МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO 13849-2— 2023

Безопасность оборудования

ЭЛЕМЕНТЫ СИСТЕМ УПРАВЛЕНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ

Часть 2

Валидация

(ISO 13849-2:2012, IDT)

Издание официальное

Москва
Российский институт стандартизации
2025

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Республиканским государственным предприятием на праве хозяйственного ведения «Казахстанский институт стандартизации и метрологии» Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Комитетом технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации по результатам голосования в АИС МГС (протокол от 25 сентября 2023 г. № 165-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Казахстан	KZ	Госстандарт Республики Казахстан
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт
Узбекистан	UZ	Узбекское агентство по техническому регулированию

4 Приказом Федерального агентства по техническому регулированию и метрологии от 20 ноября 2025 г. № 1440-ст межгосударственный стандарт ГОСТ ISO 13849-2—2023 введен в действие в качестве национального стандарта Российской Федерации с 1 декабря 2026 г.

5 Настоящий стандарт идентичен международному стандарту ISO 13849-2:2012 «Безопасность машин. Элементы систем управления, связанные с обеспечением безопасности. Часть 2. Валидация» («Safety of machinery — Safety-related parts of control systems — Part 2: Validation», IDT).

Международный стандарт ISO 13849-2:2012 подготовлен Техническим комитетом по стандартизации ISO/TC 199 «Безопасность машин» Международной организации по стандартизации (ISO).

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

6 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

Содержание

Введение

ISO 13849 состоит из следующих частей под общим заголовком «Безопасность оборудования. Элементы безопасности систем управления»:

- Часть 1. Общие принципы проектирования;
- Часть 2: Валидация.

Приложения от A до D, носящие справочный характер, структурированы в соответствии с таблицей 1.

Таблица 1 — Структура приложений от A до D данной части ISO 13849

Приложение	Технологии	Список основных принципов безопасности	Список испытанных принципов безопасности	Список испытанных элементов	Списки неисправностей и исключения неисправностей
		Таблица(ы)			
A	Механическая	A.1	A.2	A.3	A.4, A.5
B	Пневматическая	B.1	B.2	—	с B.3 по B.18
C	Гидравлическая	C.1	C.2	—	с C.3 по C.12
D	Электрическая (включая электронику)	D.1	D.2	D.3	с D.4 по D.21

Структура стандартов, относящихся к безопасности в области оборудования, следующая:

a) стандарты типа A — основные стандарты по безопасности, устанавливающие основные понятия, принципы конструирования и общие положения, которые могут быть применены ко всем машинам;

b) стандарты типа B — общие стандарты по безопасности, рассматривающие один аспект безопасности или один тип защитного устройства, которое может использоваться для широкого класса машин:

- стандарты типа B1 — стандарты по конкретным аспектам безопасности (например, по безопасным расстояниям, шумам, безопасной температуре поверхности и т. п.);
- стандарты типа B2 — стандарты по защитным устройствам (например, по двуручным управляющим устройствам, устройствам блокировки, датчикам давления, защитным ограждениям и т. п.);

c) стандарты типа C — стандарты по безопасности машин, рассматривающие детализированные требования к безопасности отдельной машины или группы машин.

Настоящий стандарт является стандартом типа B, как установлено в ISO 12100.

Требования этого документа могут быть дополнены или изменены стандартом типа C.

Для машин, на которые распространяется действие стандарта типа C и которые были сконструированы и изготовлены в соответствии с требованиями настоящего стандарта, требования стандарта типа C имеют приоритет.

Эта часть стандарта ISO 13849 определяет процесс валидации функций безопасности, категорий и уровней эффективности для связанных с безопасностью элементов систем управления. Она признает, что валидация связанных с безопасностью частей систем управления может быть достигнута путем сочетания анализа (см. раздел 5) и испытаний (см. раздел 6), и определяет конкретные обстоятельства, при которых следует проводить испытания.

Большинство процедур и условий в этой части ISO 13849 основаны на предположении, что используется упрощенная процедура оценки уровня эффективности защиты (PL), описанная в ISO 13849-1:2006, 4.5.4. Эта часть ISO 13849 не содержит указаний для ситуаций, когда для оценки PL используются другие процедуры (например, моделирование Маркова), и в этом случае некоторые из его положений не будут применяться и могут потребоваться дополнительные требования.

Руководство по общим принципам конструирования (см. ISO 12100) связанных с безопасностью элементов систем управления, независимо от типа используемой технологии (электрической, гидравлической, пневматической, механической и т. д.), приведено в ISO 13849-1. Сюда входят описания некоторых типичных функций безопасности, определение требуемых уровней их эффективности и общие требования к категориям и уровням эффективности.

В этой части ISO 13849 некоторые требования к валидации являются общими, тогда как другие зависят от типа используемой технологии.

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Безопасность оборудования

ЭЛЕМЕНТЫ СИСТЕМ УПРАВЛЕНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ

Часть 2

Валидация

Safety of machinery. Safety-related parts of control systems. Part 2. Validation

Дата введения — 2026—12—01

1 Область применения

Настоящий стандарт устанавливает процедуры и условия процесса валидации, которая проводится путем анализа и испытаний:

- заданных функций безопасности;
- достигнутой категории;
- достигнутого уровня эффективности защиты связанными с безопасностью элементами систем управления (SRP/CS), сконструированными в соответствии с ISO 13849-1.

Примечание — Дополнительные требования к программируемым электронным системам, включая встроенное программное обеспечение, приведены в ISO 13849-1:2006, 4.6, и IEC 61508.

2 Нормативные ссылки

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

ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction (Безопасность машин. Общие принципы проектирования. Оценка риска и снижение риска)

ISO 13849-1:2006, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность машин. Элементы систем управления, связанные с обеспечением безопасности. Часть 1. Общие принципы конструирования)

3 Термины и определения

В настоящем стандарте применены термины по ISO 12100 и ISO 13849-1.

4 Процесс валидации

4.1 Принципы валидации

Целью процесса валидации является подтверждение того, что конструкция SRP/CS соответствует общим требованиям безопасности машин.

Баланс между анализом и проведением испытаний зависит от конструктивных особенностей элементов, связанных со следующим:

Издание официальное

a) заданными характеристиками функций безопасности, обеспечиваемых этим элементом, как указано в обосновании проекта;

b) требованиями заданного уровня эффективности защиты (см. ISO 13849-1:2006, 4.5):

1) требованиями заданной категории (см. ISO 13849-1:2006, 6.2),

2) мерами по контролю и предотвращению систематических отказов (см. ISO 13849-1:2006, приложение G),

3) если применимо, требованиями к программному обеспечению (см. ISO 13849-1:2006, 4.6);

4) способностью выполнять функцию безопасности в ожидаемых условиях окружающей среды;

c) эргономичным дизайном интерфейса оператора, например, чтобы у оператора не было возможности действовать опасным образом, например, обойти SRP/CS (см. ISO 13849-1:2006, 4.8).

Валидацию должны проводить лица, не зависимые от разработки SRP/CS.

Примечание — При независимой экспертизе не обязательно проводить испытания третьей стороной.

Валидация состоит из применения анализа (см. раздел 5) и выполнения функциональных испытаний (см. раздел 6) в прогнозируемых условиях в соответствии с планом валидации. На рисунке 1 представлен обзор процесса валидации. Баланс между анализом и проведением испытаний зависит от технологии, используемой для компонентов, связанных с безопасностью, и требуемого уровня эффективности защиты. Для категорий 2, 3 и 4 валидация функции безопасности должна также включать испытания в условиях неисправности.

Анализ следует начинать как можно раньше в процессе конструирования и параллельно с ним. В этом случае проблемы можно решить на ранней стадии, когда их еще относительно легко исправить, т. е. на этапах «конструирование и техническая реализация функции безопасности» и «оценка уровня эффективности защиты PL» [четвертый и пятый блоки в ISO 13849-1: 2006, рисунок 3]. Может оказаться необходимым отложить некоторые части анализа до тех пор, пока схема не будет хорошо конструирована.

Там, где это необходимо из-за размера системы, сложности или последствий ее интеграции с системой управления (механизмом), должны быть приняты специальные меры:

- проверка SRP/CS отдельно перед объединением, включая моделирование соответствующих входных и выходных сигналов;
- подтверждение результатов объединения элементов безопасности в остальную часть системы управления в контексте ее использования в машине.

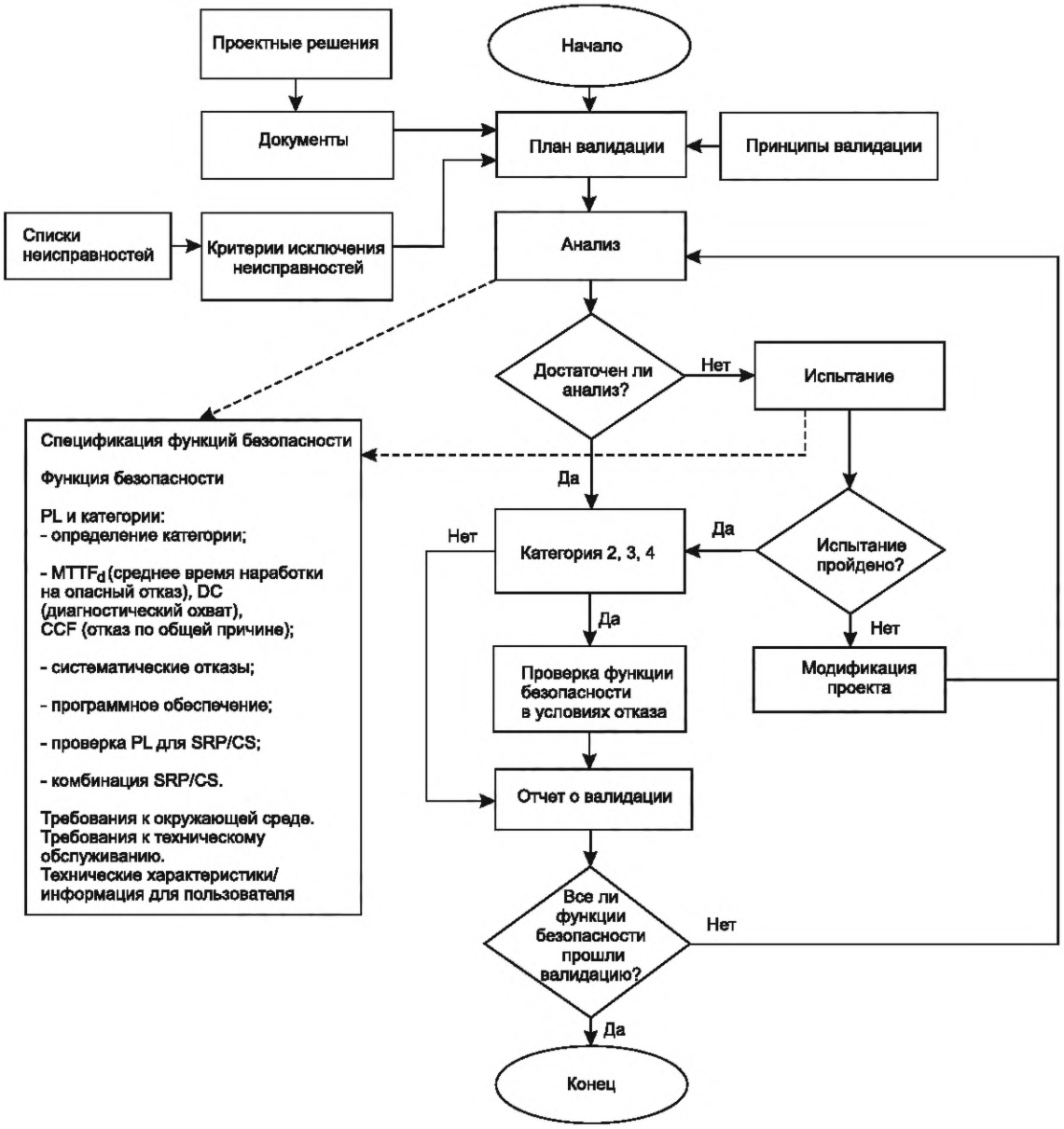


Рисунок 1 — Обзор процесса валидации

«Модификация проекта» на рисунке 1 относится к процессу конструирования. Если валидация не может быть успешно завершена, необходимы изменения в проекте. Затем следует повторить валидацию модифицированных элементов. Этот процесс следует повторять до тех пор, пока все элементы функций безопасности не пройдут успешную валидацию.

4.2 План валидации

План валидации должен определять и описывать требования к проведению процесса валидации для заданных функций безопасности, их категорий и уровней эффективности защиты.

План валидации должен также определять средства, которые будут использоваться для валидации определенных функций безопасности, категорий и уровней эффективности защиты. В нем должны быть изложены, где это уместно:

a) идентичность документов спецификации;
b) условия эксплуатации и окружающей среды во время испытаний;
c) анализы и испытания, которые необходимо применить;
d) ссылка на применяемые стандарты испытаний;

e) лица или стороны, ответственные за каждый этап процесса валидации.

Элементы безопасности, которые ранее прошли валидацию по той же спецификации, нуждаются только в ссылке на предыдущую валидацию.

4.3 Типичные неисправности

Процесс валидации включает рассмотрение поведения SRP/CS для всех рассматриваемых неисправностей. Некоторые типичные неисправности на основе данных, взятых из практики, приведены в таблицах неисправностей в приложениях от A до D. В перечень типичных неисправностей входят:

- неисправности, связанные с соединениями элементов, например проводами, кабелями (см. приложение D);
- неисправности, которые необходимо учитывать, например, короткие замыкания между проводами;
- разрешенные исключения неисправностей, принимая во внимание аспекты окружающей среды, эксплуатации и применения;
- раздел примечаний с указанием причин исключения неисправностей. В списках неисправностей учитываются неисправности, проявляющиеся постоянно.

4.4 Специфические неисправности

При необходимости, должен быть создан специальный список неисправностей, связанных с продуктом, в качестве справочного документа для процесса валидации элемента (элементов) безопасности. Список может быть основан на соответствующем (соответствующих) общем списке (списках), приведенном (приведенных) в приложениях.

Если конкретный список неисправностей, связанных с продуктом, основан на общем списке (списках), в нем должны быть указаны:

a) неисправности, взятые из общего (общих) списка (списков), которые необходимо включить;

b) любые другие значимые неисправности, которые должны быть включены, но не указаны в общем списке (например, отказы с общей причиной);

c) неисправности, взятые из общего списка (списков), которые могут быть исключены на основании того, что критерии, приведенные в общем списке (списках) (см. ISO 13849-1:2006, 7.3), удовлетворены;

d) любые другие неисправности, для которых общий (общие) список (списки) не допускает исключения, но для которых представлено обоснование и объяснение исключения (см. ISO 13849-1:2006, 7.3).

