ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Издание официальное

Москва
Стандартинформ
2019

Предисловие

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

2 ВНЕСЕН Техническим комитетом 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. № 39-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 в 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 (настоящий стандарт);
- Часть 4. Верификация полноты аппаратных средств автоматизированной системы безопасности;
- Часть 5. Руководство по практическому применению;
- Часть 6. Приложения для обеспечения безопасности промышленных предприятий с повышенным уровнем опасности.

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

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ И ИНТЕГРАЦИЯ

Обеспечение безопасности промышленных предприятий за счет использования систем автоматического управления процессами

Часть 3

Подготовка, запуск и эксплуатация устройств безопасности

Industrial automation systems and integration. Safety and security arrangements of industrial process plants by means of process control engineering. Part 3. Facility design, engineering and operation

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 содержит рекомендации по разработке, созданию и обеспечению функционирования приборных систем безопасности, соответствующих требованиям комплекса национальных стандартов ГОСТ Р МЭК 61511*.

Настоящий стандарт применяется совместно с другими частями настоящего комплекса предварительных национальных стандартов, в которых рассмотрены вопросы практической реализации устройств автоматического управления производственными процессами в рамках общей концепции безопасности.

2 Подготовка и запуск устройств безопасности

При разработке промышленных объектов необходимо учитывать, что все устройства безопасности должны быть в обязательном порядке испытаны, верифицированы и валидированы. Испытания проводят не позднее, чем перед этапом ввода системы в эксплуатацию. Если проект большой, то возникает необходимость проведения промежуточных этапов испытаний.

2.1 Спецификация устройств безопасности

2.1.1 Выбор переменных производственного процесса, соответствующих функции безопасности

Предпочтительные переменные функций безопасности производственного процесса — это переменные, которые можно измерить непосредственно простым и достоверным способом (методом). Непрямой вывод переменных функций безопасности производственного процесса (путем комбинирования измерительных сигналов) используется, когда:

1) непосредственное (прямое) измерение значений переменных функций безопасности производственного процесса невозможно;

2) надежный метод измерения отсутствует.

* ГОСТ Р МЭК 61511 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов».

Издание официальное

Переменные функций безопасности производственного процесса, параметры подготовки и активации устройств безопасности должны измеряться с необходимой точностью и достаточной скоростью.

Диапазон измерения переменных функций безопасности должен выбираться исходя из установленного при проведении измерений разрешения. Предельные значения переменных должны находиться достаточно далеко от краев диапазона измерения. Этим обеспечивается необходимое условие, при котором отклонения результатов измерений находятся в пределах допуска. При расчете предельных значений переменных должна учитываться динамика производственного процесса.

Измеренные значения аналоговых переменных производственного процесса непрерывно выводятся на экран диспетчерской вместе с соответствующими предельными значениями. Они могут также выводиться на экран соответствующего терминала оператора. Установленные предельные значения не могут быть произвольно изменены.

2.1.2 Требования к устройствам обеспечения безопасности

Требования к устройствам обеспечения безопасности определяются функциями безопасности с назначенным уровнем полноты безопасности (SIL), а также планом обеспечения безопасности предприятия. Один программируемый логический контроллер (PLC) системы безопасности может обработать сигналы сразу нескольких функций безопасности.

Спецификации корректного планирования работы устройств безопасности составляются с учетом результатов оценки риска, они должны включать:

- описание необходимых функций безопасности;
- определение безопасного состояния каждой конкретной функции безопасности;
- уровень полноты безопасности (SIL), назначенный каждой функции безопасности;
- знание безопасных состояний производственного процесса, содержащих риск при штатном срабатывании некоторых устройств безопасности (например, перегрузка аварийного контейнера, аварийный сброс газов в систему вентиляции, выброс пламени и т. п.);
- знание необходимого времени отклика каждой конкретной функции безопасности, чтобы предотвратить переход производственного процесса в небезопасное состояние (время сохранения работоспособности при отказе производственного процесса);
- описание рабочих режимов (например, режима запуска, режима отключения и т. п.) установки, перечень функций безопасности, необходимых для работы установки в каждом конкретном рабочем режиме.

Необходимая информация по планированию работы устройств безопасности должна включать:

- функциональные спецификации, требуемые интервалы времени между испытаниями, список измеряемых переменных производственного процесса, их предельные значения;
- список переменных управления, определение порядка их применения;
- функциональные соотношения между входными и выходными сигналами, включая логические операции, математические функции, авторизацию доступа;
- требования отключения установки в ручном режиме;
- требования перезагрузки устройства безопасности после отключения установки;
- возможные отказы устройства безопасности, требуемые реакции на типовые события (например, переход в аварийный режим, переход в режим автоматического отключения и т. п.);
- определения всех необходимых мер достижения (поддержания) безопасного состояния в случае выявления отказа устройства безопасности. При выборе указанных мер обязательно должен учитываться человеческий фактор;
- специальные требования по вводу в эксплуатацию и повторному запуску устройства безопасности;
- все интерфейсы связи устройств безопасности с другими системами (отсутствие паразитных обратных связей);
- требования безопасности к программному обеспечению приложений, спецификации управления с блокировкой автоматики, особенности подавления сигнала, возможности задействования обводного контура;
- достижимое время ремонта устройств безопасности (минимальное время, наихудший случай) с учетом времени перемещения к месту ремонта, определения места ремонта, наличия запчастей, наличия контракта на данную услугу, состояния окружающей среды и т. п.;
- необходимо учитывать возможные опасные комбинации начальных состояний устройств безопасности (например, наличие внутренних блокировок и т. п.).

2.2 Конструкция и планирование работы устройств безопасности

2.2.1 Общие требования

Устройства безопасности могут быть как аппаратно-, так и программно-реализуемыми. Важно, чтобы:

1) конструкция устройств безопасности была простой и понятной;

2) устройство безопасности установки не модифицировалось в ходе ее функционирования (см. раздел 3);

3) если для специальных режимов работы необходима блокировка автоматики (например, для режима запуска), то это должно происходить автоматически, в узком временном диапазоне. Отказ блокирующего устройства не должен привести к блокировке всей автоматики;

4) для релейных логических контроллеров (RLC) выбирают доступные сертифицированные системы. Предпочтение отдается «проверенным на практике» устройствам и принципам переключения;

5) для программируемых систем автоматизации, т. е. для систем управления производственными процессами (PCS) и программируемых логических контроллеров (PLC), принимается нижеследующий базовый принцип:

а) системы с сертификатом безопасности (аппаратное обеспечение, программное обеспечение) используются как в одноканальных, так и в многоканальных устройствах обеспечения безопасности. При этом необходимо учитывать допустимый диапазон приложений, указанный в отчетах об испытаниях (в руководстве по безопасности);

б) используемое программное обеспечение системы должно быть написано на понятном, хорошо известном языке программирования.

Примечание — Рекомендуются графические языки, определенные в ГОСТ Р МЭК 61131-3.

6) требования к программному обеспечению пользователя:

а) пользовательские программы должны составляться по модульному принципу с типовыми функциями и функциональными блоками. Указанные функции должны легко испытываться и безопасно модифицироваться. Рекомендуемые приемы и методы программирования:

- разработка структурированной программы;
- понятная организация программы посредством заголовков и комментариев;
- использование доступных верифицированных модулей и компонентов. Предпочтение следует отдавать функциональным блокам, предлагаемым (сертифицированным) изготовителем;
- лучше использовать символические имена, чем физические адреса;
- имена основных переменных должны быть информативными;
- безопасное программирование (например, содержащее испытания типа, проверки диапазонов значений, проверки достоверности, мониторинг конфигурации аппаратного и программного обеспечения и т. п.);
- в качестве дополнительных требований рекомендуется избегать:
- использования лишних шагов в программах;
- использования лишних переменных;
- «нестандартного программирования» (например, оптимизации памяти путем многократного использования одной переменной);

б) применение общепринятых правил программирования, ассоциированных учебников по программируемым логическим контроллерам системы безопасности;

в) все программы пользователей должны быть задокументированы. Версия документации должна быть однозначной. Соответствие пользовательских программ нормативной документации должно быть заверено (например, подписями, указанием номера версии и т. п.). Типовой список основной документации программируемого логического контроллера PLC системы безопасности должен состоять из:

- программной документации;
- спецификаций функции безопасности (регистрация результатов оценки безопасности);
- перечня перекрестных ссылок;
- таблицы присваиваний;
- информации о параметризации (конфигурации) системы.

