие меры.

6.5.2 Функциональная активация устройства позиционирования

Функциональная активация устройства позиционирования — это контрольное испытание. Его результаты должны документироваться (см. ПНСТ 366.3—2019, пункт 3.3.3.3). Объем данных контрольных испытаний оценивается в сравнении с объемом периодических контрольных испытаний.

Допускается автоматическое документирование результатов контрольных испытаний.

6.5.3 Ручные испытания в ходе работы технологической линии

Ручные испытания в ходе работы технологической линии проводятся по календарному плану. Целью данных испытаний является:

- подтверждение работоспособности устройства позиционирования в конкретных рабочих условиях;
- верификация допущений методики FMEDA, принятых, например, для анализа нового производственного процесса;
- увеличение объема контрольных испытаний:
  - для поиска невыявленных систематических (мнимых) сбоев;
  - для увеличения коэффициента безопасности установки;
- увеличение интервала между испытаниями.

Объем контрольных испытаний можно оценивать путем суммирования всех типов сбоев, оценки относительной частоты их наступления, сравнения результатов валидации и степени соответствия установленным критериям испытаний, проводимых в ходе работы технологической линии.

Критерии достоверности допущений и результатов испытаний установлены в подразделе «Периодические контрольные испытания».

Запараллеливание устройств (для повышения коэффициента их технического использования) может потребовать увеличения объема контрольных испытаний.

6.6 Автоматическая диагностика в ходе работы технологической линии

Преимуществом данного вида испытаний является то, что производственный процесс не прерывается. Данные испытания можно проводить достаточно часто (см. ПНСТ 366.3—2019, подраздел 2.5). Автоматические испытания повышают вероятность PFD устройства и обеспечивают дополнительную защиту от невыявленных систематических и мнимых сбоев. При определенных условиях интервал между контрольными испытаниями может быть увеличен.

Эффективный метод испытаний — испытания клапана при неполном ходе. При неполном ходе клапана устройство позиционирования некоторое время движется в сторону его безопасного положения. Влияние испытания на производственный процесс исключено. Проверяемые параметры:

- время задержки;
- время движения;
- приводная сила;
- запас мощности по силе.

Важным инструментом оценки является диаграмма «путь—время». При испытаниях с неполным ходом клапана выявляется большинство сбоев (кроме протечек и ухода положения замыкания).

Таблица 2 — Типовые сбои подсистем пусковых устройств и их выявление

Сбой	Возможная причина сбоя	Возможность выявления сбоев		Процедура выявления сбоя
		Испытание с неполным ходом клапана	Испытание с полным ходом клапана	
Электромагнитный клапан не переключается	Электромагнитный клапан не активируется	Выявляемый	Выявляемый	Выявляется по сигналу обратной связи о положении устройства
Электромагнитный клапан не переключается	Дефект электромагнитного клапана	Выявляемый	Выявляемый	Выявляется по сигналу обратной связи о положении устройства
Клапан срабатывает слишком медленно	Ограничена подача воздуха в клапан	Выявляемый	Выявляемый	Выявляется путем мониторинга до момента выдачи сигнала обратной связи о положении устройства
Клапан срабатывает слишком медленно	Движение клапана затруднено	Выявляемый	Выявляемый	Выявляется путем мониторинга до момента выдачи сигнала обратной связи о положении устройства
Клапан не закрывается полностью	Гнездо клапана «поцарапано», конус «размыт»	Невыявляемый	Выявляемый	Выявление сбоя путем активации клапана невозможно
Клапан не закрывается полностью	Гнездо клапана содержит отложения	Невыявляемый	Выявляемый	Выявление сбоя путем активации клапана невозможно
Клапан не закрывается	Вал клапана заблокирован	Выявляемый	Выявляемый	Выявляется по сигналу обратной связи о положении устройства
Клапан не открывается полностью	Гнездо клапана содержит отложения	Невыявляемый	Выявляемый	Выявление сбоя путем активации клапана невозможно
Клапан не открывается совсем	Клапан «заело»	Выявляемый	Выявляемый	Выявляется по сигналу обратной связи о положении устройства

Интервал между автоматическими испытаниями может быть очень коротким по сравнению с интервалом между периодическими испытаниями.