Если этот список не основан на общем списке (списках), разработчик должен дать обоснование исключения неисправностей.

4.5 Информация для валидации

Информация, необходимая для валидации, будет варьироваться в зависимости от используемой технологии, категории (категорий) и уровня (уровней) эффективности защиты, которые должны быть продемонстрированы, конструктивного обоснования системы и вклада SRP/CS в снижение риска. Документы, содержащие достаточную информацию из следующего списка, должны быть включены в процесс валидации, чтобы продемонстрировать, что элементы безопасности выполняют заданные функции безопасности на требуемом уровне (уровнях) эффективности защиты и категории (категориях):

a) спецификация требуемых характеристик каждой функции безопасности, ее требуемой категории и уровня эффективности защиты;

b) чертежи и спецификации, например, для механических, гидравлических и пневматических элементов, печатных плат, смонтированных печатных плат, внутренней проводки, корпуса, материалов, монтажа;

c) блок-схема (схемы) с функциональным описанием блоков;

d) коммутационные схемы, включая интерфейсы/соединения;

e) функциональное описание коммутационных схем;

f) диаграммы временной последовательности для функций переключения сигналов, связанных с безопасностью;

g) описание соответствующих характеристик компонентов, ранее уже прошедших валидацию;

h) для других элементов безопасности, кроме перечисленных в g), перечень с номинальными и допустимыми значениями параметров, со значениями напряжения при эксплуатации, с указанием типового представителя, сданными о количестве отказов, с информацией об изготовителе и любые другие данные, необходимые для безопасности;

i) анализ всех типичных неисправностей (см. также 4.3 и 4.4), перечисленных в таблицах приложений от A до D, включая обоснование любых исключенных неисправностей;

j) анализ влияния используемых материалов;

k) информацию по использованию, например, руководство по установке и эксплуатации/руководство по эксплуатации.

Если программное обеспечение имеет отношение к функции (функциям) безопасности, документация по программному обеспечению должна включать:

- четкую и однозначно идентифицируемую спецификацию, в которой указаны характеристики безопасности, которых должно достичь программное обеспечение;
- свидетельство того, что программное обеспечение предназначено для достижения требуемого уровня эффективности защиты (см. 9.5);
- подробную информацию об испытаниях (в частности, отчеты об испытаниях), проведенных для подтверждения того, что требуемые показатели безопасности достигнуты.

Примечание — См. требования в ISO 13849-1:2006, 4.6.2 и 4.6.3.

Требуется информация о том, как определяется уровень эффективности защиты и средняя вероятность опасного отказа в час. Документация количественных аспектов должна включать:

- блок-схему функции безопасности (см. ISO 13849-1:2006, приложение B) или назначенную архитектуру (см. ISO 13849-1:2006, 6.2);
- определение $MTTF_d$, DC_{avg} и CCF;
- определение категории (см. таблицу 2).

Информация требуется для документирования систематических аспектов SRP/CS.

Требуется информация о том, как комбинация нескольких SRP/CS обеспечивает требуемый уровень эффективности защиты.

Таблица 2 — Требования к документации для категорий в отношении уровней эффективности защиты

Требования документации	Категория, для которой требуется документация				
	B	1	2	3	4
Основные принципы безопасности	X	X	X	X	X
Ожидаемые рабочие нагрузки	X	X	X	X	X
Влияние используемого материала	X	X	X	X	X
Эффективность защиты во время других значимых внешних воздействий	X	X	X	X	X
Испытанные компоненты		X			
Испытанные принципы безопасности		X	X	X	X
Среднее время наработки на опасный отказ ($MTTF_d$) каждого канала	X	X	X	X	X
Процедура проверки функций безопасности			X		
Выполненные диагностические мероприятия, включая реакцию на неисправность			X	X	X
Интервалы валидации, если указано			X	X	X
Диагностический охват (DC_aVg)			X	X	X
Предполагаемые при конструировании отдельные неисправности и методы их обнаружения	—	—	X	X	X
Отказ по общей причине (CCF) и способы его предотвращения)			X	X	X

Окончание таблицы 2

Требования документации	Категория, для которой требуется документация				
	B	1	2	3	4
Предполагаемое исключение одиночной неисправности				X	X
Неисправности, которые необходимо обнаружить			X	X	X
Как функция безопасности поддерживается в случае каждой неисправности				X	X
Как поддерживается функция безопасности для каждой комбинации неисправностей					X
Меры против систематических отказов	X	X	X	X	X
Меры против программных неисправностей	X		X	X	X
X — документация требуется — — документация не требуется					
Примечание — Категории даны в ISO 13849-1:2006.					

4.6 Отчет о валидации

Валидация путем анализа и испытаний должна быть запротоколирована. Отчет должен демонстрировать процесс валидации для каждого из требований безопасности. Можно делать перекрестные ссылки на предыдущие отчеты о валидации при условии, что они должным образом идентифицированы.

Для любого элемента безопасности, который не прошел процесс валидации, в отчете о валидации должно быть указано, какие элементы в анализе/испытаниях оказались неудовлетворительными. Должно быть обеспечено, чтобы все элементы безопасности успешно прошли повторную валидацию после модификации.

5 Валидация анализом

5.1 Общие положения

Валидация SRP/CS должна проводиться путем анализа. Входные данные для анализа включают следующее:

- функции безопасности, их характеристики и требуемый уровень эффективности защиты, определенные в ходе анализа риска (см. ISO 13849-1:2006, рисунки 1 и 3);
- количественные аспекты ($MTTF_d$, DC_{avg} и CCF);
- «структуру системы (например, структурное построение обозначенной категории) (см. ISO 13849-1:2006, раздел 6);
- не поддающиеся количественной оценке качественные аспекты, влияющие на поведение системы (если применимо, программные аспекты);
- детерминированные параметры.

Валидация функций безопасности путем анализа, а не испытаний, требует применения детерминированных параметров.

Примечания

1 Детерминированный параметр — это параметр, основанный на качественных аспектах (например, качество изготовления, опыт использования). Он зависит от применения. Эти и другие факторы могут влиять на детерминированные параметры.

2 Детерминированные параметры отличаются от других данных тем, что они показывают, что требуемые свойства системы логически следуют из модели системы. Такие параметры могут быть построены на основе простых и понятных концепций.

5.2 Техники проведения анализа

Выбор техники проведения анализа зависит от конкретной цели. Существуют следующие две основные техники.

a) Нисходящие (дедуктивные) методы подходят для определения исходных событий, которые могут привести к выявлению основных событий, и расчета вероятности основных событий на основе вероятности исходных событий. Их также можно использовать для исследования последствий выявленных множественных неисправностей.

Пример — Анализ дерева отказов (FTA, см. IEC 61025), анализ дерева событий (ETA).

b) Восходящие (индуктивные) методы подходят для изучения последствий идентифицированных отдельных неисправностей.

Пример — Анализ видов и последствий отказов (FMEA, см. IEC 60812) и анализ видов, последствий и критичности отказов (FMECA).

6 Валидация испытанием

6.1 Общие положения

Если анализа недостаточно для доказательств установленных требований функций безопасности и категорий, валидация должна быть проведена в полном объеме вместе с испытаниями. Испытания дополняют анализ и часто являются необходимыми для полного завершения валидации.

Испытания в целях валидации должны планироваться и проводиться последовательно. В частности:

a) план испытания должен быть составлен до начала испытаний и включать:
   1) требования к испытаниям;
   2) требуемый результат испытаний на соответствие;
   3) последовательность испытаний;

b) должны вестись записи испытаний, которые включают следующее:
   1) указание фамилий лиц, проводящих испытание;
   2) данные установленных условий окружающей среды (см. раздел 10);
   3) применяемые методы испытаний и испытательное оборудование;
   4) дату испытания;
   5) результаты испытания;

c) протоколы испытаний должны сравниваться с планом испытаний, чтобы убедиться, что заданные функциональные и эксплуатационные цели достигнуты.

Опытный образец для испытаний должен быть конструирован в соответствии с окончательно отработанной конструкцией, т. е. со всеми периферийными устройствами и соответствующей защитой.

Это испытание может проводиться вручную или автоматизированным способом, например, с помощью компьютера.

Где применимо, валидация функций безопасности путем испытаний должна выполняться путем подачи входных сигналов в различных комбинациях на SRP/CS. Результирующий отклик на выходах должен сравниваться с соответствующими указанными выходами.

Рекомендуется систематически применять комбинацию этих входных сигналов к системе управления и машине. Примером этого является включение питания, запуск, управление, изменение направления, перезапуск. При необходимости должен применяться расширенный диапазон входных данных для учета аномальных или необычных ситуаций, чтобы увидеть, как реагирует SRP/CS. Такие комбинации входных данных должны учитывать предсказуемые некорректные операции.

Цели испытания будут определять условия окружающей среды для этого испытания:

- условия окружающей среды предполагаемого использования;
- условия при конкретном рейтинге;
- заданный диапазон условий, если ожидается отклонение.

Диапазон условий, который считается стабильным и при котором испытания действительны, должен быть согласован между разработчиком и лицом (лицами), ответственными за проведение испытаний, и должен быть зарегистрирован.

6.2 Погрешность измерения

Погрешность измерений при валидации испытанием должна соответствовать проводимому испытанию. Как правило, погрешность этих измерений должна быть в пределах 5 К для измерений температуры и 5 % для следующих измерений:

a) измерение времени;
b) измерение давления;
c) измерение силы;
d) электрические измерения;
e) измерение относительной влажности;
f) линейные измерения.

Отклонения от этих погрешностей измерений должны быть обоснованы.

6.3 Повышенные требования

Если согласно сопроводительной документации требования к SRP/CS превышают требования настоящего стандарта, должны применяться повышенные требования.

Примечание — Повышенные требования могут предъявляться к системам управления, если система управления должна выдерживать особенно неблагоприятные условия эксплуатации, например, небрежное обращение, воздействие влаги, гидролизация, перепады температуры окружающего воздуха, воздействие химических веществ, коррозию, высокую напряженность электромагнитных полей, например, из-за близкого расположения датчиков.

6.4 Количество испытуемых образцов

Если не указано иное, испытания должны проводиться на одном производственном образце испытуемого элемента безопасности.

Испытываемые элементы безопасности не должны модифицироваться в ходе испытаний.

Определенные испытания могут навсегда изменить эффективность защиты некоторых компонентов. Если постоянное изменение в компоненте приводит к тому, что элемент безопасности становится неспособным удовлетворять требованиям дальнейших испытаний, для последующих испытаний должен использоваться новый образец или образцы.

Если конкретное испытание является разрушающим и эквивалентные результаты могут быть получены путем изолированного испытания элемента SRP/CS, вместо целого (целых) элемента (элементов) безопасности, может быть использована часть этого элемента (элементов) безопасности с целью получения результатов испытания. Этот метод должен применяться только в том случае, если анализ показал, что испытания одной части элемента безопасности достаточно для демонстрации характеристик безопасности всего элемента безопасности, который выполняет функцию безопасности.

7 Валидация спецификации требований безопасности для функций безопасности

Перед валидацией проекта SRP/CS или комбинации SRP/CS, обеспечивающей функцию безопасности, спецификация требований к функции безопасности должна быть проверена для обеспечения согласованности и полноты ее использования по назначению.

Перед началом конструирования следует проанализировать спецификацию требований безопасности, поскольку любая другая деятельность основана на этих требованиях.

Должно быть обеспечено документирование требований ко всем функциям безопасности системы управления машиной.

Для проверки спецификации должны быть применены соответствующие меры для обнаружения систематических отказов (ошибок, упущений или несоответствий).

Валидация может выполняться путем рассмотрения и проверки требований безопасности SRP/CS и проектных спецификаций, в частности, чтобы доказать, что все аспекты требований к предполагаемому применению и безопасности и условий эксплуатации и окружающей среды, а также возможные человеческие ошибки (например, неправильное использование) были рассмотрены.

Если стандарт на продукцию устанавливает требования безопасности для конструирования SRP/CS (например, ISO 11161 для интегрированных производственных систем или ISO 13851 для устройств двуручного управления), они должны быть приняты во внимание.

8 Валидация функций безопасности

Валидация функций безопасности должна демонстрировать, что SRP/CS или комбинация SRP/CS обеспечивают функцию (функции) безопасности в соответствии с их заданными характеристиками.

Примечание — Потеря функции безопасности при отсутствии аппаратной неисправности происходит из-за систематического отказа, который может быть вызван ошибками, допущенными на этапах конструирования и интеграции (неверная интерпретация характеристик функции безопасности, ошибка в логической схеме , ошибка в аппаратной сборке, ошибка в наборе кода ПО и т. д.). Некоторые из этих систематических ошибок будут выявлены в процессе конструирования, а другие — в процессе валидации, либо останутся незамеченными. Кроме того, также возможна ошибка (например, отказ от проверки характеристики) в процессе валидации.

Валидация заданных характеристик функций безопасности должна быть достигнута путем применения соответствующих мер из следующего списка.

- Функциональный анализ схем, обзоры программного обеспечения (см. 9.5).

Примечание — Если машина имеет сложные или многочисленные функции безопасности, анализ может уменьшить количество требуемых функциональных испытаний.

- Моделирование.
- Проверка аппаратных компонентов, установленных на машине, и сведений о соответствующем программном обеспечении для подтверждения их соответствия документации (например, изготовитель, тип, версия).
- Функциональные испытания функций безопасности во всех режимах работы машины, чтобы установить, соответствуют ли они заданным характеристикам (см. ISO 13849-1:2006, раздел 5, для спецификаций некоторых типичных функций безопасности). Функциональные испытания должны гарантировать, что все выходы, связанные с безопасностью, реализуются во всем их полном диапазоне и реагируют на входные сигналы, связанные с безопасностью, в соответствии со спецификацией. Тестовые случаи обычно извлекаются из спецификаций, но могут также включать в себя некоторые случаи, полученные в результате анализа схем или программного обеспечения.
- Расширенное функциональное тестирование для проверки предсказуемых аномальных сигналов или комбинаций сигналов от любого источника входного сигнала, включая прерывание и восстановление питания, а также некорректные операции.
- Проверка взаимодействия оператора с SRP/CS на соответствие принципам эргономики (см. ISO 13849-1:2006, 4.8).