Необходимо строгое разделение функций безопасности, функций системы управления и функций контроля. Если предусматривается совместное использование указанных функций, то функции, не свя-

занные с обеспечением безопасности, не должны влиять на работу функций безопасности. Если компоненты аппаратного и программного обеспечения системы управления производственными процессами используются совместно (например, для функций безопасности и рабочих функций; для функций безопасности с различным уровнем полноты безопасности), то они должны соответствовать требованиям наивысшего уровня полноты безопасности. Устройства безопасности перезагружаются после активации в ручном режиме в случае, если альтернативные действия не прописаны в рамках процедуры оценки риска.

2.2.2 Выбор компонентов защитных устройств

Все компоненты устройств безопасности должны иметь сертификаты уровня полноты безопасности SIL, пройти испытания типа и быть опробованы на практике.

Компоненты, работоспособность которых подтверждена на практике в сравнимых условиях (устройства, прошедшие испытания типа) имеют приоритет перед устройствами, работоспособность которых определена только аналитически (в лабораторных условиях). Сравнимые устройства, используемые для работы, мониторинга и задействования функций безопасности установки, уменьшают число рабочих ошибок, повышают качество технического обслуживания. Так, полевые устройства уже по умолчанию подходят для работы в устройствах обеспечения безопасности с уровнем полноты безопасности SIL 2.

Компоненты указанных устройств могут использоваться только в соответствии с их спецификацией. Требования, оговоренные в руководстве по эксплуатации устройства, должны быть обязательны для выполнения.

Выбранные компоненты и полевые устройства должны выдерживать внешние нагрузки, характерные для места их установки. Они должны обеспечивать требуемую надежность функционирования в заданных условиях и быть просты в обслуживании.

Нижеследующие нагрузки могут снизить функциональные возможности компонентов и полевых устройств. При их эксплуатации рекомендуется принять необходимые меры предосторожности.

К воздействиям внешней среды относятся:

- механические динамические нагрузки (такие как вибрации, сотрясения, удары и т. п.) и статические нагрузки (возникающие, например, под давлением в трубопроводной системе и ведущие к блокировке пусковых механизмов);
- коррозия и прочие химические воздействия;
- засорение отложениями;
- температура и влажность, обусловленные производственным процессом и внешними климатическими условиями;
- электромагнитные нагрузки, обусловленные работой радиоустройств, попаданием молнии, скачками напряжения, отказами системы резервного энергоснабжения и т. п.

К воздействиям, обусловленным производственным процессом, относятся:

- механические нагрузки, например, пульсации, турбулентности, кавитация, внезапное замедление потока жидкости («гидроудар») и т. п.;
- физические и химические воздействия на рабочие материалы, например, коррозия, полимеризация, кристаллизация, твердые отложения, расслоение, конденсация, испарение, изменение физических свойств, таких как вязкость и плотность;
- тепловые нагрузки.

2.2.2.1 Использование компонентов с сертификатом уровня полноты безопасности SIL

а) Использование компонентов с сертификатом уровня полноты безопасности SIL 2

К компонентам устанавливаются следующие требования:

- для устройств безопасности с уровнями полноты безопасности SIL 1 и SIL 2 рекомендуются одноканальные конструкции уровня SIL 2, прошедшие периодические испытания;
- для устройств безопасности с уровнем полноты SIL 3 рекомендуются конструкции с дублирующими элементами уровня SIL 2 (с кодами 1oo2, 2oo3), прошедшие периодические испытания.

Примечание — В устройстве обеспечения безопасности допускается использовать компонент, если изготовитель в письменной форме задекларировал, что аппаратное и программное обеспечение данного компонента соответствуют требованиям ГОСТ Р МЭК 61508 и соответствующему уровню полноты безопасности SIL 2.

Если идентичные компоненты имеют дублирующие элементы, то программное обеспечение должно иметь уровень полноты безопасности SIL 3 и быть опробовано на практике.

Декларация изготовителя, являющаяся частью руководства по эксплуатации, должна содержать следующую информацию:

- тип устройства, версию программного обеспечения, версию аппаратного обеспечения;
- заявление, что данный компонент сконструирован и изготовлен на уровне полноты безопасности SIL 2;
- об интенсивности отказов, определенную в ходе анализа характера и последствий отказов по методике FMEDA (анализа отказов, их последствий и диагностики) для:
  - не выявленных отказов, связанных с обеспечением безопасности;
  - выявленных отказов, связанных с обеспечением безопасности;
  - опасных не выявленных отказов;
  - опасных выявленных отказов;
  - а также для значений, определенных для:
  - доли безопасных отказов (SFF);
  - среднего времени наработки на отказ (MTBF);
  - диагностического покрытия (DC);
  - доля отказов, выявляемых ручной проверкой.

б) Использование компонентов с сертификатом уровня полноты безопасности SIL 3

Если повышение риска оправдано, то в качестве альтернативы конструкции с дублирующими элементами, сертифицированными на соответствие уровню полноты безопасности SIL-2, может быть взята одноканальная конструкция с компонентами, сертифицированными на соответствие уровню полноты безопасности SIL-3. Это имеет смысл, если данные компоненты уменьшают затраты на техническое обслуживание.

Если одноканальных установок в наличии нет, то двухканальные конструкции обычно более предпочтительны. При наличии внутреннего отказа, их компоненты, сертифицированные на соответствие уровню полноты безопасности SIL-3, сразу активируют функции безопасности (например, приводное устройство). Если используется альтернативная конструкция с дублирующими элементами, то при наличии внутреннего отказа в одном канале функция безопасности не активируется. Формируется только сообщение об отказе. Полученные данные могут быть использованы для инициирования мер технического обслуживания без снижения работоспособности установки.

2.2.2.2 Использование компонентов, «проверенных на практике»

Для устройств, имеющих компоненты с качеством «проверено на практике», доказано, что ни отказы аппаратного обеспечения, ни отказы программного обеспечения не снижают работоспособность приборных функций безопасности данных устройств. Так как сбои программного обеспечения — это систематические сбои, то свойство программного обеспечения «проверено на практике» означает: какие-либо систематические сбои, не выявленные в ходе испытаний изготовителя, не отражаются на работе устройств, связанных с обеспечением безопасности. В ходе поиска сбоев рассматриваемые устройства подвергаются различным нагрузкам так, чтобы можно было проверить как можно больше программируемых функций. Свойство аппаратного обеспечения «проверено на практике» означает, что оно существенно зависит от качества соединений элементов производственного процесса (а также свойств материала, рабочих условий и т. п.). Качество указанных соединений внимательно проверяют в первую очередь в каждом индивидуальном случае. Именно пользователь несет ответственность за использование на производстве «проверенных на практике» компонентов.

Документация на установку, содержащую «проверенные на практике» компоненты, должна включать сертификаты проверки всех соответствующих компонентов на практике.

Если компонент «проверен на практике», то его можно использовать в устройстве обеспечения безопасности с учетом нижеследующих требований:

- для устройств безопасности с уровнем полноты безопасности SIL 1 и SIL 2 рекомендуются одноканальные устройства, прошедшие периодические испытания;
- для устройств безопасности с уровнем полноты SIL 3 рекомендуются устройства с запараллеливанием по схеме 1oo2 и 2oo3, прошедшие периодические испытания.