Если испытания автоматические, то соответствующие измеренные значения можно документировать также в автоматическом режиме. Сюда, например, относится регистрация конечного положения клапана с неполным ходом (полученного с помощью контактов дискретных положений, детекторов положений в независимой системе и т. п.).

Для оценки эффективности пускового устройства могут потребоваться соответствующие дополнительные системы датчиков (датчики температуры, расхода, дифференциального давления и т. п.). Датчики устанавливаются до или после (по потоку) устройства позиционирования.

7 Рекомендации для логического решающего устройства

7.1 Спецификация рабочего диапазона

Логическим решающим устройством (логическим решателем) приборной системы безопасности SIS может быть:

- Программируемый логический контроллер устройства обеспечения безопасности SPLC;
- Программируемый JPC-контроллер.

Логический решатель содержит следующие компоненты: входной модуль, логический решатель (центральный процессор) и выходной модуль. Необходимость в дополнительных модулях определяется изготовителем. Как правило, это устройства передачи данных от входного модуля к логическому решателю и далее к выходному модулю.

SPLC-контроллер может иметь:

- интегральную структуру типа «три-в-одном» (включает сразу входной модуль, логический решатель и выходной модуль);
- модульную структуру (включает отдельно входной модуль, отдельно логический решатель и отдельно выходной модуль, соединенные, например, шиной данных).

7.2 Особенности логического решателя

Устройство SPLC-контроллера намного сложнее устройства полевого оборудования. Поэтому очень важно следовать рекомендациям руководства пользователя и инструкциям изготовителя. Определяющими факторами являются:

- временные характеристики (продолжительность цикла, время работы программы и т. п.);
- особенности конкретного отказа;
- несанкционированный доступ к оборудованию;
- сложность прикладной программы пользователя;
- устройство интерфейсов компонентов и систем.

Для работы с указанными системами требуются специалисты повышенной квалификации.

7.3 Инженерное обеспечение

7.3.1 Спецификация конструкции логического устройства

Одним из условий использования SPLC-контроллера является оценка и учет положений и требований руководства изготовителя по обеспечению безопасности. От этого зависит степень эффективности использования модуля, правильность выбора типа соединения полевых устройств, работоспособность прикладной программы пользователя. Указанные положения и требования следует сравнить с требованиями спецификации требований к безопасности SRS и верифицировать их.

Время реакции логического решателя определяется:

- текущими значениями электрических сигналов;
- пределами допуска;
- особенностями конкретного сбоя.

При возникновении проблем принимаются меры по модификации, адаптации и настройке оборудования с учетом современного состояния техники.

7.3.2 Особенности инженерного обеспечения

Эффективность применения SPLC контроллера зависит от выполнения требований, установленных в руководстве по безопасности и индивидуальным листом технических данных.

Если в исключительных случаях функции обеспечения безопасности и рабочие функции соединены в одной системе, то следует добиться их полной независимости и исключить их взаимовлияние (см. ПНСТ 366.3—2019, пункт 2.2.3.1).

При запараллеливании устройств необходимо обеспечить соответствие коэффициента технического использования функций безопасности и рабочих функций оборудования установленным требованиям.

7.3.3 Программирование

Важным требованием к программам является простота и доступность при проведении испытаний и воспроизведении (см. ПНСТ 366.3—2019, пункт 2.2.1).

Внутренняя автоматическая диагностика (выполняемая операционной системой) должна дополняться программируемой диагностикой и мониторингом (например, мониторингом отклонений, мониторингом времени работы клапана, оценкой сигналов сбоя и т. п.). Результаты диагностики имеют смысл, если они своевременно попадают к оператору. Результаты диагностики используются при оценке расчетной интенсивности наступления сбоев. Для эффективной обработки сигналов может потребоваться дополнительная диагностика (например, диагностика типовых рабочих функций полевых устройств, работающих с параллельными каналами, см. рисунок 2).