Примечание — Другие меры против систематических отказов, упомянутые в 9.4 (например, многообразие, обнаружение отказов с помощью автоматических испытаний), также могут способствовать обнаружению функциональных неисправностей.

9 Валидация уровней и категорий эффективности защиты

9.1 Анализ и тестирование

Для SRP/CS или комбинации SRP/CS, которая обеспечивает функцию (функции) безопасности, валидация должна продемонстрировать, что требуемые уровни эффективности защиты (PL_r) и категории в спецификации требований безопасности выполняются. В основном это потребует анализа отказов с использованием принципиальных схем (см. раздел 5), и если анализ отказов не дает результатов, проводятся:

- испытания по определенной схеме и моделирование неисправностей на испытуемых образцах, в частности в областях риска относительно производительности, установленной при анализе отказов (см. раздел 6);
- моделирование поведения системы управления в случае неисправности, например, с помощью моделей аппаратного обеспечения и (или) программного обеспечения.

В некоторых ситуациях может возникнуть необходимость разделить связанные элементы безопасности на несколько функциональных групп и подвергнуть эти группы и их интерфейсы испытаниям с имитацией неисправности.

При валидации испытанием испытания должны включать, в зависимости от обстоятельств:

- испытания по внедрению ошибок в серийный образец;

- испытания по внедрению ошибок в аппаратную модель;
- программное моделирование неисправностей;
- отказ подсистемы, например, источников питания.

Момент, когда неисправности могут проявиться в системе, может оказаться критическим. Самые неблагоприятные варианты проявления неисправностей должны быть определены при анализе, соответственно с этим анализом неисправности должны быть выявлены для предупреждения наступления критических моментов.

9.2 Валидация на соответствие категорий

9.2.1 Категория B

SRP/CS категории B должны пройти валидацию в соответствии с основными принципами безопасности (см. таблицы A.1, B.1, C.1 и D.1) подтверждением того, что требования, проект, конструкция и выбор компонентов соответствуют ISO 13849-1:2006, 6.2.3. Должно быть продемонстрировано, что $MTTF_d$ канала составляет не менее трех лет. Для этого проводится проверка элементов безопасности системы управления на соответствие требованиям, установленным в документах для валидации (см. 4.5). Требования по условиям окружающей среды для валидации см. 6.1.

Примечание — В особых случаях могут потребоваться более высокие значения $MTTF_d$, например, когда $PL_r = b$.

9.2.2 Категория 1

Валидацию на соответствие категории 1 элементов безопасности систем управления следует проводить для подтверждения того, что:

a) они соответствуют требованиям категории B;

b) компоненты испытаны (см. таблицы A.3 и D.3) и соответствуют хотя бы одному из следующих условий:

1) они широко использовались в прошлом с успешными результатами в аналогичных приложениях;

2) были изготовлены и проверены с использованием принципов, демонстрирующих их пригодность и надежность для применений, связанных с безопасностью;

c) хорошо зарекомендовавшие себя принципы безопасности (там, где это применимо, см. таблицы A.2, B.2, C.2 и D.2) были реализованы правильно, а там, где использовались новые разработанные принципы, была проведена валидация:

1) предупреждение ожидаемых видов отказов;

2) предупреждение неисправностей или снижение их вероятности до приемлемого уровня.

Соответствующие стандарты компонентов могут быть использованы для демонстрации соответствия требованиям настоящего пункта (см. таблицы A.3 и D.3). Должно быть продемонстрировано, что $MTTF_d$ канала составляет не менее 30 лет.

9.2.3 Категория 2

Валидацию на соответствие категории 2 элементов безопасности систем управления следует проводить для подтверждения того, что:

a) они соответствуют требованиям категории B;

b) используемые проверенные принципы безопасности (если применимо) соответствуют 9.2.2 c);

c) контрольное оборудование обнаруживает все соответствующие неисправности, применяемые по одному в процессе проверки, и производит соответствующее контрольное действие, которое:

1) инициирует безопасное состояние;

2) когда это невозможно, предупреждает о риске;

d) проверка, обеспечиваемая контрольным оборудованием, не приводит к небезопасному состоянию;

e) инициирование проверки осуществляется:

1) при запуске машины и до возникновения опасной ситуации;

2) периодически, в процессе эксплуатации, в соответствии с техническим заданием и если оценка рисков и вид работ показывают, что это необходимо.

Примечание — Необходимость и объем проверок во время эксплуатации определяются оценкой риска проектировщиком и типом необходимой операции;

f) $MTTF_d$ функционального канала ($MTTF_{d,L}$) не менее 3 лет;

g) $MTTF_{d,TE}$ больше половины $MTTF_{d,L}$;

h) скорость испытания ≥ 100 x ожидаемая скорость испытания;

i) DC_{avg} составляет не менее 60 %;

j) количество отказов по общей причине значительно снижено (см. ISO 13849-1:2006, приложение F).

Примечание — В отдельных случаях могут потребоваться более высокие значения $MTTF_d$ и/или DC_{avg}, например, из-за высокого PL_r.

9.2.4 Категория 3

Валидацию на соответствие категории 3 элементов безопасности систем управления следует проводить для подтверждения того, что:

a) они соответствуют требованиям категории B;

b) испытанные принципы безопасности (если применимо) соответствуют требованиям 9.2.2 c);

c) отдельная неисправность не приводит к потере функции безопасности;

d) выявление отдельных неисправностей (включая неисправности по общей причине) в соответствии с проектным обоснованием и применяемой технологией;

e) $MTTF_d$ каждого канала составляет не менее трех лет;

f) DC_{avg} составляет не менее 60 %;

g) количество отказов по общей причине значительно снижено (см. ISO 13849-1:2006, приложение F).

Примечание — В особых случаях могут потребоваться более высокие значения $MTTF_d$ и/или DC_{avg}, например, из-за высокого PL_r.

9.2.5 Категория 4

Валидацию на соответствие категории 4 элементов безопасности систем управления следует проводить для подтверждения того, что:

a) они соответствуют требованиям категории B;

b) испытанные принципы безопасности (если применимо) соответствуют 9.2.2 c);

c) отдельная неисправность (включая неисправности группового типа) не приводит к потере функции безопасности;

d) отдельные неисправности обнаруживаются во время или до следующего требования к функции безопасности, что достигается при DC_{avg} не менее 99 %;

e) если неисправность не обнаружена при DC_{av} не менее 99 %, накопление неисправностей не приводит к потере функции (й) безопасности, а степень рассматриваемого накопления неисправностей соответствует проектному обоснованию;

f) $MTTF_d$ каждого канала составляет не менее 30 лет;

g) количество отказов по общей причине значительно снижено (см. ISO 13849-1:2006, приложение F).

9.3 Валидация $MTTF_d$, DC_{avg} и CCF

Проверка $MTTF_d$, DC_{avg} и CCF обычно выполняется путем анализа и визуального осмотра.

Значения $MTTF_d$ для компонентов (включая значения B_{10d}, T_{10d} и n_{op}) должны быть проверены на правдоподобие (например, в соответствии с ISO 13849-1:2006, приложение C). Например, значение, указанное в таблице данных поставщика, необходимо сравнить с ISO 13849-1:2006, приложение C. Если заявления об исключении неисправностей означают, что определенные компоненты не вносят вклад в канал $MTTF_d$, должно быть проверено правдоподобие исключения неисправностей.

Примечания

1 Исключение неисправностей подразумевает бесконечное $MTTF_d$; следовательно, компонент не будет участвовать в расчете $MTTF_d$ канала.

2 Для определения значения B_{10d}, например, см. IEC 60947-4-1:2010, приложение K.

$MTTF_d$ каждого канала SRP/CS, включая применение формулы симметрирования (см. ISO 13849-1:2006, приложение D) к разнородным резервным каналам, должно быть проверено на правильность расчета. До применения формулы симметрирования должно быть обеспечено, чтобы $MTTF_d$ отдельных каналов не превышало 100 лет.

Значения DC для компонентов и/или логических блоков должны быть проверены на правдоподобие (например, в сравнении с мероприятиями в ISO 13849-1:2006, приложение E). Правильное проведение (аппаратное и программное обеспечение) проверок и диагностики, включая соответствующую реакцию на неисправность, должны быть подтверждены испытаниями в типичных условиях окружающей среды при использовании.

DC_{avg} SRP/CS должен быть проверен на корректность расчета.

Правильное выполнение достаточных мер против отказов по общей причине должно пройти валидацию (например, в соответствии с ISO 13849-1:2006, приложение F). Типичными способами валидации являются статический анализ оборудования и функциональные испытания в условиях окружающей среды.

Примечание — Для расчета значений $MTTF_d$ электронных компонентов за основу принимается температура окружающей среды +40 °C. Во время валидации важно убедиться, что для значений $MTTF_d$ соблюдены условия окружающей среды и функциональные условия (в частности, температура), взятые за основу. Если устройство или компонент эксплуатируются при температуре, значительно превышающей (например, более 15 °C) указанную температуру +40 °C, необходимо использовать значения $MTTF_d$ для повышенной температуры окружающей среды.

9.4 Валидация мер против систематических отказов, связанных с уровнем эффективности защиты и категорией SRP/CS

Валидация мер против систематических отказов (определенных в ISO 13849-1:2006, 3.1.7), связанных с уровнями эффективности защиты и категориями каждого SRP/CS, обычно может быть обеспечена:

a) проверками проектной документации, подтверждающей применение:

1) основных и испытанных принципов безопасности (см. приложения от A до D);

2) дополнительных мер по предотвращению систематических отказов (см. ISO 13849-1:2006, G.3);

3) дополнительных мер по контролю систематических отказов, таких как разнообразие аппаратных средств (см. ISO 13849-1:2006, приложение G), защита от модификаций или программирование подтверждения отказов;

b) анализом отказов (например, FMEA);

c) испытаниями с введением/инициированием неисправности;

d) проверками и испытаниями средств передачи данных, если применимо;

e) проверками того, что система менеджмента качества позволяет избежать причин систематических отказов в производственном процессе.

9.5 Валидация программного обеспечения, связанного с безопасностью

Валидация как встроенного программного обеспечения функций безопасности (SRESW), так и прикладного программного обеспечения функций безопасности (SRASW), должна включать:

- заданное функциональное поведение и критерии эффективности защиты (например, временные характеристики) программного обеспечения при выполнении на целевом оборудовании;
- проверку того, что меры программного обеспечения достаточны для заданного PL_r функции безопасности;
- меры и действия, предпринятые во время конструирования программного обеспечения для предотвращения систематических ошибок программного обеспечения.

В качестве первого шага, проверьте наличие документации по техническому регламенту и проектному решению программного обеспечения функции безопасности. Эта документация должна быть проверена на полноту и отсутствие ошибочных толкований, упущений или несоответствий.

Примечание — В случае небольших программ, анализ программы посредством обзоров или прогона потока управления, процедур и т.д. с использованием документации к программному обеспечению (схема потока управления, исходный код модулей или блоков, ввод-вывод и списки распределения переменных, списки перекрестных ссылок) может быть достаточно.

В общем, программное обеспечение можно рассматривать как «черный ящик» или «серый ящик» (см. ISO 13849-1:2006, 4.6.2) и подтверждать испытанием черного или серого ящика соответственно.

В зависимости от PL_r [ISO 13849-1:2006, 4.6.2 (для SRESW) и 4.6.3 (для SRASW)], испытания должны включать:

- испытание функционального поведения и эффективности защиты методом «черного ящика» (например, временные характеристики);
- дополнительные расширенные тестовые примеры, основанные на анализе предельных значений, рекомендуемые для PL d или e;
- испытания ввода/вывода, чтобы гарантировать правильное использование входных и выходных сигналов функции безопасности;
- контрольные примеры, которые моделируют ошибки, определенные предварительно аналитически, вместе с ожидаемой реакцией, чтобы оценить адекватность мер программного обеспечения для контроля отказов.

Отдельные программные функции, которые уже прошли валидацию, не нуждаются в повторной валидации. Однако, если несколько таких функциональных блоков безопасности объединены для конкретного проекта, должна быть подтверждена результирующая общая функция безопасности.

Документация по программному обеспечению должна быть проверена, чтобы подтвердить, что были реализованы достаточные меры и действия против систематических ошибок программного обеспечения в соответствии с упрощенной V-моделью (ISO 13849-1:2006, рисунок 6).

Меры по внедрению программного обеспечения в соответствии с ISO 13849-1:2006, 4.6.2 (для SRESW) и 4.6.3 (для SRASW), которые зависят от требуемого PL, должны быть рассмотрены в отношении их надлежащей реализации.

Если связанное с безопасностью программное обеспечение будет впоследствии модифицировано, оно должно пройти повторную валидацию в соответствующем масштабе.

9.6 Валидация и верификация уровня эффективности защиты

Для упрощенной процедуры оценки PL SRP/CS в соответствии с ISO 13849-1:2006, 4.5.4 и ISO 13849-1:2006, приложения B — F и приложение K, должны быть выполнены следующие этапы верификации и валидации:

- проверка правильности оценки PL на основе категории, DC_{avg} и $MTTF_d$ (согласно ISO 13849-1:2006, 4.5.4 и приложения K);
- проверка того, что PL, достигнутый SRP/CS, удовлетворяет требуемому уровню эффективности защиты PL_r в спецификации требований безопасности для машинного оборудования: $PL \geq PL_r$.

Если для оценки достигнутого PL используются другие методы, основанные на расчетной средней вероятности опасного отказа в час, валидация должна учитывать:

- значение $MTTF_d$ для каждого компонента;
- DC;
- CCF;
- структуру;
- документацию, применение и расчет, правильность которых должна быть проверена.

9.7 Валидация комбинации элементов безопасности

Если функция безопасности реализуется двумя или более элементами, должна быть проведена валидация комбинации — путем анализа и, при необходимости, испытаний — для установления того, что комбинация обеспечивает уровень характеристик, указанный в проекте. Существующие зарегистрированные результаты проверки элементов безопасности могут быть приняты во внимание. Должны быть выполнены следующие шаги валидации:

- проверка проектной документации, описывающей общие функции безопасности;
- проверка того, что общий PL комбинации SRP/CS был правильно оценен на основе PL каждого отдельного элемента безопасности (согласно ISO 13849-1:2006, 6.3).