а) Определение свойства «проверено на практике» с помощью изготовителя

Наличие у устройства свойства «проверено на практике» в особых случаях может быть установлено пользователем на основе декларации изготовителя. Декларация изготовителя должна содержать нижеследующую информацию:

- тип устройства, версия программного обеспечения, версия аппаратного обеспечения;
- начало выпуска данной модели (месяц, год);

- утверждение, что никаких систематических пассивных отказов не выявлено и не зарегистрировано в течение указанного времени;

- заявление, что в настоящее время используются, по крайней мере, десять таких устройств. Каждое работает не менее одного года. Их суммарная наработка составляет более 10^5 часов;

- об интенсивности возникновения отказов, определенную в ходе анализа по методике FMEDA, для:

  - не выявленных отказов, связанных с обеспечением безопасности;
  - выявленных отказов, связанных с обеспечением безопасности;
  - опасных не выявленных отказов;
  - опасных выявленных отказов;
  - а также значения нижеследующих величин, определенные по вышеуказанной методике;
  - доли безопасных отказов (SFF);
  - среднего времени наработки на отказ (MTBF);
  - диагностического покрытия (DC);
  - почтовый адрес, электронная почта и т. п., по которому пользователи получают от изготовителя информацию о систематических пассивных сбоях. Гарантийное обязательство предоставлять пользователю, зарегистрированному по данному адресу, всю информацию о систематических пассивных сбоях рассматриваемого устройства.

б) Определение свойства «проверено на практике» с помощью оператора

Оператор может выдать документ в том, что устройство, не имеющее сертификата уровня полноты безопасности SIL и использующееся в установке данного оператора, проверено на практике на основе предшествующего опыта. Данный документ имеет форму самодекларации (декларации оператора). Декларация оператора имеет юридическую силу только для соответствующего компонента той установки, с которой работает данный оператор.

Требованиями к декларации оператора являются (также может быть использован опыт работы других операторов):

- использование в большом количестве проектов в течение длительного времени (например, в десяти различных местах с различными рабочими условиями, наработка каждого устройства не менее одного года);

- наличие статистики отказов данного компонента за весь указанный период;

- документация требований к компоненту, используемому по назначению (технический паспорт изделия, место в контуре автоматического управления и т. п.).

Для дальнейшего использования компонентов с декларацией оператора может потребоваться удовлетворение дополнительных требований и подтверждение необходимых свойств.

2.2.2.3 Дальнейшее использование компонентов в существующих устройствах обеспечения безопасности

Далее рассматриваются:

- частичная модернизация приборной системы безопасности;

- расширение установки за счет дополнительной приборной системы безопасности.

а) Частичная модернизация приборной системы безопасности

При замене индивидуальных компонентов приборной системы безопасности, нужно иметь гарантию, что новые компоненты, по крайней мере, эквивалентны старым с учетом их функциональной безопасности.

б) Расширение установки за счет дополнительной приборной системы безопасности

Если оператор хочет расширить существующую установку за счет приборной системы безопасности, хочет использовать компоненты, ранее использованные в устройствах обеспечения безопасности (например, при наличии запасов, при необходимом уровне подготовки сотрудников и т. п.), то необходимо выполнение нижеследующих требований:

- использование компонентов с качеством «проверено на практике», компонентов с сертификатом уровня полноты безопасности SIL;

- требования к новой приборной системе безопасности и требования к старой системе не должны противоречить друг другу.

2.2.3 Контроль пассивных сбоев

Требования в части контроля пассивных сбоев выводятся исходя из:

1) результатов оценки риска;

2) функциональных спецификаций (например, спецификаций интервалов времени между испытаниями);

3) свойств компонентов.

В одноканальных устройствах обеспечения безопасности пассивный сбой приводит к отказам работы данного устройства. После выявления сбоя (путем диагностики, испытаний, другими средствами) производится ремонт оборудования. Для этого от электропитания отключается либо вся установка, либо ее часть. Могут быть предприняты другие действия (например, организационного характера) для перевода системы в безопасное состояние (удержания системы в безопасном состоянии). Указанные меры (наложенные ограничения) должны уменьшить риск. По крайней мере, значение риска после совершения указанных действий не должно превышать значение риска функционирования данного устройства безопасности до наступления отказа. Все дополнительные меры и наложенные ограничения регистрируются и документируются.

Для многоканальных устройств безопасности, устойчивых к одному сбою, при наличии сбоя производственный процесс можно безопасно продолжать параллельно с ремонтом неисправной части установки. При этом важно соблюдать установленные сроки ремонта. В противном случае, принимаются соответствующие компенсирующие меры (дополнительная информация приведена в разделе 3).

Для приборных систем безопасности установлены специальные технические и организационные меры по предотвращению сбоев и контролю отказов. Главное — это обеспечить высокий уровень доступности к устройствам обеспечения безопасности.

2.2.3.1 Базовые меры и процедуры

- использование отработанной и надежной процедуры установки;
- конструкция приборной системы безопасности должна быть простой и понятной. Влияние отказов на работоспособность системы должно быть ограничено, преимущественно, путем сооружения специальных барьеров на пути их распространения, например, путем:
- установки развязывающих устройств с высоким сопротивлением;
- повышения стойкости к коротким замыканиям;
- установки гальванических развязок и т. п.;
- повсеместного использования принципа «обесточить для аварийного отключения». Необходимо максимально задействовать свойство оборудования работать без сбоев;
- установки предельных значений параметров производственного процесса должны быть защищены от изменений неуполномоченными лицами;
- отклонения параметров производственного процесса от допустимых значений (например, давления сжатого воздуха, используемого в пневматических устройствах, входной мощности электрического тока и т. п.) не должны приводить к отказу приборной системы безопасности. Это достигается путем:
- учета характерных свойств самих устройств;
- резервного электроснабжения путем запараллеливания;
- автоматического мониторинга резервного электроснабжения со световым оповещением и активацией функций безопасности.
- конструкция и порядок применения совместно используемых компонентов приборной системы безопасности и основных систем управления процессами (BPCS-систем) должны соответствовать стандартам приборных систем безопасности. Если в приборную систему безопасности включены пусковые механизмы BPCS-системы, то сигнал активации функции безопасности всегда должен иметь приоритет перед сигналами BPCS-системы и перед сигналами системы контроля производственным процессом;
- приборная система безопасности должна быть независимой от BPCS-системы. В случае отказа BPCS-системы, задействуется функция приборной системы безопасности. Так, инициирующий сигнал приборной системы безопасности может парироваться только в отсутствие паразитной обратной связи в управляющем контуре BPCS-системы;
- если приборная система безопасности имеет дублирующие элементы, то вероятность сбоя (по общей причине) в дублирующем канале должна быть минимальной;
- если технологические соединения приборной системы безопасности имеют барьеры, то состояние их активации легко подавляется. Их необходимо защитить от аварийного закрытия (например, стопорными втулками, цепными блоками, путем удаления маховиков ручной подачи и т. п.);
- автоматический повторный пуск функции безопасности после активации следует дезактивировать. Повторный пуск производится только под контролем и в ручном режиме;
- дополнительные организационные меры, описанные в разделе 3.1.