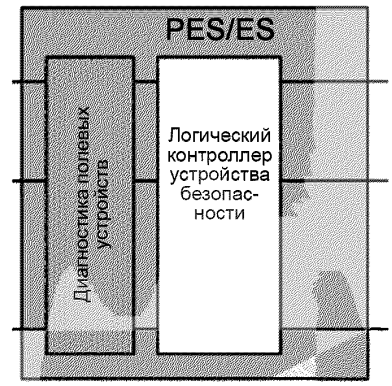

Рисунок 2 — Диагностика рабочих функций полевых устройств, работающих с параллельными каналами

Система обеспечения безопасности должна включать необходимое программное обеспечение и установленную процедуру верификации.

7.4 Техническое обслуживание

Техническое обслуживание выполняется только квалифицированным персоналом в соответствии с руководством изготовителя.

Ниже устанавливаются временные интервалы между испытаниями, а также определяются требования к испытаниям.

Охват диагностикой рассматриваемых систем очень велик. Вероятность наступления отказа достаточно мала. Поэтому изготовители «закладывают» в оборудование большие интервалы между испытаниями. В среднем они составляют 10 и более лет.

Корректность и работоспособность прикладной программы пользователя обязательно проверяется во время периодических испытаний приборной системы безопасности SIS.

7.5 Модификации

Модификации подразделяются на модификации:

- аппаратных средств (текущее обновление, производится изготовителем);
- операционной системы (обновление текущей версии, производится изготовителем);
- аппаратных средств и прикладной программы пользователя (производится пользователем).

В целях обеспечения безопасности обновлений приборной системы безопасности SIS, по возможности, следует избегать.

Решение по обновлению оборудования и программного обеспечения принимается пользователем по экономическим соображениям. Обновление оборудования и программного обеспечения не связано с повышением безопасности установки.

Модификация установки производится в соответствии с руководством пользователя и инструкциями изготовителя по обеспечению безопасности.

7.5.1 Обновление оборудования

Прежде чем устанавливать новое оборудование, необходимо проверить его сертификацию. В большинстве случаев новое оборудование имеет новую версию операционной системы.

При обновлении оборудования необходимо проверить листы технических данных новых модулей, уточнить требования безопасности (изложенные в руководстве по обеспечению безопасности и т. п.).

Учет вышесказанного может потребовать:

- дополнительной модификации подсистемы датчиков, подсистемы пусковых устройств приборной системы безопасности SIS (приборной функции безопасности SIF);
- изменения интервалов между испытаниями;
- дополнительных испытаний;
- дополнительного технического обслуживания;
- оформления сопроводительной документации.

7.5.2 Обновление версии программного обеспечения

Обновление версии программного обеспечения — это установка нового программного обеспечения системы. Прежде чем устанавливать новое программное обеспечение, нужно проверить его сертификацию, соответствие имеющемуся устройству обеспечения безопасности, соответствие имеющимся аппаратным средствам.

В большинстве случаев новые версии операционной системы (ОС) обеспечивают устранение ранее выявленных сбоев (сбоев, выявленных ОС предшествующей версии). Новая версия ОС может иметь свои особенности, а также более продвинутые возможности диагностики.

Возможные последствия обновления версии программного обеспечения аналогичны рассмотренным в 7.5.1. Обычно обновление версии программного обеспечения никак не влияет на прикладную программу пользователя. Если такое влияние существует, то оно должно быть отражено в сопроводительных документах изготовителя. Обязательно проводятся испытания установленной новой версии программного обеспечения. Результаты испытаний должны документироваться.

7.5.3 Модификации аппаратных средств и/или прикладных программ пользователя

Указанные модификации оказывают влияние на:

- ранее установленные модули и компоненты;
- новые инсталляции старых модулей и компонентов;
- новые инсталляции ранее не использованных модулей (новые принципы работы функций, модули следующего поколения и т. п.);
- прикладные программы пользователей.

Функциональность оставшейся без изменения приборной системы безопасности SIS должна верифицироваться. Это особенно важно, когда старые аппаратные средства (старое программное обеспечение) удалено. Выполняются процедуры, аналогичные определенным в 7.5.1. Принятые решения рассматриваются и утверждаются в установленном порядке.