Примечание — В качестве альтернативы ISO 13849-1:2006, таблица 11, может быть использована сумма средней вероятности опасных отказов в час для всех объединенных SRP/CS. Важно проверить не поддающиеся количественной оценке ограничения систематических, архитектурных аспектов и аспектов CCF, которые могут ограничивать общий уровень эффективности защиты до более низких значений;

- учет характеристик интерфейсов, например, напряжение, ток, давление, формат данных, уровень сигнала;
- анализ отказов, связанных с комбинацией/интеграцией, например, с помощью FMEA;

- для систем с резервированием, испытания с вводом отказов, связанные с комбинацией/интеграцией.

10 Валидация требований окружающей среды

Характеристики, указанные в проекте SRP/CS, должны быть подтверждены в отношении условий окружающей среды, указанных для системы управления.

Валидация должна проводиться путем анализа и, при необходимости, испытаний. Масштабы анализа и испытаний будут зависеть от элементов безопасности системы, в которой они установлены, используемой технологии и условий окружающей среды, которые проходят валидацию. Использование данных об эксплуатационной надежности системы или ее компонентов либо подтверждение соответствия применимым стандартам окружающей среды (например, в отношении гидроизоляции, защиты от вибрации) могут содействовать процессу валидации.

Там, где это применимо, валидация должна касаться:

- ожидаемых механических нагрузок от ударов, вибрации, попадания загрязнений;
- механической прочности;
- электрических параметров и источников питания;
- климатических условий (температура и влажность);
- электромагнитной совместимости (защищенности).

Когда необходимы испытания для определения соответствия экологическим требованиям, необходимо следовать процедурам, изложенным в соответствующих стандартах, насколько это требуется для применения.

После завершения валидации испытаниями функции безопасности должны оставаться в соответствии с требованиями безопасности технических условий, или SRP/CS должен обеспечивать выходные данные для безопасного состояния.

11 Валидация требований к техническому обслуживанию

Процесс валидации должен продемонстрировать, что положения требований к техническому обслуживанию, указанные в ISO 13849-1:2006, раздел 9, параграф 2, выполнены.

Валидация требований к техническому обслуживанию должна включать следующее, если применимо:

a) обзор информации для использования, подтверждающий, что:

1) инструкции по техническому обслуживанию доработаны [включая процедуры, необходимые инструменты, частота осмотров, временной интервал для замены компонентов, подверженных износу (T_{10d}) и т. д.] и понятны;

2) при необходимости предусмотрена возможность проведения технического обслуживания только квалифицированным обслуживающим персоналом;

b) проверку, которая измеряет простоту обслуживания (например, предоставление диагностических инструментов для помощи в поиске неисправностей и ремонте).

Кроме того, при применении должны быть включены следующие меры:

- меры против ошибок во время технического обслуживания (например, обнаружение неправильных входных данных посредством проверки правдоподобия);
- меры против модификации (например, защита паролем для предотвращения доступа к программе посторонних лиц).

12 Валидация технической документации и информации для использования

Процесс валидации должен продемонстрировать, что требования к технической документации, указанные в ISO 13849-1:2006, раздел 10, и к информации для пользователя, указанные в ISO 13849-1:2006, раздел 11, выполнены.

Приложение А
(справочное)

Валидация механических систем

Когда механические системы используются в сочетании с другими технологиями, следует также учитывать приложение А.

В таблицах А.1 и А.2 перечислены основные и испытанные принципы безопасности.

В таблице А.3 перечислены испытанные компоненты для приложений безопасности, основанные на применении испытанных принципов безопасности и/или стандарта для их конкретных приложений. Испытанный компонент для одних приложений может оказаться неподходящим для других.

В таблицах А.4 и А.5 перечислены исключения неисправностей и их обоснование. Дополнительные исключения см. в 4.4. Точный момент возникновения неисправности может быть критическим (см. 9.1).

Таблица А.1 — Основные принципы безопасности

Основной принцип безопасности	Примечания
Использование подходящих материалов и надлежащего производства	Выбор материала, способы изготовления и обработки по отношению, например, к напряжению, долговечности, эластичности, трению, износу, коррозии, температуры
Правильные размеры и форма	Учитывайте, например, напряжение, деформацию, усталость, шероховатость поверхности, допуски, застревание, изготовление
Правильный выбор, комбинация, расположение, сборка и установка компонентов/системы	Используйте указания производителя по применению, например, каталожные листы, инструкции по установке, технические условия, а также установившуюся практику в области машиностроения в аналогичных компонентах/системах
Использование принципа обесточивания	Безопасное состояние достигается путем отключения электрического напряжения. См. правильный процесс останова в ISO 12100:2010, 6.2.11.3. Энергия подается для начала движения механизма. См. правильный процесс пуска в ISO 12100:2010, 6.2.11.3. Рассмотрите различные режимы, например режим эксплуатации, режим технического обслуживания. **ВАЖНО — Этот принцип не следует соблюдать, когда потеря энергии может создать опасность, например, для сохранения энергии в зажимных устройствах**
Правильное крепление	Для применения винтовой блокировки рассмотрите указания производителя по применению. Необходимо избегать перегрузок путем применения соответствующей технологии прилагаемой нагрузки, создаваемой крутящим моментом
Ограничение генерации и/или передачи силы и подобных параметров	Примерами являются распорный болт, тормозная пластина и муфта ограничения крутящего момента. **ВАЖНО — Этот принцип не следует соблюдать, когда постоянная целостность компонентов необходима для поддержания требуемого уровня контроля**
Ограничение диапазона параметров окружающей среды	Примерами являются температура, влажность и загрязнение в месте установки. См. раздел 10 и учтите указания производителя по применению
Ограничение скорости и подобные параметры	Учитывайте, например, скорость, ускорение, замедление, требуемые приложением
Необходимое время срабатывания	Например, следует учитывать усталостное напряжение пружин, трение, смазку, температуру, инерцию во время ускорения и замедления, сочетание допусков

Окончание таблицы А.1

Основной принцип безопасности	Примечания
Защита от самопроизвольного пуска	Учитывайте самопроизвольный пуск, вызванный накопленной энергией, а также после восстановления питания для различных режимов (рабочий режим, режим обслуживания и т.д.). Может потребоваться специальное оборудование для высвобождения накопленной энергии. Специальные приложения, например, для сохранения энергии для зажимных устройств или обеспечения положения, необходимо рассматривать по отдельности
Упрощение	Избегайте ненужных компонентов в системе безопасности
Разделение	Отделение функций безопасности от других функций
Правильная смазка	Учитывайте потребность в смазочных приспособлениях, информацию о смазочных материалах и интервалах смазки
Надлежащее предотвращение попадания жидкостей и пыли	Учитывайте степень IP-защиты (см. IEC 60529)

Таблица А.2 — Испытанные принципы безопасности

Испытанный принцип безопасности	Примечания
Использование тщательно отобранных материалов и методов производства	Выбор подходящего материала, соответствующих методов производства и обработки, связанных с применением
Использование компонентов с определенным режимом отказа	Преобладающий вид отказа компонента известен заранее и всегда один и тот же. См. ISO 12100:2010, 6.2.12.3
Сверхзаданные параметры или показатели безопасности	Коэффициенты безопасности указаны в стандартах или на основании положительного опыта в приложениях, связанных с безопасностью
Безопасное положение	Подвижная часть компонента удерживается в безопасном положении механическим путем (одного трения недостаточно). Для выхода из безопасного положения требуется сила
Увеличенная сила отключения	Безопасное положение/состояние достигается увеличением силы отключения по сравнению с силой включения
Правильный выбор, комбинирование, размещение, монтаж и установка элементов, системы	—
Тщательный выбор крепления, связанного с приложением	Не полагайтесь только на трение
Положительное механическое воздействие	Для достижения положительного механического воздействия, все движущиеся механические компоненты, необходимые для выполнения функции безопасности, неизбежно должны перемещать связанные компоненты, т.е. кулачковая шайба напрямую размыкает контакты электрического переключателя, а не опирается на пружину. См. ISO 12100:2010, 6.2.5
Составные части	Уменьшение влияния отказов за счет параллельной работы нескольких элементов, например, когда выход из строя одной из нескольких пружин не приводит к опасному состоянию

Окончание таблицы А.2

Испытанный принцип безопасности	Примечания
Использование испытанной пружины (см. также таблицу А.3)	Испытанная пружина требует: - использования тщательно отобранных материалов, методов изготовления (например, предварительная установка и циклование перед использованием) и обработки (например, прокатка и дробеструйная обработка); - обоснованной документации на пружины; - обоснованных показателей безопасности при усталостном напряжении (т. е. с высокой вероятностью того, что разрушение не произойдет). Испытанные винтовые пружины сжатия также могут быть разработаны путем: - использования тщательно отобранных материалов, методов изготовления (например, предварительная установка и циклование перед использованием) и обработки (например, прокатка и дробеструйная обработка); - зазора между витками меньше диаметра проволоки в ненагруженном состоянии; - сохранения остаточной работоспособности после разлома (т.е. разлом не приведет к опасному состоянию). Примечание — Предпочтительны пружины сжатия.
Ограниченный диапазон силы и аналогичные параметры	Определите необходимое ограничение в части опыта и применения. Примерами являются распорный болт, тормозная пластина и муфта ограничения крутящего момента. **ВАЖНО. Этот принцип не следует соблюдать, когда важна постоянная целостность компонентов. Это необходимо для поддержания необходимого уровня контроля**
Ограниченный диапазон скоростей и подобных параметров	Определить необходимое ограничение, учитывая опыт и применение. Примерами являются центробежный регулятор, безопасный контроль скорости и ограничение перемещения
Ограниченный диапазон параметров окружающей среды	Определите необходимые ограничения. Примерами являются температура, влажность, загрязнение на месте установки. См. раздел 10 и примите к сведению указания производителя по применению
Ограниченный диапазон времени реакции, ограниченный гистерезис	Определите необходимые ограничения. Рассмотрите, например, усталостное напряжение пружины, трение, смазку, температуру, инерцию при разгоне и торможении, сочетание допусков

Таблица А.3 — Испытанные компоненты

Испытанный компонент	Условия для «испытанного» компонента	Стандарт или технические условия
Винт	Необходимо учитывать все факторы, влияющие на винтовое соединение и применение. См. таблицу А.2	Механические соединения, такие как винты, гайки, шайбы, заклепки, штифты, болты и т. д. стандартизированы
Пружина	См. таблицу А.2, «Использование испытанной пружины»	Технические спецификации для пружинных сталей и других специальных применений приведены в ISO 4960
Кулачковая шайба	Необходимо учитывать все факторы, влияющие на расположение кулачковой шайбы (например, блокировочные устройства). См. таблицу А.2	См. ISO 14119 (блокировочные устройства)
Распорный болт	Необходимо учитывать все факторы, влияющие на применение. См. таблицу А.2	—

Таблица А.4 — Неисправности и исключения неисправностей. Механические устройства, компоненты и элементы (например, кулачковая шайба, ведомый механизм, цепь, зажимное устройство, тормоз, вал, винт, болт, направляющее устройство, подшипник)

Рассматриваемая неисправность	Исключение неисправности	Примечания
Износ/коррозия	Да, в случае тщательно подобранного материала (избыточного) размера, производственного процесса, обработки и надлежащей смазки в соответствии с указанным сроком службы (см. также таблицу А.2)	См. ISO 13849-1:2006, 7.3
Растягивание/ ослабление	Да, в случае тщательно отобранного материала процесса изготовления, средства блокировки и обработки в соответствии с установленным сроком службы (см. также таблицу А.2)	—
Повреждение	Да, в случае тщательно подобранного материала (избыточного) размера, производственного процесса, обработки и надлежащей смазки в соответствии с указанным сроком службы кже таблицу А.2)	—
Деформация при перенапряжении	Да, в случае тщательно подобранного материала (избыточного) размера, обработки и производственного процесса в соответствии с указанным сроком службы (см. также таблицу А.2)	—
Жесткость/ заедание	Да, в случае тщательно подобранного материала (избыточного) размера, производственного процесса, обработки и надлежащей смазки в соответствии с указанным сроком службы (см. также таблицу А.2)	—

Таблица А.5 — Неисправности и исключения неисправностей — Винтовые пружины

Рассматриваемая неисправность	Исключение неисправности	Примечания
Износ/коррозия	Да, при использовании испытанных пружин и тщательно подобранных креплений (см. таблицу А.2)	См. ISO 13849-1:2006, 7.3
Снижение силы за счет схватывания и повреждения		
Повреждение		
Жесткость/застревание		
Ослабление		
Деформация при перенапряжении		

Приложение B
(справочное)

Валидация пневматических систем

Когда пневматические системы используются в сочетании с другими технологиями, следует также учитывать приложение B. Если пневматические компоненты имеют электрическое соединение/управление, следует учитывать соответствующие списки неисправностей в приложении D.

Примечание — Дополнительные требования могут существовать в национальном законодательстве. В таблицах B.1 и B.2 перечислены основные и испытанные принципы безопасности.

Перечень испытанных компонентов не приводится в приложении B к настоящему изданию. Статус «испытанного» в основном зависит от приложения. Компоненты можно охарактеризовать как «испытанные», если они соответствуют ISO 13849-1:2006, 6.2.2 и ISO 4414:2010, разделы 5—7. Испытанный компонент для одних приложений может оказаться неподходящим для других приложений.

В таблицах с B.3 по B.18 перечислены исключения неисправностей и их обоснование. Дополнительные исключения см. в 4.4. Точный момент возникновения неисправности может быть критическим (см. 9.1).