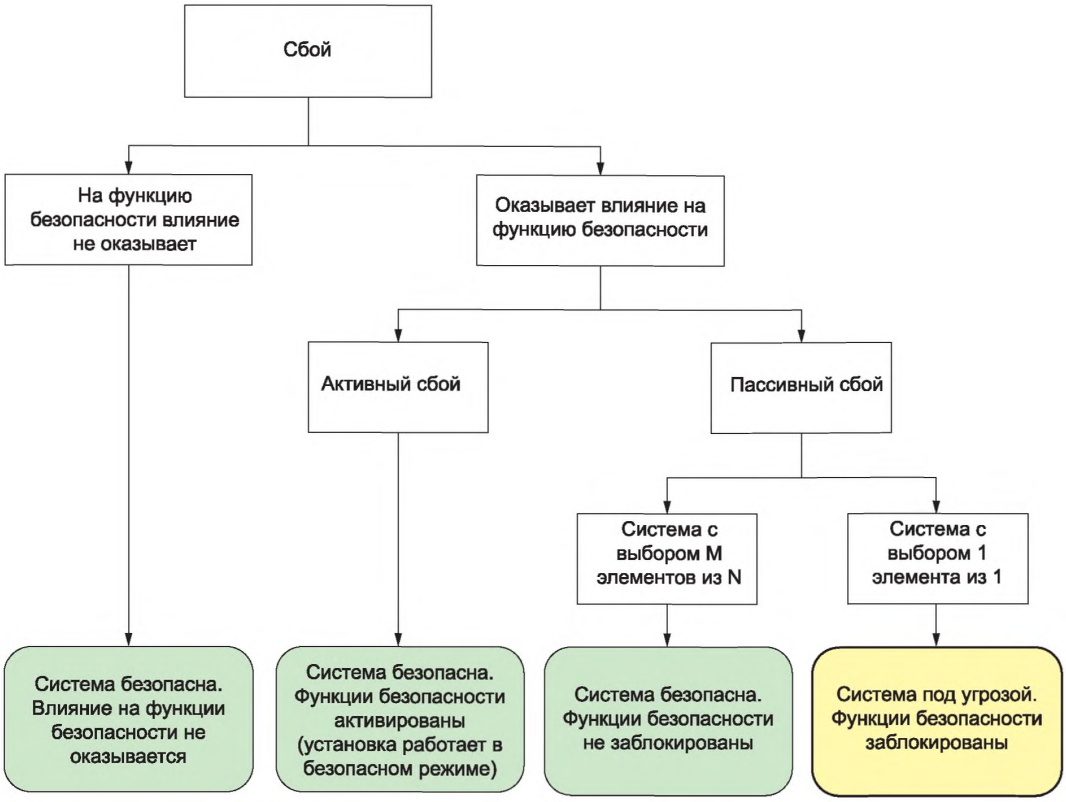

Рисунок 1 — Типы сбоев и их влияние на функции безопасности

2.2.3.2 Дополнительные меры

В дополнение к базовым мерам, могут быть приняты нижеследующие дополнительные меры в зависимости от требуемого уровня полноты безопасности SIL:

- уровень SIL 1 и уровень SIL 2 (пониженный риск).

Одноканальные конструкции приборных систем безопасности, прошедшие периодические испытания. Если рабочие условия являются тяжелыми, и если использование компонентов, связанных с обеспечением безопасности, затруднено, то следует:

- существенно сократить интервал между испытаниями;
- задействовать устройства автоматического мониторинга рабочих функций (например, сторожевой таймер, устройства мониторинга положения, устройства проверки достоверности считываемой информации, устройства пошагового мониторинга, мониторинга времени выполнения операций и т. п.);
- частично запараллеливать устройства, особенно одиночные устройства и модули (особенно датчики).
- уровень SIL 3 (повышенный риск).

Запараллеливание датчиков и пусковых механизмов приборной системы безопасности в контурах типа 1oo2. Повышенную работоспособность установки обеспечивает контур типа 2oo3. В обоих случаях необходимы периодические испытания. Риски оборудования многоканальных конструкций, связанных с обеспечением безопасности, оцениваются в соответствии с частью 4. Введение в рассмотрение переменных для нескольких физически различных производственных процессов, сбор измеренных данных с большого количества физически различных устройств не приводит автоматически к увеличению количества устройств, связанных с обеспечением безопасности (в отличие от конструкций с равномерным распределением дублирующих элементов). Запараллеливание физически различных устройств — это дополнительная мера контроля возможных систематических сбоев. Данная мера уменьшает вероят-

ность того, что сразу несколько каналов дублированной системы откажут одновременно (вследствие наступления систематического сбоя). Использование конструкций без дублирующих элементов допустимо только в случае, если их компоненты имеют сертификаты уровня полноты безопасности SIL 3.

2.2.4 Интерфейс устройства безопасности

На данный интерфейс устройства выводится нижеследующая информация:

- фактические значения переменных производственного процесса;
- индикация активации функций безопасности;
- статус датчиков и пусковых механизмов (например, выполнение требований технического обслуживания);
- результаты работы диагностических функций сравнения (если данные функции предусмотрены законодательством, то вывод результатов на экран является обязательным);
- отказ установки, вызванный изменением рабочих условий. Обеспечение надлежащих рабочих условий — важный фактор функционирования устройств безопасности (например, неисправность кондиционера воздуха в диспетчерской).

2.2.4.1 Устройства безопасности с функцией переключения

До оператора должна быть доведена нижеследующая информация о функции безопасности:

- функция обеспечивает индикацию того, что устройство безопасности управляется вручную при выключенной автоматике;
- функция обеспечивает сигнал тревоги при аварийном отключении питания, если это снижает безопасность (например, при использовании принципа «обесточить для аварийного отключения»).

2.2.4.2 Устройство безопасности без функции переключения

В данном случае, реакция оператора — это часть устройства безопасности, указываемая в рабочей инструкции. Функция аварийной сигнализации (аварийный сигнал тревоги может быть акустическим или визуальным) должна соответствовать установленным требованиям безопасности. Аварийный сигнал должен резко отличаться от других рабочих сигналов.

2.2.4.3 Устройство безопасности без датчиков

В данном случае, способность оператора воспринимать опасность и реакция оператора — это части устройства безопасности, указываемые в рабочей инструкции. Все действия устройства (в том числе удаленная активация пускового механизма) должны соответствовать установленным требованиям безопасности.

2.2.5 Требования к техническому обслуживанию и к испытательным устройствам

Конструкция устройства безопасности обеспечивает испытания как всей цепи (от датчика до пускового устройства приводного механизма), так и отдельных агрегатов. Если интервалы между плановыми отключениями установки превышают интервалы между плановыми испытаниями, то необходимо иметь возможность испытывать устройство в ходе его функционирования.

Если испытание установки проводится в ходе ее функционирования, то отдельные агрегаты (например, перемычки, байпасные устройства и т. п.) проверяются на наличие пассивных отказов как части устройства безопасности.

Если устройство безопасности содержит испытательные устройства (устройства тестирования), а также устройства управления с блокировкой автоматики, то они должны удовлетворять нижеследующим требованиям:

- оператор получает сообщения о каждом факте блокировки автоматики в отдельных агрегатах устройства безопасности. Процедура блокировки автоматики определяется рабочей инструкцией (например, блокировки открыто защищенного клапана обводного контура и т. п.);
- принудительное перенастраивание входных и выходных характеристик программируемого логического контроллера PLC системы безопасности производится в соответствии с разделом 3.

2.2.6 Вероятность возникновения отказа устройства безопасности

Вероятность возникновения отказа каждого устройства безопасности не должна превышать вероятность возникновения отказа, установленную соответствующим уровнем полноты безопасности SIL.

Если используются компоненты, сертифицированные на соответствие уровню полноты безопасности SIL 3, то их степень соответствия подтверждается вычислениями с учетом наличия запараллеленных структур и установленных интервалов между испытаниями.

«Проверенные на практике» компоненты используются в соответствии с разделом 2.2.2.2.

2.2.7 Документация и маркировка

Документация должна содержать необходимую информацию о конструкции, о взаимодействии различных установок, о дизайне и планировке оборудования в трехмерном пространстве (3D).

Все основные компоненты приборной системы безопасности маркируются в документации как компоненты приборной системы безопасности, расположенные в как в автоматном зале, так и в диспетчерской. Приборные системы безопасности идентифицируются обозначением (меткой) производственного процесса:

- для функций переключения, следует использовать символ «Z» вместо символа «S»;
- для датчиков без функций переключения, сообщения, соответствующие установленным требованиям безопасности, помечаются символом (Z) (например, QR(Z)A+);
- для приборных систем безопасности, функция пускового устройства приводного механизма также маркируется символом (Z) (например, UV(Z) и т. п.).