8 Право на продолжение использования

8.1 Продолжение использования существующей приборной системы безопасности

При оценке возможности продолжения использования существующей приборной системы безопасности нет необходимости пересматривать (модифицировать) существующие приборные системы безопасности SIS, если они были надлежащим образом спроектированы, установлены и приняты в эксплуатацию в соответствии с имевшими юридическую силу нормативными документами. Это означает, что:

а) анализ безопасности установки должен показывать, что функция безопасности определена корректно. Конструкция устройства и порядок его технического обслуживания соответствуют имеющемуся производственному риску. На все определенные меры обеспечения безопасности имеются соответствующие документы. Все необходимые меры могут быть при необходимости приняты;

б) запросы на активацию приборной системы безопасности SIS, поданные в процессе анализа безопасности установки, успешно выполнены. Накопленный опыт эксплуатации, задокументированные результаты функциональных испытаний и «выпадающая» статистика не дают оснований к замене действующей приборной системе безопасности SIS.

Если существующая приборная система безопасности SIS не соответствует имевшим место ранее нормативным требованиям, то пользователь данной системы SIS не имеет права на продолжение ее использования. В таком случае, данная система должна быть модифицирована, чтобы удовлетворять новым нормативным документам. Если же имеет место некомплект документации, то радикальную модификацию можно заменить совершенствованием установки с учетом ее особенностей.

Если анализ безопасности установки, выполненный в соответствии с новыми нормативными документами, показывает, что уровень полноты безопасности установки превышает необходимый, то систему SIS можно оставить как есть. Данное решение рассматривается и утверждается в установленном порядке.

8.2 Процедура модификации приборной системы безопасности

В результате модификации, обновления и совершенствования технологической установки (приборной системы безопасности), может потребоваться переоценка области применения и типа модификации. Право на продолжение использования оборудования может быть утрачено по нижеследующим причинам:

- изменился риск (например, используется новый материал, изменились условия производства и т. п.);
- изменились функции безопасности (план использования функций);
- изменились условия производства и снизилась надежность SIS (например, датчики и пусковые устройства больше не соответствуют условиям производства);
- изменилось инженерное обеспечение производственного процесса (произошла замена оборудования);
- изменилось законодательство, например, экологические нормативные документы (предохранительный клапан не соответствует требованиям, так как его выбросы больше не соответствуют установленным нормативам).

Вместе с тем, право на продолжение использования оборудования может сохраниться, если изменения оборудования произведены на уровне отдельных компонентов, например:

- компонентов на замену старых модулей (полевого оборудования, контроллеров) больше нет в продаже. Приходится приобретать устройства новой конструкции;
- при замене старых систем SIS на новые, в случае, когда старые системы заменяются на системы новой конструкции по экономическим и другим причинам;
- изменение условий производства (с известными слабыми местами) может потребовать изменения интервала между испытаниями, типа испытаний, замены некоторых модулей;
- изменение предельных значений.

9 Применение на основе предшествующего опыта (качество «проверено-на-практике»)

Цель обеспечения качества «проверено-на-практике» (на основе предшествующего опыта) заключается в максимальном уменьшении числа систематических сбоев самого модуля во время его использования. Вышесказанное относится к сбоям, причина которых лежит в технологии разработки изделия, а также в технологии его изготовления (например, ошибки спецификации, ошибки программного обеспечения, ошибки при изготовлении и т. п.). Сюда относятся ошибки эксплуатации и установки модуля (например, ошибки калибровки, неправильно выбранное место установки, ошибки технического обслуживания и т. п.). Сюда также относятся сбои, обусловленные тяжелыми условиями эксплуатации (например, сильные вибрации, крайне высокая/низкая температура, чрезмерная коррозия/эрозия и т. п.).

Вероятность наступления таких сбоев можно снизить до начала производства путем принятия соответствующих мер изготовителем и пользователем.

УДК 658.52.011.56:006.354 ОКС 13.110, 25.040.01

Ключевые слова: системы автоматического управления производственными процессами; производственные процессы; приборные системы безопасности; уровень полноты безопасности

БЗ 10—2019/120

Редактор *П.К. Одинцов*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 24.09.2019. Подписано в печать 03.10.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,16.
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.
www.gostinfo.ru info@gostinfo.ru