Таблица B.1 — Основные принципы безопасности

Основной принцип безопасности	Примечания
Использование подходящих материалов и надлежащее производство	Выбор материала, методов изготовления и обработки в отношении, например, напряжения, долговечности, эластичности, трения, износа, коррозии, температуры
Правильные размеры и форма	Учитывайте, например, напряжение, деформацию, усталостное напряжение, шероховатость поверхности, допуски и производство
Правильный выбор, комбинация, расположение, сборка и установка компонентов/системы	Используйте указания производителя по применению, например, каталожные листы, инструкции по установке, технические условия, а также установившуюся практику в области машиностроения в аналогичных компонентах/системах
Использование принципа обесточивания	Безопасное состояние достигается за счет отключения энергии на всех соответствующих устройствах. См. основное действие для остановки в ISO 12100:2010, 6.2.11.3. Энергия подводится для начала движения механизма. См. правильный процесс пуска в ISO 12100:2010, 6.2.11.3. Рассмотрите различные режимы, например режим эксплуатации, режим технического обслуживания. Этот принцип не должен использоваться в некоторых приложениях, например, когда потеря пневматического давления создаст дополнительную опасность
Правильное крепление	При применении, например, винтовых замков, фитингов, клейких средств или зажимного кольца учитывайте указания производителя по применению. Перегрузки можно избежать, применяя адекватную технологию нагрузки крутящим моментом
Ограничение давления	Примерами являются предохранительный клапан, редукционный/регулирующий клапан
Ограничение скорости/снижение скорости	Примером является ограничение скорости хода поршневого или дроссельного клапана
Достаточное предотвращение загрязнения жидкости	Следует учитывать фильтрацию и отделение твердых частиц и воды в жидкости
Надлежащий диапазон времени переключения	Учитывайте, например, длину труб, давление, мощность выхлопа, силу, усталостное напряжение пружины, трение, смазку, температуру, инерцию при ускорении и торможении, а также комбинацию допусков

Окончание таблицы В.1

Основной принцип безопасности	Примечания
Устойчивость к условиям окружающей среды	Сконструируйте оборудование таким образом, чтобы оно могло работать во всех ожидаемых условиях и в любых предсказуемых неблагоприятных условиях, например температура, влажность, вибрация, загрязнение. См. раздел 10 и учитывайте технические характеристики/примечания производителя
Защита от самопроизвольного запуска	Учитывайте самопроизвольный пуск, вызванный накопленной энергией, а также после восстановления питания для различных режимов, например, режим эксплуатации, режим технического обслуживания. Может потребоваться специальное оборудование для высвобождения накопленной энергии (см. ISO 14118:2000, 5.3.1.3). Специальные применения (например, для сохранения энергии для зажимных устройств или обеспечения положения) необходимо рассматривать по отдельности
Упрощение	Избегайте ненужных компонентов в системе безопасности
Правильный температурный диапазон	Необходимо учитывать во всей системе
Разделение	Разделение функций безопасности от других функций (например, логическое разделение)

Таблица В.2 — Испытанные принципы безопасности

Испытанный принцип безопасности	Примечания
Сверхзаданные параметр или показатели безопасности	Показатели безопасности приводятся в стандартах или устанавливаются на основании имеющегося опыта в их безопасном применении
Безопасное положение	Подвижная часть детали удерживается в одном из возможных положений механическими средствами (одного трения недостаточно). Для изменения положения необходимо применить силу
Увеличенная сила отключения	Одним из решений может быть то, что отношение площади для перемещения выключателя в безопасное положение (положение «ВЫКЛ») будет значительно больше, чем для перемещения выключателя в положение «ВКЛ» (коэффициент безопасности)
Клапан, закрывающийся под давлением	Обычно это относится к клапанам пневмоаппаратов, например, тарельчатые клапаны, шаровые клапаны. Следует учитывать давление нагрузки, чтобы клапан оставался закрытым, даже если, например, сломается пружина, закрывающая клапан
Положительное механическое воздействие	Положительное механическое воздействие используется для движущихся частей внутри пневматических компонентов. См. также таблицу А.2
Множественные элементы	См. таблицу А.2
Использование испытанной пружины	См. таблицу А.2
Ограничение скорости/снижение скорости сопротивлением заданному потоку	Примерами являются фиксирующая дроссельная шайба, фиксирующий дроссель
Ограничение силы/уменьшение силы	Это может быть достигнуто с помощью сброса давления испытанного клапана, который, например, оснащен испытанной пружиной, имеет правильные размеры и корректно выбран
Соответствующий диапазон рабочих условий	Следует учитывать ограничения рабочих условий, например, диапазон давления, скорости потока и температурный диапазон

Окончание таблицы В.2

Испытанный принцип безопасности	Примечания
Надлежащее предотвращение загрязнения жидкости	Учитывать необходимость высокой степени фильтрации и отделения твердых частиц и воды в жидкости
Достаточное принудительное закрытие поршневого клапана	Принудительное перекрытие обеспечивает функцию остановки и предотвращает недопустимые движения
Ограниченный гистерезис	Например, повышенное трение или комбинация допусков увеличат гистерезис

Таблица В.3 — Неисправности и исключения неисправностей. Направляющие пневмораспределители

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение времени переключения	Да, в случае принудительного механического воздействия (см. таблицу А.2) движущихся компонентов, если приводная сила достаточно велика	—
Непереключение (застревание в конечном или нулевом положении) или неполное переключение (застревание в произвольном промежуточном положении)	Да, в случае положительного механического воздействия (см. таблицу А.2) движущихся компонентов, если приводная сила достаточно велика	
Самопроизвольное изменение исходного положения переключения (без входного сигнала)	Да, в случае положительного механического воздействия (см. таблицу А.2) движущихся компонентов, если удерживающая сила достаточно велика или если используются испытанные пружины (см. таблицу А.2) и применяются нормальные условия установки и эксплуатации (см. примечание), или в случае использования переключателей с эластичной перемычкой и при нормальных условиях установки и эксплуатации (см. примечание)	Нормальные условия установки и эксплуатации применяются, когда: - учтены условия, установленные изготовителем; - вес подвижного компонента не оказывает неблагоприятного воздействия на безопасность (например, горизонтальная установка); - отсутствуют силы инерции, отрицательно воздействующие на движущиеся компоненты (например, направление движения компонента клапана учитывает величину и направление сил инерции), и отсутствие экстремальных вибрационных и ударных нагрузок.
Утечка	Да, в случае применения переключателей с эластичной перемычкой, при наличии достаточного принудительного перекрытия [см. примечание 1)], применяются нормальные условия эксплуатации, и обеспечивается достаточная очистка и фильтрация сжатым воздухом; или, в случае применения клапанного пневмоаппарата, если применяются нормальные условия эксплуатации [см. примечание 2)] и обеспечивается достаточная обработка и фильтрация сжатым воздухом	1) В случае применения переключателей с эластичной перемычкой возможно исключение утечек. Однако небольшая утечка может произойти в течение длительного периода времени. 2) Нормальные условия эксплуатации применяются, когда учитываются условия, установленные изготовителем.

Окончание таблицы В.3

Рассматриваемая неисправность	Исключение неисправности	Примечания
Если функции управления реализуются рядом однофункциональных клапанов, то анализ неисправностей должен быть выполнен для каждого клапана. Та же процедура должна быть выполнена в случае управляемых клапанов		
Изменение скорости потока утечки в течение длительного периода использования	Нет	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также поломка/трещина крепежных или установочных винтов	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	
Для вспомогательных и пропорциональных клапанов: пневматические неисправности, вызывающие неконтролируемое поведение	Да, в случае вспомогательных и пропорциональных направляющих клапанов, если они могут быть оценены с точки зрения технической безопасности как обычные направляющие пневмораспределители, благодаря их форме и конструкции	—
Если функции управления реализуются рядом однофункциональных клапанов, то анализ неисправностей должен быть выполнен для каждого клапана. Та же процедура должна быть выполнена в случае управляемых клапанов		

Таблица В.4 — Неисправности и исключения неисправностей. Запорные (отсечные) клапаны/невозвратные (обратные) клапаны/быстродействующие выпускные клапаны/регулирующие клапаны и т. д.

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение времени переключения	Нет	
Неоткрытие, неполное открытие, незакрытие или неполное закрытие (застревание в конечном положении или в случайном промежуточном положении)	Да, если система управления подвижным компонентом(-ами) с конструирована так же, как и для пневморегулятора непрерывного действия с шаровыми клапанами без тормозной системы (см. примечание), и, если используются испытанные пружины (см. таблицу А.2)	Для пневморегулятора непрерывного действия с шаровыми клапанами без тормозной системы, система управления, как правило, сконструирована таким образом, чтобы не существовала вероятность застревания подвижного компонента
Самопроизвольное изменение исходного положения переключения (без входного сигнала)	Да, при нормальных условиях установки и эксплуатации (см. примечание), а также при наличии достаточного закрывающего усилия в зависимости от предусмотренных давлений и площадей	Нормальные условия установки и эксплуатации соблюдаются, когда: - выполняются условия, установленные производителем; - на движущиеся компоненты не действуют никакие силы инерции, например, направление движения учитывает ориентацию движущихся частей машины; - отсутствие экстремальных вибрационных или ударных нагрузок
Для регулируемых клапанов: одновременное закрытие обоих входных соединений	Да, если, исходя из конструкции и проекта подвижного элемента, одновременное закрытие маловероятно	—

Окончание таблицы В.4

Рассматриваемая неисправность	Исключение неисправности	Примечания
Утечка	Да, если применяются нормальные условия эксплуатации (см. примечание) и осуществляется достаточная очистка и фильтрация сжатым воздухом	Нормальные условия эксплуатации применяются, когда учитываются условия, установленные изготовителем
Изменение скорости потока утечки в течение длительного периода использования	Нет	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также поломка/трещина крепежных или нажимных винтов	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	

Таблица В.5 — Неисправности и исключения неисправностей. Клапаны управления потоком

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение скорости потока без каких-либо изменений в установочном устройстве	Да, для клапанов управления потоком с неподвижными элементами [см. примечание 1)], например, дроссельных клапанов, если применимы нормальные условия эксплуатации [см. примечание 2)], и обеспечена достаточная очистка и фильтрация сжатым воздухом	1) Основное устройство не предусматривает движение элементов. Изменение расхода зависит от разницы давлений, имеет физическое ограничение для этого типа распределителя и является незащищенным как предполагаемая неисправность. 2) Нормальные условия эксплуатации применяются, когда учитываются условия, установленные изготовителем
Изменение скорости потока в случае нерегулируемых круглых отверстий и форсунок	Да, если диаметр ≥ 0,8 мм, применяются нормальные условия эксплуатации [см. примечание 2)], и если обеспечивается достаточная обработка и фильтрация сжатым воздухом	
Для пропорциональных клапанов управления потоком: изменение скорости потока из-за непреднамеренного изменения заданного значения	Нет	—
Непосредственное изменение в установочном устройстве	Да, где есть эффективная защита установочного устройства, адаптированная к конкретному случаю, на основании технических условий безопасности	
Непреднамеренное ослабление (отвинчивание) рабочего элемента(ов) установочного устройства	Да, если предусмотрено эффективное принудительное блокирующее устройство в случае ослабления (отвинчивания)	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также поломка/разлом крепежных или установочных винтов	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	

Таблица В.6 — Неисправности и исключения неисправностей. Клапаны давления

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неоткрытие или недостаточное открытие при превышении заданного давления (застревание или застой подвижного компонента) [см. примечание 1)]	Да, если: - система управления подвижным(и) компонентом(ами) аналогична методике пневморегулятора непрерывного действия с шаровым или мембранным клапаном [см. примечание 2)], например, для редукционного клапана со вторичным сбросом давления и - установлены испытанные пружины (см. таблицу А.2)	1) Эта неисправность проявляется только тогда, когда клапан(ы) давления используется для принудительных действий, например, для зажима. Эта неисправность не проявляется при обычном функционировании таких клапанов в пневматических системах, например, ограничение давления, снижение давления. 2) Для пневморегулятора непрерывного действия с шаровым или мембранным клапаном, система управления, как правило, сконструирована таким образом, чтобы не было вероятности застревания движущихся элементов
Незакрытие или недостаточное закрытие при падении давления ниже установленного значения (застревание или застой подвижного компонента) [см. примечание 1)]		
Изменение режима регулирования давления без изменения установочного устройства [см. примечание 1)]	Да, для клапанов ограничения давления прямого действия и клапанов переключения давления, если установлены испытанные пружины (см. таблицу А.2)	
Для пропорциональных клапанов давления: изменение режима регулирования давления из-за непреднамеренного изменения заданного значения [см. примечание 1)]	Нет	
Непосредственное изменение в установочном устройстве	Да, где есть эффективная защита установочного устройства в соответствии с требованиями применения, например, запайка ввода	—
Непреднамеренное отвинчивание рабочего элемента установочного устройства	Да, если предусмотрено эффективное принудительное блокирующее устройство в случае отвинчивания	
Утечка	Да, для клапанов пневмоаппаратов, мембранных клапанов и регулируемых клапанов с эластичной перемычкой в нормальных условиях эксплуатации (см. примечание) и при условии достаточной обработки и фильтрации сжатым воздухом	Нормальные рабочие условия выполняются, когда соблюдаются условия, установленные изготовителем
Изменение расхода при утечке при длительном использовании	Нет	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также поломка/разрыв установки или корпуса крепежных соединений	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	

Таблица В.7 — Неисправности и исключения неисправностей. Трубопроводы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв и утечка	Да, если размеры, выбор материалов и крепление соответствуют надлежащей инженерной практике (см. примечание)	При использовании пластиковых труб, необходимо учитывать данные производителя, в частности, в отношении эксплуатационных воздействий окружающей среды, например, термические воздействия, химические воздействия или воздействия радиации. При использовании стальных труб, не обработанных антикоррозионным средством, особенно важно обеспечить достаточную осушку сжатым воздухом
Неисправность на соединителе (например, отрыв, утечка)	Да, при использовании врезных фитингов или труб с резьбой (например, стальные фитинги, стальные трубы), и если размеры, выбор материалов, изготовление, конфигурация и крепление соответствуют надлежащей инженерной практике	—
Закупорка (блокировка)	Да, для трубопроводов в силовой цепи. Да, для контрольно-измерительных трубопроводов, если номинальный диаметр ≥ 2 мм	
Скручивание пластиковых труб с малым номинальным диаметром	Да, если они должным образом защищены и установлены, принимая во внимание соответствующие данные производителя, например, минимальный радиус изгиба	

Таблица В.8 — Неисправности и исключения неисправностей. Шланговые установки

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв, отрыв в месте крепления фитинга и протечка	Да, если в шланговых установках используются шланги, изготовленные в соответствии с ISO 4079-1, или аналогичные шланги (см. примечание) с соответствующими фитингами для шлангов	Исключение неисправности не рассматривается, когда: - истек предполагаемый срок службы; - произошло изменение усталостных характеристик; - произошло внешнее повреждение
Закупорка (блокировка)	Да, для шланговых трубопроводов силовой цепи, а в случае контрольно-измерительных шлангов в сборе, если номинальный диаметр ≥ 2 мм	—

Таблица В.9 — Неисправности и исключения неисправностей. Соединения

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв, поломка винтов или срыв резьбы	Да, если размеры, выбор материала, изготовление, конфигурация и соединение с трубопроводом и/или фитингами для труб/шлангов соответствуют надлежащей инженерной практике	—
Утечка (потеря герметичности)	Нет	Исключение дефектов невозможно, если в течение длительного времени эксплуатации произошли износ, старение, ухудшение эластичности и т. д. Внезапная серьезная неисправность в герметичности не допускается
Закупорка (блокировка)	Да, для применения в силовых цепях и, в случае контрольно-измерительных соединителей, если номинальный диаметр ≥ 2 мм	—