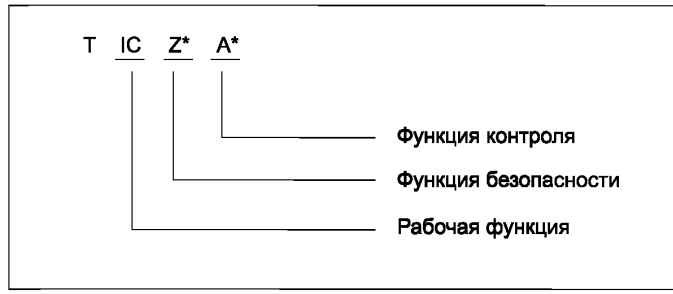

Рисунок 2 — Пример обозначения (метки) производственного процесса (метка измерения температуры процесса)

2.3 Установка и ввод в эксплуатацию устройств безопасности

Планирование установки и ввода в эксплуатацию устройств — это часть общего плана обеспечения безопасности предприятия (его системы менеджмента). Данный план должен включать:

- мероприятия по установке и вводу в эксплуатацию;
- процедуры, принимаемые меры и методы установки и ввода в эксплуатацию;
- календарный план проведения указанных мероприятий;
- назначение ответственных путем выдвижения кандидатов из числа физических лиц, подразделений предприятия и смежных организаций.

Все компоненты устройств безопасности устанавливаются в соответствии с вышеуказанным планом.

Крайне полезно производить сборку и установку в несколько шагов. Каждый шаг должен проверяться.

Первичное тестирование гарантирует, что устройство безопасности работает корректно и может быть введено в эксплуатацию. Первичные требования определяются инструкцией по проведению испытаний. Данная инструкция разрабатывается для каждого устройства безопасности (см. раздел 2.4).

Обязательно должна проводиться регистрация надлежащей установки устройств безопасности и ввода их в эксплуатацию. Если выявляется отказ, то документируются его причины.

Если существующая установка не соответствует проекту, то выявленные отклонения оцениваются компетентным специалистом. Оценивается влияние последствий сбоя на безопасность. Если указанные отклонения не влекут опасных последствий, то проектная документация корректируются и в них отражается новое состояние установки. Если же указанные отклонения влекут опасные последствия, то проект устройства безопасности переделывается. Для нового проекта обязательно выполняется новая оценка безопасности.

2.4 Тестирование устройств безопасности

Первичные испытания должны подтвердить, что рассматриваемые устройства безопасности корректно установлены и введены в эксплуатацию. При этом ассоциированные функции безопасности удовлетворяют требованиям всех стандартов, указанных в спецификации безопасности.

Проектные функции устройств безопасности подтверждаются путем регулярного повторного тестирования. Это способствует своевременному обнаружению и устранению пассивных сбоев.

Все мероприятия, необходимые для организации испытаний, специально планируются. Инструкции по проведению испытаний разрабатываются для каждого устройства безопасности. Данные инструкции необходимы для проведения первичных испытаний устройств при вводе их в эксплуатацию.

2.4.1 Содержание инструкции по проведению испытаний

Инструкция по проведению испытаний должна включать:

- определение интервалов между повторными испытаниями (см. разделы 2.1.2 и 2.5);
- определение испытаний всех соответствующих рабочих режимов производственного процесса и всех рабочих режимов соответствующих установок. В том числе:
- режимы функционирования, задания настроек, калибровки;
- режимы запуска, режимы автоматического, полуавтоматического и ручного управления, работа в стационарном режиме;
- перезагрузку, отключение, техническое обслуживание;
- обработку предсказуемых неисправностей;
- выбор метода испытаний (например, испытания всей системы, визуальный осмотр, моделирование, пробный пуск и т. п.);
- оформление испытательной документации:
- обозначение объекта испытаний;
- отчет об испытаниях (при наличии отказов, в отчете указывают подробности события, подтверждение устранения неисправности, особенности повторного пуска);
- дата испытаний;
- подпись инспектора (начальника подразделения);
- подпись оператора технологической установки.

Проверка пользовательской программы должна включать в себя:

- идентификатор программы, проверяемой перед вводом в эксплуатацию каждого рабочего режима установки. Проверяются все ее параметризуемые компоненты;
- корректность назначения каналов входа/выхода, их сигнальный диапазон;
- время отклика;
- диапазон измерений, допуски на измеренные значения.

2.4.2 Объекты проверки

К объектам проверки относятся:

- корректность калибровки всех измерительных инструментов;
- соответствие документации на производственный процесс фактическому состоянию оборудования;
- организационные мероприятия (например, обеспечение оборудования персоналом, процедура приведения оборудования в рабочее состояние и т. п.).

2.4.3 Тестирование оборудования

При проведении тестирования оборудования необходимо ответить на следующие вопросы:

- Соответствуют ли показатели устройства безопасности, работающего в штатном или специальном режиме (например, в режиме пуска, в режиме отключения и т. п.) требованиям спецификации безопасности?
- Имеются ли паразитные обратные связи системы управления производственным процессом (системы мониторинга) с устройствами обеспечения безопасности?
- Корректно ли работают каналы связи системы управления производственным процессом (системы мониторинга) с устройствами обеспечения безопасности?
- Соответствуют ли режимы работы функций логического обеспечения установки (например, режим 1oo2, режим 2oo3 и т. п.) требованиям спецификации безопасности?
- Корректна ли работа функций безопасности при выходе измеренных значений за пределы установленного диапазона?
- Корректно ли работает измерительная система (например, калибровка измерительной системы, возможность проведения сравнительных измерений, возможность выявления тренда и т. п.) при отказах системы сбора данных (постепенные отказы, переходы устройства в неизменяемое состояние, циклические отказы и т. п.)?
- Корректна ли последовательность активации функций переключения?
- Корректен ли вывод на экран (устройства безопасности) рабочих сообщений, информации о режиме функционирования?

- Соответствует ли процедура перезагрузки функций устройства безопасности требованиям спецификации безопасности?
- Корректно ли работает система управления с блокировкой автоматики? Блокируется ли режим активации системы в случае отказа (см. раздел 2.2.5)?
- Корректно ли работает механизм ручного отключения устройства?
- Соответствует ли работа диагностических устройств установленным требованиям?
- Корректно ли работают устройства безопасности в случае аварийного отключения питания? Возвращается ли система (после возобновления энергоснабжения) в рабочее состояние автоматически, или оператор делает это вручную?

2.4.4 Документирование результатов испытаний

Все результаты испытаний устройств безопасности должны тщательно документироваться.

2.5 Переход к гибким интервалам проверок приборных систем безопасности

Функции, тестирующие приборные системы безопасности, выявляют пассивные, т. е. наиболее опасные сбои, нарушающие их корректную работу. До настоящего момента максимальный интервал между испытаниями устройств безопасности составляет один год.

Вместе с тем, отдельные рабочие функции требуют дополнительных испытаний. Дополнительные испытания рабочих функций могут привести к ухудшению качества выпускаемой продукции, так как данные испытания часто требуют остановки технологического процесса. Увеличение объема испытаний должно производиться в строгом соответствии с планом выпуска продукции и планом загрузки оборудования.

Примечание — Действующие ГОСТ Р МЭК 61511 и ГОСТ Р МЭК 61508 обеспечивают возможность сделать интервалы между испытаниями гибкими без снижения надежности функционирования приборной системы безопасности.

План испытаний можно адаптировать к ситуации путем:

- пересмотра системы управления испытаниями, оптимальной интеграции испытаний в производственный процесс, использования рабочих прерываний производства продукции;
- оценки оптимального интервала между испытаниями (для конкретных компонентов устройства безопасности) индивидуальными методами диагностического покрытия на основе накопленного опыта работы;
- обновления существующего устройства безопасности, чтобы получить «целевое значение» интервала между испытаниями. Целевое значение может быть заложено в план работы оборудования.

Для заданной конструкции устройства безопасности, можно составить перечень всех возможных сбоев (fault list)». В перечне сбоев учитывается каждый компонент устройства безопасности (датчики, устройства обработки сигналов, пусковые устройства приводных механизмов и т. п.). Составление перечня сбоев является начальной точкой для последующего анализа.

Перечень сбоев фокусируется на признаках возникновения сбоев и причинах сбоев. Например, систематическая погрешность измеренного значения — это симптом сбоя. Причинами сбоев могут быть налипание материала на поверхность чувствительного элемента датчика или отказ электронного устройства.