Таблица В.10 — Неисправности и исключения неисправностей. Датчики давления и преобразователи давления

Рассматриваемая неисправность	Исключение неисправности	Примечания
Потеря или изменение герметичности или маслопроницаемости напорных камер	Нет	—
Разрыв напорных камер, а также разлом соединений или крышек креплений	Да, если размеры, выбор материала, конфигурация и крепление соответствуют надлежащей инженерной практике	

Таблица В.11 — Неисправности и исключения неисправностей. Обработка сжатым воздухом. Фильтры

Рассматриваемая неисправность	Исключение неисправности	Примечания
Закупорка фильтрующего элемента	Нет	—
Разрыв или частичный порыв фильтрующего элемента	Да, если фильтрующий элемент достаточно устойчив к давлению	
Повреждение индикатора загрязненности или устройства для контроля загрязненности	Нет	
Разрыв корпуса фильтра или разлом крепежных или соединительных элементов	Да, если размеры, выбор материала, расположение в системе и крепление соответствуют надлежащей инженерной практике	

Таблица В.12 — Неисправности и исключения неисправностей. Обработка сжатым воздухом. Лубрикаторы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение заданного значения (объема масла в единицу времени) без изменения установочного устройства	Нет	—
Самопроизвольное изменение в установочном устройстве	Да, если обеспечена эффективная защита установочного устройства, адаптированная к конкретному случаю	
Непреднамеренное развинчивание рабочего элемента установочного устройства	Да, при применении эффективных блокирующих устройств, предохраняющих от развинчивания	
Разрыв корпуса или разлом крышки, фиксирующего или соединительного элементов	Да, если размеры, выбор материалов, расположение в системе и крепление соответствуют надлежащей инженерной практике	

Таблица В.13 — Неисправности и исключения неисправностей. Обработка сжатым воздухом. Глушители

Рассматриваемая неисправность	Исключение неисправности	Примечания
Блокировка (закупорка) глушителя	Да, если проект и конструкция элемента глушителя соответствует примечанию	Закупорка элементов глушителя и (или) увеличение выхлопов из-за повышенного давления до критических значений являются маловероятными в случае, если глушитель имеет достаточно большой диаметр и разработан с учетом условий эксплуатации

Таблица В.14 — Неисправности и исключения неисправностей. Аккумуляторы и баллоны со сжатым газом

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разлом или разрыв аккумулятора или баллона со сжатым газом или соединителей, либо истирание резьбы крепежных элементов	Да, если конструкция, выбор оборудования, выбор материалов и расположение в системе соответствуют надлежащей инженерной практике	—

Таблица В.15 — Неисправности и исключения неисправностей. Датчики

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неисправный датчик (см. примечание)	Нет	Датчики в этой таблице предназначены для приема сигнала, обработки данных, выхода сигнала и в особых случаях для давления, расхода воздуха, температуры и т. д.
Изменение обнаруживающих или выводных характеристик	Нет	—

Таблица В.16 — Неисправности и исключения неисправностей. Обработка информации. Логические элементы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неисправный логический элемент (например, элемент «И», элемент «ИЛИ», логический элемент запоминающего устройства), например из-за изменения времени переключения, отказа при переключении или неполного переключения	Для соответствующих предположений о неисправностях и исключений неисправностей см. таблицы В.3, В.4 и В.5 и соответствующие связанные компоненты	—

Таблица В.17 — Неисправности и исключения неисправностей. Обработка информации. Реле времени

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неисправное реле времени, например, пневматические и пневмомеханическое реле времени и вычислительные элементы	Да, для реле времени без подвижных компонентов, например, с постоянным сопротивлением, если применимы нормальные условия эксплуатации (см. примечание) и обеспечена достаточная очистка и фильтрация сжатым воздухом	Нормальные рабочие условия выполняются, когда соблюдаются условия, установленные изготовителем
Изменение характеристик определения и выхода		
Разрыв корпуса или разлом соединений или крышек креплений	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	—

Таблица В.18 — Неисправности и исключения неисправностей. Обработка информации. Преобразователи

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неисправный преобразователь [см. примечание 1)]	Да, для преобразователей без подвижного компонента, например, автоматический переключатель, если применимы нормальные условия эксплуатации [см. примечание 2)] и обеспечена соответствующая очистка и фильтрация сжатым воздухом	1) Сюда относятся, например, преобразование пневматического сигнала в электрический, определение положения (цилиндрических переключателей, автоматических переключателей), усиление пневматических сигналов. 2) Нормальные рабочие условия выполняются при соблюдении условий, установленных изготовителем
Изменение характеристик на входе или выходе		
Разрыв корпуса или разлом крепежных элементов	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	

Приложение С
(справочное)

Валидация гидравлических систем

Когда гидравлические системы используются в сочетании с другими технологиями, следует также учитывать приложение С. Если гидравлические компоненты имеют электрическое соединение/управление, следует учитывать соответствующие списки неисправностей в приложении D.

Примечание — Дополнительные требования могут существовать в национальном законодательстве.

В таблицах С.1 и С.2 перечислены основные и испытанные принципы безопасности. Следует избегать пузырьков воздуха и кавитации в гидравлической жидкости, поскольку они могут создавать дополнительные опасности, например, непреднамеренные движения.

Перечень испытанных компонентов не приводится в приложении С к настоящему изданию. Статус «испытанного» в основном зависит от приложения. Компоненты можно охарактеризовать как «испытанные», если они соответствуют ISO 13849-1:2006, 6.2.2 и ISO 4414:2010, разделы 5—7. Испытанный компонент для одних приложений может оказаться неподходящим для других приложений.

В таблицах С.3—С.12 перечислены исключения неисправностей и их обоснование. Дополнительные исключения см. в 4.4. Точный момент возникновения неисправности может быть критическим (см. 9.1).

Таблица С.1 — Основные принципы безопасности

Основной принцип безопасности	Примечания
Использование подходящих материалов и надлежащее производство	Следует сделать правильный выбор материала, технологии изготовления и обработки с учетом, например, напряжения, долговечности, эластичности, трения, износа, коррозии, температуры, гидравлической жидкости
Правильный выбор параметров и формы	Следует учитывать, например, напряжение, деформацию, усталостное напряжение, неровность поверхности, допуски, производство.
Правильный выбор, комбинирование, размещение, монтаж и установка элементов, системы	Используйте указания производителя по применению, например, каталожные листы, инструкции по установке, спецификации и надлежащую инженерную практику в аналогичных компонентах/системах
Применение принципа передачи энергии	Безопасное состояние достигается при отключении энергии в соответствующих устройствах. См. основное действие для остановки в ISO 12100:2010, 6.2.11.3. Для приведения механизма в движение подается энергия. См. основное действие для запуска в ISO 12100:2010, 6.2.11.3. Рассмотрите различные режимы, например режим работы, режим обслуживания. Этот принцип нельзя использовать в некоторых случаях, например, когда потеря гидравлического давления создает дополнительную опасность
Правильное скрепление	При использовании винтов, фурнитуры, клейких средств, зажимных колец следует учитывать рекомендации изготовителя по применению. Перегрузки можно избежать, применяя адекватную технологию нагрузки крутящим моментом
Ограничение давления	Примерами являются клапан сброса давления, редукционный клапан, клапан регулирования давления
Ограничение/снижение скорости	Примером является ограничение скорости хода поршневого клапана или дроссельного клапана
Обоснование избежания загрязнения жидкости	Следует учитывать фильтрацию и отделение твердых частиц и воды в жидкости. Также следует учитывать необходимые указания служб, занимающихся фильтрацией жидкости

Окончание таблицы С.1

Основной принцип безопасности	Примечания
Надлежащий диапазон времени переключения	Необходимо, например, учитывать длину труб, давление, способность выхлопов, силу, усталостное напряжение пружин, трение, смазку, температуру, вязкость, инерцию во время ускорения и замедления, сочетание допусков
Устойчивость к условиям окружающей среды	Следует конструировать оборудование таким образом, чтобы оно могло работать во всех ожидаемых условиях и в любых предсказуемых неблагоприятных условиях, например температура, влажность, вибрация, загрязнение. См. раздел 10 и примите к сведению спецификации производителя и указания по применению
Защита от самопроизвольного запуска	Следует учитывать самопроизвольный пуск, вызванный сохранившейся остаточной энергией, а также после восстановления питания для различных режимов, например, режима работы, режима обслуживания. Может потребоваться специальное оборудование для высвобождения накопленной энергии. Специальные применения (например, для сохранения энергии для зажимных устройств или обеспечения положения) необходимо рассматривать по отдельности
Упрощение	Избегайте ненужных компонентов в системе безопасности
Правильный температурный диапазон	Необходимо учитывать во всей системе
Разделение	Разделение функций, связанных с безопасностью, от других функций

Таблица С.2 — Испытанные принципы безопасности

Испытанный принцип безопасности	Примечания
Сверхзаданные параметры, показатель безопасности	Показатели безопасности приводятся в стандартах или устанавливаются на основании имеющегося опыта в их безопасном применении
Безопасное положение	Подвижная часть элемента безопасности перемещается в одно из необходимых положений при помощи механических средств (одно трение является недостаточным). Для изменения положения необходимо применить силу
Увеличенная сила выключения	Один из способов решения: соотношение площади для переключения выключателя в безопасное положение (положение «выключено») должно значительно превышать площадь для переключения выключателя в положение «включено» (фактор безопасности)
Клапан, закрывающийся под давлением нагрузки	Примерами являются клапаны и картриджи гидроаппаратов. Следует учитывать применение давления для того, чтобы клапан, находящийся в состоянии равновесия, закрывался даже при поломке пружины
Положительное механическое воздействие	Положительное механическое воздействие используется для движущихся частей внутри гидравлических компонентов. См. также таблицу А.2.
Составные части	См. таблицу А.2
Использование испытанной пружины	См. таблицу А.2
Ограничение скорости/снижение скорости за счет сопротивления заданному потоку	Примерами являются фиксирующая дроссельная шайба, фиксирующий дроссель

Окончание таблицы С.2

Испытанный принцип безопасности	Примечания
Ограничение силы/уменьшение силы	Это может быть достигнуто с помощью испытанного клапана сброса давления, который, к примеру, оснащен испытанной пружиной, имеет правильные размеры и корректно выбран
Соответствующий диапазон рабочих условий	Следует учитывать ограничения рабочих условий, например диапазон давления, скорости потока и температурный диапазон
Мониторинг состояния жидкости	Следует учитывать высокую степень фильтрации/отделения твердых частиц/воды в жидкости. Следует также учитывать химические/физические условия жидкости. Рассмотрение указаний на необходимость обслуживания фильтра
Обоснованное принудительное закрытие поршневого клапана	Принудительное закрытие обеспечивает функцию остановки и предупреждает нежелательные движения
Ограниченный гистерезис	Например, увеличение трения повышает гистерезис. Комбинация допусков также повлияет на гистерезис

Таблица С.3 — Неисправности и исключения неисправностей. Управляемые гидрораспределители

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение времени переключения	Да, в случае положительного механического воздействия (см. таблицу А.2) движущихся компонентов, если приводное усилие достаточно велико; или, в случае нераскрытия специального картриджа клапанного гидрораспределителя, если при необходимости отработанный клапан заменяется другим для регулирования основного потока жидкости [см. примечание 1)]	1) Специальные особенности картриджа клапанного гидрораспределителя достигаются, если: - активная зона для безопасного переключения движения составляет как минимум 90 % всей площади подвижного элемента (клапана гидрораспределителя);
Непереключение (застревание на конечном или нулевом положении) или неполное переключение (застревание в случайном промежуточном положении)	Да, в случае положительного механического воздействия (см. таблицу А.2) на подвижные элементы, если приложено достаточно большое усилие, или Да, в случае нераскрытия специального картриджа клапанного гидрораспределителя, если при необходимости отработанный клапан заменяется другим для регулирования основного потока жидкости [см. примечание 1)]	- давление, действующее на активную зону в системе регулирования, должно возрастать за счет увеличения до максимума рабочего давления (в соответствии с ISO 5598:2008, 3.2.429) в клапанном гидрораспределителе; - давление, действующее на участке, расположенном в активной зоне подвижных элементов системы регулирования, сводится к очень низкому значению в сравнении с максимальным рабочим давлением, например противодавление при давлении в кранах сброса воды или давление в области нагнетания при применении всасывающих или наполнительных клапанов; - подвижный элемент (клапан гидрораспределителя) оснащен пазами с периферийной балансировкой; - управляемые клапаны в этих клапанных гидрораспределителях выполнены по проекту как часть коллектора гидросистемы (т. е. без шланговых установок и труб для соединений с этими клапанами)

Окончание таблицы С.3

Рассматриваемая неисправность	Исключение неисправности	Примечания
Самопроизвольное изменение начального положения переключения (без входного сигнала)	Да, в случае положительного механического воздействия (см. таблицу А.2) движущихся компонентов, если удерживающая сила достаточно велика; или если используются испытанные пружины (см. таблицу А.2) и применяются нормальные условия монтажа и эксплуатации [см. примечание 2)]; или, в случае нераскрытия специального картриджа клапанного гидрораспределителя, если при необходимости отработанный клапан заменяется другим для регулирования основного потока жидкости (см. графу примечания 1) и при применении нормальных условий установки и эксплуатации [см. примечание 2)]	2) Нормальные условия установки и эксплуатации применяются, когда: - учтены условия, установленные изготовителем; - вес подвижного компонента не оказывает неблагоприятного воздействия на безопасность, например, при горизонтальной установке; - на движущиеся компоненты не воздействуют никакие специальные силы инерции (например, направление движения учитывает их ориентацию); - отсутствие экстремальных вибрационных и ударных нагрузок
Утечка	Да, в случае применения клапанного гидрораспределителя при соблюдении нормальных условий установки и эксплуатации (см. примечание), а также имеется достаточная система фильтрации	Нормальные условия установки и эксплуатации применяются, когда учитываются условия, предусмотренные производителем
Изменение скорости потока утечки в течение длительного периода использования	Нет	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также разлом крепежных или установочных винтов	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	—
Для вспомогательных и пропорциональных клапанов: неисправности гидравлики, вызывающие неконтролируемое поведение	Да, в случае вспомогательных и пропорциональных распределителей, если они могут быть оценены с точки зрения безопасности как направляющие гидрораспределители по форме и конструкции	—
Если функции управления реализуются рядом функциональных клапанов, то анализ неисправностей должен быть выполнен для каждого клапана. Такая же процедура должна выполняться в случае испытываемых клапанов		

Таблица С.4 — Неисправности и исключения неисправностей. Запорные (отсечные) клапаны, невозвратные (обратные) клапаны, регулирующие клапаны и др.