По симптому сбоя можно определить, является ли данный сбой активным или пассивным. Сюда включается оценка вероятности рассматриваемого события, полученная на основании данных изготовителя, накопленного опыта.

Все выявленные сбои сортируются по вероятности их наступления. Это позволяет правильно спланировать работу: на сбои высокой вероятности тратится сил больше, чем на сбои маловероятные.

Каждый сбой тщательно изучается. Учитывается возможность его выявления и предотвращения:

- предотвращаемые сбои:
  - сбои, не оказывающие влияния на работу функций безопасности,
  - активные сбои;
- выявление пассивных, диагностируемых сбоев;
- выявление пассивных, не диагностируемых сбоев путем тестирования рабочих функций.

После этого, уточняется нормативный интервал времени между испытаниями. Для больших интервалов между испытаниями следует увеличить степень запараллеливания производственного процесса, уровень его диагностики. После внесения изменений в производственный процесс, интервал между испытаниями повторно уточняется.

3 Эксплуатация устройств безопасности

В ходе функционирования производственных установок, устройство безопасности должно управляться и поддерживаться так, чтобы вероятность возникновения отказа не превышала величины, соответствующей уровню SIL.

Для выполнения указанного требования, важно уметь быстро предотвращать отказы, приводящие к сбоям, быстро выявлять и устранять сбои, возникающие в устройствах обеспечения безопасности. Необходимо принятие нижеследующих мер:

- контроль производственного процесса операторами и инженерами;
- проверки (тестирование рабочих функций, визуальный осмотр);
- плановое техническое обслуживание;
- корректирующее техническое обслуживание.

3.1 Определения, связанные с организацией работ

В рамках системы менеджмента безопасности предприятия должны быть назначены физические лица и подразделения предприятия, ответственные за проведение мероприятий, связанных с устройствами безопасности. Должны быть также назначены ответственные за работу самих устройств безопасности. Все работы на устройствах обеспечения безопасности, оказывающие влияние на производственный процесс, проводятся на основании письменных разрешений, выданных ответственными за данные работы. В данных разрешениях (см. 3.3.2.1) указывается, что данные работы проводятся на устройствах обеспечения безопасности. При необходимости, для обеспечения безопасности принимаются дополнительные меры.

Обслуживание устройств безопасности в ходе функционирования технологической установки производится на основании руководящих документов. В данных документах устанавливаются:

- функциональные мероприятия, проводимые:
  - в ходе штатного функционирования,
  - в ходе специальных режимов работы;
- коммуникации между рабочим персоналом и персоналом технического обслуживания систем управления производственным процессом;
- мероприятия технического обслуживания.

Рабочий персонал должен быть специально обучен и должен понимать важность и цели функционирования устройств безопасности. Рабочий персонал должен уметь управлять технологическим процессом в ручном режиме (например, в режиме управления с блокировкой автоматики). В специальных случаях, может оказаться полезным повышение квалификации на рабочем месте через установленные интервалы времени путем моделирования аварийных ситуаций.

Устройства с ручным управлением, позволяющие отключать функции безопасности (например, отсечные клапаны, расположенные (по потоку) выше датчиков давления), должны быть защищены от постороннего вмешательства.

Работы, выполняемые на устройствах обеспечения безопасности, требуют координации между рабочим персоналом и персоналом технического обслуживания. Диспетчер должен иметь полную картину происходящего. Он всегда должен быть готов принять решительные меры и не может быть застигнут врасплох внезапной активацией функции безопасности. Необходимо принять все возможные меры предосторожности: телефоны, Интернет, оборудование связи и т. п. должны быть всегда легкодоступны. Все сотрудники должны находиться на связи, должны координировать свою работу даже на большом удалении от центральной диспетчерской и диспетчера технологической установки.

Техническое обслуживание выполняется только обученными специалистами системы управления производственным процессом. Все возможные исключения (например, для повторной заливки раствора реагента, запуска устройства анализа характеристик производственного процесса и т. п.) подтверждаются разрешениями в письменной форме.

3.2 Функциональное обслуживание устройств безопасности

Отслеживание переменных производственного процесса и проверка их измеренных значений на достоверность позволяют обученному рабочему персоналу выявлять неисправности устройств безопасности (с учетом случайного разброса результатов измерений) и инициировать их устранение.

Предельные значения характеристик приборных систем безопасности могут изменяться только по письменному запросу оператора. В запросе оператор указывает, как данное изменение влияет на результаты оценки безопасности.

Работы по внесению изменений указанных предельных значений (время внесения изменений, инициатор изменений, исполнитель работ) документируются. Вносимые новые настройки предельных значений характеристик верифицируются путем испытаний. Соответствующая спецификация испытаний должна быть пересмотрена.

В случае кратковременного отключения устройств безопасности, должны действовать нижеследующие правила:

- повторный ввод установки в эксплуатацию производится только после активации функции безопасности. Автоматический повторный запуск устройства после активации функции безопасности в ответ на возмущение производственного процесса должен быть предотвращен. Повторный запуск отдельных агрегатов установки производится вручную. Это можно сделать только после возвращения всей установки в безопасное состояние. То же самое относится к ситуации, когда сама функция безопасности включается в ответ на активный сбой оборудования (см. 3.3.2.2);

- режим отключения, режим кратковременного управления с блокировкой автоматики. Если невозможно избежать временного отключения оборудования (кратковременного режима управления приборной системы безопасности с блокировкой автоматики), то данное вмешательство должно быть задокументировано. Безопасность должна обеспечиваться в течение всего времени отключения (управления с блокировкой автоматики) с помощью вспомогательных технических (организационных) мер. Режим отключения (управления с блокировкой автоматики) должен четко идентифицироваться на экране. Если управление с блокировкой автоматики производится с помощью функции переключения (например, путем внешнего воздействия, с помощью переключателя с ключом и т. п.), то это должно четко идентифицироваться на экране в течение всего периода управления. Прямые вмешательства оператора во входные (выходные) параметры (операции на терминалах, установка проволочных перемычек и т. п.) должны быть по возможности запрещены. Повторные вмешательства оператора производятся на основе особых технических решений.

Если ввод установки в эксплуатацию производится повторно, то рабочие функции можно уже не тестировать, если это не оговорено специально процедурой технического обслуживания (например, процедурой калибровки) данной установки.

3.3 Техническое обслуживание устройств безопасности

Меры технического обслуживания обеспечивают устойчивую работу устройств безопасности в течение всего жизненного цикла.

3.3.1 Квалификация персонала

Персонал, выполняющий техническое обслуживание систем управления производственным процессом должен отвечать за проведение проверок и обладать следующими знаниями и квалификацией:

- знание измерительных инструментов и устройств автоматического регулирования и управления, знание как электротехнических, так и не электротехнических средств обеспечения взрывобезопасности установок;

- знание организационных правил технического обслуживания устройств безопасности;

- знание технических особенностей устройств безопасности (например, мероприятий по обеспечению работы без сбоев, способов запараллеливания агрегатов и т. п.);

- знание принципа работы используемых устройств (например, принципа работы программируемого логического контроллера PLC системы безопасности и т. п.).

Крайне желательно знание особенностей взаимодействия технологических установок в целом и особенностей взаимодействия их отдельных агрегатов.

3.3.2 Организация технического обслуживания

Все операции технического обслуживания устройств безопасности должны выполняться в соответствии с утвержденным планом. Это относится не только к регулярным испытаниям и регламентированному техническому обслуживанию, но также и к корректирующему техническому обслуживанию.

3.3.2.1 Тестирование и техническое обслуживание

а) Общие положения

Если необходимое тестирование и техническое обслуживание не были определены на этапе планирования работ, то ответственные специалисты и операторы системы управления производственным процессом должны задать требования к процедуре испытаний и к мерам технического обслуживания:

- требования высшего порядка, применимые не только к устройствам обеспечения безопасности (например, общие требования регулировки измерительных инструментов и т. п.);
- инструкции по испытаниям специальных устройств безопасности;
- сроки проведения испытаний.