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение времени переключения	Нет	
Неоткрытие, неполное открытие, незакрытие или неполное закрытие (застревание в конечном положении или в произвольном промежуточном положении)	Да, если руководство системы подвижных элементов разработано аналогично методике гидрорегулятора непрерывного действия с шаровыми клапанами без тормозной системы (см. примечание), и если используются испытанные пружины (см. таблицу А.2)	Руководство для гидрорегулятора непрерывного действия с шаровыми клапанами без тормозной системы обычно разрабатывается так, чтобы не существовала вероятность застревания подвижных элементов
Самопроизвольное изменение начального положения переключения (без входного сигнала)	Да, для нормальных условий установки и эксплуатации (см. примечание), а также при наличии достаточного закрывающего усилия в зависимости от предусмотренных давлений и площадей	Нормальные условия установки и эксплуатации соблюдаются, когда: - соблюдены условия, установленные изготовителем, и - на движущиеся компоненты не действуют особые силы инерции, например, направление движения учитывает ориентацию движущихся частей машины; - отсутствие экстремальных вибрационных или ударных нагрузок
Для регулируемых клапанов: одновременное закрытие обоих входных разъемов	Да, если на основании конструкции и проекта подвижных элементов одновременное закрывание является маловероятным	
Утечка	Да, если применимы нормальные условия эксплуатации (см. примечание) и обеспечена достаточная система фильтрации	Нормальные условия эксплуатации применяются, когда учитываются условия, установленные изготовителем
Изменение скорости движения струи при утечке в течение длительного периода использования	Нет	—
Разрыв корпуса клапана корпуса или поломка подвижного(ых) компонента(ов), а также разлом крепежных или установочных винтов	Да, если конструкция, определение размеров и установка соответствуют надлежащей инженерной практике	

Таблица С.5 — Неисправности и исключения неисправностей. Клапаны гидрораспределителей

Рассматриваемая неисправность	Исключение неисправности	Примечания
Изменение скорости потока без изменения в установочном устройстве	Да, в случае применения гидрораспределителей с неподвижными элементами [см. примечание 1)], например, дроссельные клапаны, если применяются нормальные условия эксплуатации [см. примечание 2)] и имеется соответствующая система фильтрации [см. примечание 3)]	1) Установочное устройство не считается движущейся частью. Изменения скорости потока из-за изменений перепада давления и вязкости в этом типе клапана физически ограничены и не покрываются этой предполагаемой ошибкой. 2) Нормальные рабочие условия выполняются при соблюдении условий, установленных изготовителем. 3) Если в гидрораспределителе применяется невозвратный клапан, тогда должны быть учтены все предполагаемые неисправности невозвратных клапанов
Изменение скорости потока в случае нерегулируемых круговых отверстий и форсунок	Да, если диаметр > 0,8 мм, применяются нормальные условия работы [см. примечание 2)] и обеспечивается достаточная система фильтрации	
Для пропорциональных клапанов расхода: изменение скорости потока из-за непреднамеренного изменения заданного значения	Нет	—
Самопроизвольное изменение в установочном устройстве.	Да, если имеется эффективная защита установочного устройства, адаптированного к конкретному случаю, основанному на технической(их) спецификации(ях) безопасности	—
Непреднамеренное ослабление (развинчивание) рабочего элемента(ов) установочного устройства	Да, если предусмотрено эффективное принудительное блокирующее устройство в случае ослабления (развинчивания)	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также поломка или разлом крепежных или установочных винтов	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	—

Таблица С.6 — Неисправности и исключения неисправностей. Клапаны давления

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неоткрытие или недостаточное открытие (в пространстве и времени) при превышении установленного давления (застревание или застой подвижных элементов) [см. примечание 1)]	Да, в случае нераскрытия специального картриджа клапанного гидрораспределителя, если при необходимости отработанный клапан заменяется другим для регулирования основного потока жидкости [см. примечание 1)] в таблице С.3); или если руководство системы подвижных элементов разработано аналогично методике гидрорегулятора непрерывного действия с шаровым клапаном без тормозного устройства (см. графу примечания 2) или если установленные пружины являются испытанными (см. таблицу А.2)	1) Эта неисправность проявляется только тогда, когда клапаны давления используются для вынужденных действий, например для остановки и регулирования опасных явлений, таких как временная приостановка под нагрузкой. Эта неисправность не проявляется при нормальном функционировании гидравлических систем, например ограничении давления, падении давления. 2) Для гидрорегулятора непрерывного действия с шаровым клапаном без тормозного устройства руководство системы обычно разрабатывается таким образом, чтобы не было вероятности застревания движущихся элементов

Окончание таблицы С.6

Рассматриваемая неисправность	Исключение неисправности	Примечания
Незакрытие или недостаточное закрытие (в пространстве и времени), если давление падает ниже установленного значения (застревание или застой подвижных элементов) [см. примечание 1)]	—	—
Изменение режима регулирования давления без изменения установочного устройства [см. примечание 1)]	Да, в случае предохранительных клапанов прямого действия, если установлены испытанные пружины (см. таблицу А.2)	—
Для пропорциональных клапанов давления: изменение режима регулирования давления из-за непреднамеренного изменения установленного значения [см. примечание 1)]	Нет	—
Непосредственное изменение в установочном устройстве	Да, если имеется эффективная защита установочного устройства, адаптированная к конкретному случаю с точки зрения технической безопасности (например, запайка ввода)	—
Непреднамеренное развинчивание рабочего элемента установочного устройства	Да, если предусмотрено эффективное принудительное блокирующее устройство в случае отвинчивания	—
Утечка	Да, для клапанов гидроаппаратов, если применяются нормальные рабочие условия (см. примечание), и если имеется достаточная система фильтрации	Нормальные условия эксплуатации применяются, когда учитываются условия, установленные изготовителем
Изменение расхода при утечке в течение длительного периода использования	Нет	—
Разрыв корпуса клапана или поломка подвижного(ых) компонента(ов), а также поломка или разрыв установки или корпуса крепежных соединений	Да, если конструкция, размеры и установка соответствуют надлежащей инженерной практике	—

Таблица С.7 — Неисправности и исключения неисправностей. Металлические трубопроводы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв и утечка	Да, если размеры, выбор материалов и крепление соответствуют надлежащей инженерной практике	—
Поломка в соединениях (например, порыв, утечка)	Да, если используются приварные фитинги, приварные фланцы или развальцовочные фитинги, а также размеры, выбор материалов, производство, конфигурация и крепление соответствуют передовой инженерной практике	—
Закупорка (блокировка)	Да, для трубопроводов в силовой цепи и для контрольно-измерительных трубопроводов, если номинальный диаметр ≥ 3 мм	—

Таблица С.8 — Неисправности и исключения неисправностей. Шланговые установки

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв, отрыв в месте крепления фитинга и утечка	Нет	—
Закупорка (блокировка)	Да, для шланговых трубопроводов в силовой цепи, и при контроле и измерении шлангов, если номинальный диаметр ≥ 3 мм.	

Таблица С.9 — Неисправности и исключения неисправностей. Соединения

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв, поломка винтов или срыв резьбы	Да, если размеры, выбор материала, изготовление, конфигурация и подключение к трубопроводу и/или к компоненту жидкостной технологии соответствуют надлежащей инженерной практике	—
Утечка (потеря герметичности)	Нет (см. примечание)	Исключение дефектов невозможно, если в течение длительного времени эксплуатации произошли износ, старение, ухудшение эластичности и т. д. Непредвиденная серьезная неисправность в герметичности не допускается
Закупорка (блокировка)	Да, для применения в силовой цепи, а также для контроля и измерения соединителей, если номинальный диаметр ≥ 3 мм	—

Таблица С.10 — Неисправности и исключения неисправностей. Фильтры

Рассматриваемая неисправность	Исключение неисправности	Примечания
Закупорка фильтрующего элемента	Нет	—
Разрыв фильтрующего элемента	Да, если фильтрующий элемент достаточно устойчив к давлению и имеет эффективный перепускной клапан, либо обеспечивается эффективный мониторинг загрязнения	
Выход из строя перепускного клапана	Да, если система управления перепускным клапаном сконструирована аналогично методике гидрорегулятора непрерывного действия с шаровым клапаном без тормозного устройства (см. таблицу С.4), и если используются испытанные пружины (см. таблицу А.2)	
Повреждение индикатора загрязненности или устройства для контроля загрязненности	Нет	
Разрыв корпуса фильтра или разлом крепежных или соединительных элементов	Да, если размеры, выбор материала, расположение в системе и крепление соответствуют надлежащей инженерной практике	

Таблица С.11 — Неисправности и исключения неисправностей. Накопитель энергии

Рассматриваемая неисправность	Исключение неисправности	Примечания
Разрыв, разлом приспособления для накопления энергии или крепежных соединений, а также истирание резьбы	Да, если конструкция, выбор оборудования, выбор материалов и размещение в системе соответствуют надлежащей инженерной практике	—
Утечка в разделяющем элементе между газом и рабочей жидкостью	Нет	
Выход из строя/поломка разделяющего элемента между газом и рабочей жидкостью	Да, если это цилиндр (поршень) (см. примечание)	Не следует рассматривать внезапную крупную утечку
Выход из строя заправочного клапана на стороне газа	Да, если заправочный клапан установлен в соответствии с надлежащей инженерной практикой и если обеспечена достаточная защита от внешних воздействий	—

Таблица С.12 — Неисправности и исключения неисправностей. Датчики

Рассматриваемая неисправность	Исключение неисправности	Примечания
Неисправный датчик (см. примечание)	Нет	Датчики в этой таблице предназначены для приема сигнала, обработки данных, выхода сигнала и в особых случаях для давления, расхода воздуха, температуры и т. д.
Изменение характеристик обнаружения или вывода	Нет	—

Приложение D
(справочное)

Валидация электрических систем

D.1 Общие положения

Когда электрические системы используются в сочетании с другими технологиями, следует также учитывать приложение D.

Условия окружающей среды IEC 60204-1 применяются к процессу валидации. Если указаны другие условия окружающей среды, их также следует учитывать.

В таблицах D.1 и D.2 перечислены основные и испытанные принципы безопасности.

Компоненты, перечисленные в таблице D.3, считаются «испытанными», если они соответствуют описанию, данному в ISO 13849-1:2006, 6.2.4. Стандарты, перечисленные в таблице D.3, можно использовать для демонстрации их пригодности и надежности для конкретного применения. Испытанный компонент для одних приложений может оказаться неподходящим для других приложений.

Примечание — Сложные электронные компоненты, такие как программируемые логические контроллеры (PLC), микропроцессоры и специализированные интегральные схемы, не могут считаться эквивалентными «испытанным» компонентам.

В разделе D.2 и таблицах D.4—D.18 перечислены исключения неисправностей и их обоснование. Дополнительные исключения см. в 4.4.

Для проверки следует учитывать как постоянные неисправности, так и кратковременные нарушения.

Точный момент возникновения неисправности может быть критическим (см. 9.1).

Таблица D.1 — Основные принципы безопасности

Основной принцип безопасности	Примечания
Использование подходящих материалов и качественное производство	Следует сделать правильный выбор материала, методов изготовления и обработки в отношении, например, напряжения, долговечности, эластичности, трения, износа, коррозии, температуры, электропроводности, диэлектрической прочности
Правильные размеры и форма	Следует учитывать, например, напряжение, деформацию, усталость, шероховатость поверхности, допуски, изготовление
Правильный выбор, комбинирование, размещение, монтаж и установка элементов, системы	Используйте указания производителя по применению, например, каталожные листы, инструкции по установке, спецификации и надлежащую инженерную практику
Правильное защитное соединение	Одна сторона цепи управления, одна клемма рабочей катушки каждого электромагнитного устройства или одна клемма другого электрического устройства подключены к цепи защитного заземления (см. IEC 60204), 1:2005, 9.4.3.1)
Контроль изоляции	Использование устройства контроля изоляции, которое либо указывает на замыкание на землю, либо автоматически прерывает цепь после замыкания на землю (см. IEC 60204-1:2005, 6.3.3)
Отключение питания	Безопасное состояние достигается путем отключения питания во всех соответствующих устройствах, например, путем использования нормально замкнутых (NC) контактов для входов (кнопочных и переключателей с нормально разомкнутыми контактами (NO), контактов для реле (см. также ISO 12100:2010, 6.2.11.3). Исключения могут существовать в некоторых приложениях, например, когда потеря электропитания создает дополнительную опасность. Функции временной задержки могут быть необходимы для достижения безопасного состояния системы (см. IEC 60204-1:2005, 9.2.2)

Окончание таблицы D.1

Основной принцип безопасности	Примечания
Подавление помех	Следует применять устройства подавления помех (дистанционное управление, диоды, регулируемые сопротивления) параллельно нагрузке, исключая непараллельное соединение. Примечание — Диод увеличивает время выключения.
Сокращение времени срабатывания	Необходимо сводить к минимуму время срабатывания отключения питания элементами переключения
Совместимость	Используйте компоненты, совместимые с применяемыми напряжением и током
Устойчивость к условиям окружающей среды	Следует конструировать оборудование так, чтобы оно могло работать во всех ожидаемых условиях и в любых прогнозируемых неблагоприятных условиях, например, при температуре, влажности, вибрации и электромагнитных помехах (EMI) (см. раздел 10)
Безопасная установка входных устройств	Следует применять безопасные входные устройства, например, блокирующие переключатели, позиционные выключатели, концевые выключатели, бесконтактные выключатели, чтобы положение, выравнивание и допуск переключения сохранялись при всех ожидаемых условиях, например, при вибрации, нормальном износе, попадании посторонних предметов, температуре. См. ISO 14119:1998, раздел 5
Защита от самопроизвольного пуска	Предупреждение самопроизвольного пуска, например, после восстановления подачи питания (см. ISO 12100:2010, 6.2.11.4, ISO 14118, IEC 60204-1)
Защита цепи управления	Цепь управления должна быть защищена в соответствии с IEC 60204-1:2005, 7.2 и 9.1.1
Последовательное переключение для схемы последовательных контактов резервных сигналов	Во избежание отказа по общей причине привариванием обоих контактов, включение и выключение не происходит одновременно, так что один контакт всегда переключается без тока