б) Приведение установки в рабочее состояние

Необходимо установить правила, регламентирующие условия выполнения испытаний. Проведение испытаний обычно требует вмешательства оператора в работу устройств безопасности. Данное вмешательство временно деактивирует функции безопасности. На указанный период может потребоваться принятие дополнительных мер.

Вмешательство оператора производится на основании письменного указания, которое должно включать нижеследующую минимальную информацию:
- обозначение обслуживаемого устройства безопасности;
- краткое описание принимаемых штатных мер;
- описание дополнительных мер;
- имя руководителя, давшего разрешение на проведение работ;
- сроки начала и окончания работ.

в) Процедура испытаний

Процедура испытаний определяется инструкцией по проведению испытаний. Данная инструкция может содержать либо общие указания, либо конкретные указания для конкретной контрольной точки (измерений). Если инструкция по проведению испытаний не соответствует сложившейся ситуации (это часто бывает на начальном этапе работ), то данная инструкция перерабатывается с учетом конкретных условий работы установки. При этом учитываются конкретные требования используемой промышленной технологии и особенности ее практической реализации.

Результаты испытаний обязательно должны документироваться. Форма документации должна соответствовать установленным требованиям. Если в ходе испытаний выявляется сбой, то в документы немедленно должны вноситься изменения, и сбой и принятые меры должны регистрироваться (см. 3.3.4).

При определенных обстоятельствах может оказаться полезным испытывать не все устройство безопасности целиком, а только отдельные его агрегаты. Такие испытания могут выполняться в разное время, они имеют разную продолжительность. Необходимо убедиться, что ни один компонент установки не пропущен и все интерфейсы компонентов функционируют корректно.

Инструкции по проведению испытаний должны содержать:
- обозначения проверяемых устройств безопасности, в том числе назначенные уровни SIL;
- обозначения компонентов;
- принимаемые меры по контролю режима отключения и повторного ввода устройства в эксплуатацию;
- данные изготовителя и данные модели рассматриваемого компонента (спецификацию изготовителя);
- диапазон измерения и предельные значения характеристик;
- перекрестные ссылки на документацию контрольной точки измерений (например, графики рабочих функций);
- информацию по запараллеливанию (разветвлениям технологического процесса);
- данные, связанные с обеспечением безопасности (например, значение характеристики K_V элементов пускового устройства приводного механизма);
- специальные требования (например, время наступления конкретного события, степень герметичности элементов приводного механизма и т. п.);
- инструкции для работника проводящего испытания;
- контактные данные автора инструкции.

Желательно привести ссылку на общие правила проведения испытаний.

г) Сроки проведения испытаний

Сроки испытаний рабочих функций определяются требованиями уровня полноты безопасности SIL. Оператор должен гарантировать, что все рабочие функции испытываются в соответствии с планом испытаний. Персонал технического обслуживания системы управления производственным процессом должен быть проинформирован о сроках проведения указанных испытаний.

Сроки выполнения технического обслуживания установки определяются так, чтобы обеспечить необходимый запас ее безопасности по истечении срока годности отдельных агрегатов (например, для

устройств контроля производственного процесса: время замены фильтра, время пополнения запаса раствора химического катализатора и т. п.). Кроме того, испытания проводятся после продолжительных отключений оборудования, после корректирующего технического обслуживания устройств безопасности.

3.3.2.2 Корректирующее техническое обслуживание

Для выполнения немедленного корректирующего технического обслуживания устройств безопасности с дефектами нужно создать определенные условия. Прежде всего, необходимо обеспечить доступ к:

- рабочей документации на устройства безопасности;
- описаниям оборудования и руководствам по эксплуатации его компонентов;
- необходимым запчастям.

Любые возникающие сбои устраняются немедленно после их выявления. После устранения сбоя должны проводиться испытания. Они подтверждают корректность рабочей функции устройства безопасности. Все прочие устройства безопасности, охватываемые рассматриваемым отказом (например, многоканальные входные модули программируемого логического контроллера PLC системы безопасности и т. п.), также должны тестироваться. Сбой, принятые меры и причины сбоя (если они известны) обязательно должны документироваться. Запчасти устройств безопасности складируются в соответствии с принятой концепцией материально-технического обеспечения производства. Важно учитывать, что компоненты устройств безопасности задействуются достаточно редко. Несмотря на это, для обеспечения работоспособности установки, необходимо создать достаточный запас запчастей указанных редко используемых компонентов.

3.3.3 Практические рекомендации по испытанию рабочих функций установки

Испытания рабочих функций позволяют выявить пассивные сбои. Данные испытания выполняются в соответствии с инструкциями по проведению испытаний. Они выполняются в условиях, максимально приближенных к реальным. Испытания устройства безопасности должны всегда охватывать всю установку полностью: от датчика до контроллера и приводного механизма (включая агрегаты, контактирующие с продуктом производства). Функции безопасности активируются преимущественно самим производственным процессом. Если такая активация при тестировании невозможна, то устройства запускаются путем изменения переменных производственного процесса.

Отдельные компоненты можно испытывать индивидуально. Для них определяются специальные циклы испытаний. Испытания должны гарантировать, что все устройство безопасности функционирует в соответствии с установленными требованиями.

Испытания рабочих функций производятся регулярно в соответствии с инструкциями по проведению испытаний, разработанными отделом технического обслуживания в кооперации с операторами технологической установки. Такая кооперация является крайне важной.

Сбои, выявленные в ходе тестирования установки, должны устраняться немедленно.

3.3.3.1 Компоненты датчиков и устройств возбуждения установки

Чувствительные (воспринимающие) элементы должны устанавливаться непосредственно на рабочие агрегаты технологической установки. Поэтому в ряде случаев доступ к ним может быть затруднен.

а) Тестирование аналоговых датчиков

Прежде всего, необходимо удостовериться, что чувствительный элемент передает измеренные значения корректно, в установленном допуске. Это можно отрегулировать путем подстройки измеряемых переменных производственного процесса. Датчики давления, например, можно отрегулировать, прикладывая заранее известное давление. Процедура регулировки может быть выполнена либо самими испытательными устройствами независимо, либо в ходе технологического процесса путем независимых измерений. Диапазон измерения датчика сравнивается с нормативным диапазоном по трем контрольным точкам. Точку переключения располагают ближе к середине интервала. Она не должна находиться в окрестности границы диапазона измерения.

При определенных обстоятельствах целесообразно проводить мониторинг сразу по двум измеренным значениям. Следует учитывать, что данное решение делает процедуру мониторинга более трудоемкой. Следует убедиться в том, что значение, измеренное с учетом наложенных допусков, корректно воспринимается и другими электронными устройствами управляющего контура (датчиками предельного значения, входными аналоговыми устройствами и т. п.).

б) Испытания датчиков предельного значения

Изменение состояния датчика предельного значения производится в установленном допуске в заданной точке переключения. Испытания датчика предельного значения с измененной настройкой предела производятся только в исключительных случаях. Изменение предела означает, что не все потенциальные сбои рассматриваемого компонента могут быть выявлены. Обязательно предусматривается возможность восстановления старой настройки датчика для исходного предельного значения.

в) Испытания бинарных датчиков

Для бинарного датчика обязательно проверяются режимы приема и передачи соответствующего бинарного сигнала.

г) Испытание устройств с μ-процессорами

Обязательно проверяется соответствие значений параметров установки, связанной с обеспечением безопасности, требованиям документации на данную установку. Также проверяется эффективность защиты настроек данного устройства от несанкционированного изменения. Если данная проверка требует вмешательства оператора устройств, то это должно быть оговорено в специальной инструкции. После проверки установка должна быть возвращена в исходное состояние. Нужно гарантировать, что конфигурация и значения настроек установки не могут быть изменены не санкционированно. Все изменения настроек технологического оборудования регистрируются в сопроводительной документации.

Исключением являются испытания устройств подачи тестовых воздействий в ходе функционирования установки.

Перед началом испытания датчика необходимо принять меры по предотвращению активации функции переключения (см. 2.2.5). Если заодно тестируются и логические устройства, то нужно гарантировать, что функция переключения активируется только самим тестируемым каналом (а не каналом, его дублирующим).

3.3.3.2 Обработка сигнала

В принципе, проверяются и функции логических переменных. Это означает, что результат преобразования входного значения в выходное значение является воспроизводимым. Для функций памяти (например, для кодовых замков), нужно иметь в виду, что выходной сигнал зависит не только от входного сигнала, но и от некоторого предварительно заданного состояния. У таймеров проверяется их работоспособность, точность хода и время отклика.

При периодических испытаниях приборных систем безопасности, проверяются интеллектуальные прогнозные датчики технологической линии (SPLC). Это обеспечивает соответствие аппаратного и программного обеспечения установки заданному уровню безопасности.

3.3.3.3 Включающий компонент (триггер)

Если используется специальный включающий компонент (триггер), то необходимо проверить цепь передачи сигнала от контроллера до пускового устройства приводного механизма. Проверяется также возможность остановки потока материала (энергии) в технологической установке.

Критерии оценки работоспособности пускового устройства приводного механизма:

- работа электромагнитного клапана;
- возможность перевода установки в безопасное состояние в рабочих условиях;
- обеспечение максимально (минимально) допустимого времени срабатывания пускового устройства;
- соответствие спецификации безопасного состояния и рабочего состояния оборудования (в части герметичности, конфигурации и т. п.), соответствие оценке безопасности конкретного приложения;
- работоспособность электрических пусковых механизмов (контакторов, автоматов защиты цепи и т. п.).

В некоторых обстоятельствах, можно оценивать работоспособность пусковых устройств приводных механизмов с помощью ассоциированных переменных производственного процесса (например, с помощью расходомера можно оценить угол раскрытия клапана).

Если правильно выбран метод оценки сигнала, если дублирующие компоненты можно испытывать независимо друг от друга, то указанные дублирующие компоненты можно испытывать без остановки технологического процесса, без оказания паразитного воздействия на устройства безопасности. Каждую рабочую (штатную) активацию пускового устройства приводного механизма можно рассматривать как испытание. Все результаты испытаний должны документироваться.

3.3.4 Документирование мер технического обслуживания

Все операции технического обслуживания устройств безопасности должны документироваться. Это позволяет отслеживать технологический процесс, получать необходимую информацию о надежности устройств безопасности. Данные должны храниться не менее 5 лет.

3.3.4.1 Документирование испытаний

Каждое испытание должно документироваться. Минимально допустимая информация для документирования включает в себя:

- обозначение тестируемого объекта;
- результаты испытаний (в случае сбоя, регистрируются особенности данного сбоя, подтверждается факт его устранения, факт корректного повторного пуска);
- дата проведения испытаний;
- подпись инспектора (начальника подразделения);
- подпись оператора технологической установки.

Информация об устраненном сбое должна содержать характеристику сбоя: пассивный или активный сбой. Подписи инспектора и оператора установки подтверждают передачу (приемку) работоспособного устройства безопасности.

3.3.4.2 Оценка результатов испытаний

Для повышения надежности устройств безопасности, необходимо тщательно проанализировать устраненный сбой. Непрерывная регистрация результатов испытаний — эффективное средство выявления слабых мест установки. Если один и тот же сбой происходит повторно, — это слабое место установки. Оно известно, и можно уменьшить интервал времени между испытаниями. Отсутствие сбоев — важный аргумент за увеличение интервала времени между испытаниями, за упрощение конфигурации устройства безопасности.

3.3.4.3 Документирование корректирующего технического обслуживания

Процедура документирования корректирующего технического обслуживания аналогична процедуре документирования испытаний. Принятые меры корректирующего технического обслуживания регистрируются на специальном бланке. Данный документ должен содержать полный перечень всех принятых мер корректирующего технического обслуживания установки. Для корректирующего технического обслуживания используется только специально приспособленное оборудование. Если для корректирующего технического обслуживания используется стороннее неучтенное оборудование, то его надо модифицировать, приспособить и освидетельствовать для выполнения работ на устройствах обеспечения безопасности.

3.4 Модификация устройств безопасности

Модификации устройств безопасности накапливают риск наступления непреднамеренных и внезапных систематических сбоев, препятствующих штатному функционированию технологического оборудования и функционированию устройств безопасности. Риски сбоев следует учитывать при проектировании, при планировании работы, при вводе в эксплуатацию устройств безопасности (см. раздел 2). Рабочий персонал, персонал технического обслуживания и руководители предприятия должны быть в курсе проводимой модификации. Они должны организовать обучение персонала для работы на модифицированном оборудовании.

3.4.1 Оптимизация устройств безопасности

На этапе планирования устройств безопасности, как правило, не хватает опыта управления технологическим процессом в новых производственных (экологических) условиях. Если производственный опыт, накопленный при вводе устройств безопасности в эксплуатацию, указывает на слабые места установки, на потенциал ее совершенствования, если уже появились более современные устройства (например, с повышенной точностью измерений), и они успешно прошли полевые испытания, то может оказаться целесообразным модифицировать имеющиеся устройства безопасности, обновить их рабочие функции и повысить надежность. За принятие решения о модификации обычно отвечают ведущие специалисты системы управления производственным процессом. Данные физические лица должны грамотно оценить дополнительные риски, вносимые модификацией устройств безопасности. Они должны доказать отсутствие паразитных обратных связей с другими устройствами обеспечения безопасности. Если модифицируется программируемый логический контроллер PLC системы безопасности, то нужно обосновать:

1) возможность непрерывной работы технологической линии при загрузке модифицированной программы пользователя (модификация типа «on-line»);

2) необходимость остановки технологической линии во время модификации контроллера. Модификация типа «on-line» выполняется только в соответствии со специальной инструкцией изготовителя после детальной оценки влияния модификации на работоспособность системы.

Ведущие специалисты системы управления производственным процессом отвечают прежде всего за надлежащее планирование и установку оборудования. Они также отвечают за испытания начальной стадии, выполняемые независимыми органами перед вводом установки в эксплуатацию. В случае модификации вся техническая документация на обновленные устройства безопасности и инструкции по проведению испытаний приводятся в соответствие установленным требованиям.

3.4.2 Адаптация модифицированного производственного процесса

Если производственный процесс претерпел изменения, то оценки безопасности и результаты анализа рисков пересматриваются и адаптируются к новым условиям. Для некоторых устройств безопасности результатами практической реализации пересмотренной концепции безопасности могут быть новое производственное задание, обновленные требования надежности и обеспечения безопасности. Процедуры планирования, установки и ввода в эксплуатацию адаптируемых систем должны совпадать с процедурами планирования, установки и ввода в эксплуатацию новых систем.

Изменения в определении производственных заданий устройств безопасности часто ассоциируются с модификацией устройств обработки сигналов. Модификация устройств обработки сигналов должна проводиться осторожно и осмотрительно. Важно учесть все аспекты модификации, особенно при модификации систем с устройствами связи повышенной сложности.

3.4.3 Вывод из эксплуатации устройств безопасности

Если производственная установка выводится из эксплуатации, то новые производственные задания для устройств безопасности являются следствием оценок безопасности вывода из эксплуатации. Другие требования здесь не рассматриваются.

Если выводятся из эксплуатации индивидуальные устройства безопасности (в результате оценки безопасности функционирования), то их процедуру обработки сигналов следует адаптировать к новой ситуации. Работа устройств безопасности в части обработки сигналов, выведенных из эксплуатации устройств безопасности, должна испытываться повторно.

Документация на установку должна обновляться по мере происходящих изменений. В ней должны документироваться данные о выводе установки из эксплуатации и разборе отдельных устройств безопасности. Если устройство безопасности продолжает работать, то частично должна изменяться его маркировка. Это отражается в технической документации.

Повторный ввод в эксплуатацию устройств безопасности, ранее выведенных из эксплуатации, требует полного испытания всех рабочих функций.

УДК 658.52.011.56:006.354 ОКС 25.040.40

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

БЗ 10—2019/142

Редактор *П.К. Одинцов*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 24.09.2019. Подписано в печать 15.10.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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