Таблица D.2 — Испытанные принципы безопасности

Испытанный принцип безопасности	Примечания
Положительное механическое соединение контактов	Следует использовать положительное механическое соединение контактов, например, для функции контроля в системах категорий 2, 3 и 4 (см. EN 50205, IEC 60947-4-1:2001, приложение F, IEC 60947-5-1:2003 + A1:2009, приложение L)
Предотвращение неисправности кабеля	Чтобы избежать короткого замыкания между двумя соседними проводниками: - используйте экранированный кабель, подключенный к цепи защитного заземления на каждом отдельном проводнике; - в плоских кабелях используйте один заземленный проводник между каждым сигнальным проводником
Интервал	Используйте достаточное расстояние между клеммами положения, компонентами и проводкой, чтобы избежать непреднамеренных подключений
Ограничение подачи энергии	Использование конденсатора для подачи конечного количества энергии, например, при применении регуляторов
Ограничение электрических параметров	Ограничение напряжения, тока, энергии или частоты для ограничения движения, например, ограничение крутящего момента, удержание в рабочем состоянии с ограничением смещения/времени, снижение скорости во избежание опасного состояния

Окончание таблицы D.2

Испытанный принцип безопасности	Примечания
Непредсказуемое состояние	Следует избегать непредсказуемых состояний в системах управления. Необходимо прогнозировать и планировать проектирование и конструирование системы управления так, чтобы обеспечить нормальную эксплуатацию, а также рабочие условия, например производительность
Приведение в действие	Прямое действие передается посредством формы (и без усилия) с неэластичными элементами, например, при помощи пружины между рукояткой привода и контактами (см. ISO 14119:1998, 5.1, ISO 12100:2010, 6.2.5)
Ориентация режима отказа	Там, где это возможно, устройство/схема должны перейти в безопасное положение или состояние
Ориентированный режим отказа	Компоненты или системы, ориентированные на режим отказа, должны использоваться везде, где это возможно (см. ISO 12100:2010, 6.2.12.3)
Сверхзаданные параметры	В целях безопасности следует использовать снижение значений следующих параметров: - ток, проходящий через переключаемые контакты, должен быть меньше половины их номинального тока; - частота переключения компонентов должна быть менее половины их номинального значения; - общее количество ожидаемых переключений должно быть не более 10 % электрического ресурса устройства. Примечание — Снижение номинальных характеристик может зависеть от обоснования проектного решения.
Сведение к минимуму возможности возникновения неисправностей	Разделение функции безопасности на другие функции
Баланс между сложными и простыми процессами	Следует установить баланс между: - сложными процессами для достижения более совершенного управления и - простыми процессами для достижения большей надежности

Таблица D.3 — Испытанные элементы

Испытанный компонент	Дополнительные условия для «испытаний»	Стандарт или технические условия
Переключатели с приведением в действие положительным воздействием (прямое действие включения), например: - кнопка; - позиционный переключатель; - кулачковый управляемый переключатель, например, для более эффективного включения	—	IEC 60947-5-1:2003, приложение K
Устройство аварийной остановки	—	ISO 13850 IEC 60947-5-5
Предохранитель	—	IEC 60269-1
Автоматический выключатель	—	IEC 60947-2
Выключатели, разъединители	—	IEC 60947-3
Дифференциальный выключатель/RCD (устройство защитного отключения)	—	IEC 60947-2:2006, приложение B

Продолжение таблицы D.3

Испытанный компонент	Дополнительные условия для «испытаний»	Стандарт или технические условия
Главный контактор	Считается испытанным, только если: a) учитываются другие воздействия, например вибрация; б) неисправности можно избежать с помощью соответствующих методов, например завышения размеров (см. таблицу D.2); в) ток нагрузки ограничивается устройством тепловой защиты; г) цепи защищены устройством защиты от перегрузки. Примечание — Исключение неисправности невозможно.	IEC 60947-4-1
Устройство или оборудование управления и защитного переключения (CPS)	—	IEC 60947-6-2
Вспомогательный контактор (например, реле контактора)	Испытания подтверждаются, если: a) были учтены другие влияния, например, вибрация; b) используется положительное воздействие от напряжения; c) согласно соответствующей методике были исключены повреждения, например, возникшие из-за сверхзаданных параметров (см. таблицу D.2); d) ограничение тока в контактах, за исключением сварных контактов, осуществляется плавким предохранителем или масляным выключателем; e) используемые для контроля контакты функционируют под положительным механическим воздействием. Примечание — Исключение неисправности невозможно.	EN 50205 IEC 60947-5-1 IEC 60947-4-1:2001, приложение F
Реле	Испытания подтверждаются, если: a) были учтены другие влияния, например вибрация, и b) используется положительное воздействие от напряжения, и c) согласно соответствующей методике были исключены повреждения, например, возникшие из-за сверхзаданных параметров (см. таблицу D.2), и d) ограничение тока в контактах, за исключением сварных контактов, осуществляется плавким предохранителем или масляным выключателем. Примечание — Исключение неисправности невозможно.	IEC 61810-1 IEC 61810-2
Трансформатор		IEC 61558
Кабель	Поверхность укладываемого кабеля должна быть защищена от механических повреждений (включая, например, вибрацию или изгиб)	IEC 60204-1:2005, раздел 12

Окончание таблицы D.3

Испытанный компонент	Дополнительные условия для «испытаний»	Стандарт или технические условия
Штепсельная вилка и розетка	—	Согласно электрическому стандарту, соответствующему предполагаемому применению. Для блокировки см. также ISO 14119
Температурный переключатель		По электротехнике см. EN 60730-1
Переключатель давления	—	По электротехнике см. IEC 60947-5-1. По давлению см. приложения B и C
Соленоидный клапан	—	—

D.2 Исключение неисправностей

D.2.1 Общие положения

Исключение неисправности действительно только в том случае, если детали работают в пределах своих указанных номинальных характеристик.

D.2.2 «Оловянные усы»

Если применяются бессвинцовые процессы и продукты, могут возникнуть электрические короткие замыкания из-за роста «оловянных усов». Эту возможность следует оценивать и учитывать при применении исключения неисправности «короткое замыкание» любого компонента. Например, если риск роста «оловянных усов» считается высоким, то исключение неисправности «короткое замыкание резистора» бесполезно, так как необходимо учитывать замыкание между контактами этого компонента.

Примечания

1 Рост «оловянных усов» — это явление, связанное, главным образом, с отделкой из чистого блестящего олова. Игольчатые выступы могут достигать нескольких сотен микрометров в длину и могут вызывать короткое замыкание. Преобладающая теория состоит в том, что «усы» вызваны накоплением напряжения сжатия в оловянном покрытии.

2 Ссылки [34] и [35] могут быть полезны для оценки этого явления.

3 Об «усах» на печатных платах до сих пор не сообщалось. Дорожки обычно состоят из меди без оловянного покрытия. Контактные площадки могут быть покрыты оловянным сплавом, но производственный процесс, по-видимому, не стимулирует склонность к росту «усов».

D.2.3 Короткие замыкания на частях, установленных на печатной плате

Короткие замыкания для деталей, смонтированных на печатной плате (PCB), могут быть исключены только в том случае, если выполнено исключение неисправности «короткое замыкание между двумя соседними дорожками/контактными площадками», описанное в таблице D.5.

D.2.4 Исключение неисправностей и интегральные схемы

Так как невозможно исключить неисправности, которые могут вызвать неисправность интегральной схемы (см. таблицы D.20 и D.21), единичная неисправность может привести к потере функции безопасности (включая ее проверку/испытание), реализованной в единой интегральной схеме. Следовательно, маловероятно, что многоканальная функциональность, необходимая для отказоустойчивости и/или требований по обнаружению категорий 2, 3 или 4, может быть достигнута с использованием одной интегральной схемы, если только она не удовлетворяет специальным требованиям к архитектуре IEC 61508-2:2010, приложение E.

Таблица D.4 — Неисправности и исключения неисправностей. Провода/кабели

Рассматриваемая неисправность	Исключение неисправности	Примечания
Короткое замыкание между любыми двумя проводами	Короткого замыкания можно избежать, если провода являются: - постоянно соединенными (скрепленными) и защищенными от внешнего повреждения, например, в канальной системе для кабелей, в арматуре; - отдельными многожильными кабелями; - находящимися внутри электроизоляции (см. примечание); - индивидуально защищенными заземлением	При условии, что и провода и корпус удовлетворяют соответствующим требованиям (см. IEC 60204-1)
Короткое замыкание любого провода к открытой проводящей части или к земле, или к защитному проводнику	Короткие замыкания между проводом и любой открытой проводящей частью в электрическом корпусе (см. примечание)	
Обрыв цепи на любом проводе	Нет	—

Таблица D.5 — Неисправности и исключения неисправностей. Печатные платы/узлы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Короткое замыкание между двумя смежными проводниками в дорожках, колодках	Исключение короткого замыкания между смежными проводниками в соответствии с примечаниями	В качестве базового материала используется как минимум EP GC согласно IEC 60893-1. Воздушные зазоры и пути утечки соответствуют, по крайней мере, IEC 60664-5 (IEC 60664-1 для сечения более 2 мм) со степенью загрязнения 2/категорией перенапряжения III; если обе дорожки снабжаются от источника питания SELV/PELV, применяется степень загрязнения 2/категория перенапряжения II с минимальным зазором 0,1 мм. Собранная плата монтируется в корпус, обеспечивающий защиту от токопроводящих загрязнений, например, корпус со степенью защиты не менее IP54, а печатная сторона (стороны) покрыта стойким к старению лаком или защитным слоем, покрывающим все дорожки проводников. Примечания 1 Опыт показал, что паяльные маски удовлетворительны в качестве защитного слоя. 2 Дополнительное покрытие защитным слоем в соответствии с IEC 60664-3 может уменьшить пути утечки и размеры воздушных зазоров
Обрыв цепи на любой дорожке	Нет	—

Таблица D.6 — Неисправности и исключения неисправностей. Контактная колодка

Рассматриваемая неисправность	Исключение неисправности	Примечания
Короткое замыкание между смежными контактами	Короткое замыкание между смежными контактами в соответствии с примечаниями 1) или 2)	1) Используемые контакты и соединения находятся в соответствии с IEC 60947-7-1 или IEC 60947-7-2 и требования IEC 60204-1:2006, 13.1.1, удовлетворены. 2) Конструкция должна обеспечивать предупреждение от короткого замыкания, например, посредством формирования усадки в точке изгиба сквозь изолированную трубку
Обрыв цепи в отдельных контактах	Нет	—

Таблица D.7 — Неисправности и исключения неисправностей. Многоразъемное соединение

Рассматриваемая неисправность	Исключение неисправности	Примечания
Короткое замыкание между любыми двумя смежными разъемами	Короткое замыкание между смежными разъемами в соответствии с примечанием. Если разъем смонтирован на печатной плате, применяются положения таблицы D.5	С помощью наконечников или других подходящих средств для многожильных проводов. Пути утечки и воздушные зазоры, а также все прерывания должны быть рассчитаны как минимум в соответствии с IEC 60664-1 с категорией перенапряжения III
Перестановка или неправильная установка разъема, если для этого не предусмотрено устройство автоматической защиты	Нет	—
Короткое замыкание любого провода (см. примечание) на землю или токопроводящую часть или на защитный провод	Нет	Жила кабеля является проводящей частью многоразъемного соединения
Обрыв цепи в отдельных разъемах	Нет	—

Таблица D.8 — Неисправности и исключения неисправностей. Переключатели. Электромеханический позиционный переключатель, ручной переключатель (например, кнопка, переключатель возвратного действия, переключатель типа DIP, магнитоуправляемые контакты, язычковый переключатель, реле давления, датчик температуры)

Рассматриваемая неисправность	Исключение неисправности	Примечания
Контакт не замыкается	Устройства, чувствительные к давлению в соответствии с ISO 13856	—
Контакт не размыкается	Ожидается, что контакты в соответствии с IEC 60947-5-1:2003, приложение K, разомкнутся	—
Короткое замыкание между смежными контактами, изолированными друг от друга	Короткое замыкание может быть исключено для переключателей в соответствии с IEC 60947-5-1 (см. примечание)	Токопроводящие части не должны соприкасаться между собой изоляцией
Одновременное короткое замыкание между тремя периодически переключаемыми контактами	Одновременные короткие замыкания могут быть исключены для переключателей в соответствии с IEC 60947-5-1 (см. примечание)	

Окончание таблицы D.8

Для PL e, исключение неисправностей по механическим (например, механической связи между исполнительным механизмом и контактным элементом) и электрическим аспектам не допускается. В этом случае необходимо резервирование. Для устройств аварийной остановки в соответствии с IEC 60947-5-5, допускается исключение неисправности по механическим аспектам, если учитывается максимальное количество операций
Примечание — Списки неисправностей для механических аспектов рассматриваются в приложении А.

Таблица D.9 — Неисправности и исключения неисправностей. Переключатели. Электромеханические устройства (например, реле, контакторные реле)

Рассматриваемая неисправность	Исключение неисправности	Примечания
Все контакты остаются под напряжением, когда катушка обесточена (например, из-за механической неисправности).	Нет	—
Все контакты остаются в обесточенном положении при подаче питания (например, из-за механической неисправности, обрыва цепи катушки)	Нет	
Контакт не размыкается	Нет	
Контакт не замыкается	Нет	
Одновременное короткое замыкание между тремя периодически переключаемыми контактами	Одновременное короткое замыкание можно исключить, если принять во внимание примечания	Пути утечки и воздушные зазоры соответствуют, по крайней мере, IEC 60664-1 со степенью загрязнения не менее 2/категорией перенапряжения III. Проводящие части, которые ослабевают, не могут соединить изоляцию между контактами и катушкой
Короткое замыкание между двумя парами контактов и/или между контактами и клеммой катушки	Короткое замыкание можно исключить, если учесть примечания	
Одновременное замыкание нормально разомкнутых и нормально замкнутых контактов	Одновременное замыкание контактов можно исключить, если учесть примечание	Необходимо использовать жестко соединенные (или механически соединенные) контакты (см. IEC 60947-5-1:2003, приложение L)

Таблица D.10 — Неисправности и исключения неисправностей. Переключатели. Неконтактные переключатели

Рассматриваемая неисправность	Исключение неисправности	Примечания
Постоянно низкое сопротивление на выходе	Нет (см. примечание)	См. IEC 60947-5-3
Постоянно высокое сопротивление на выходе	Нет (см. примечание)	Должны быть описаны меры по предотвращению неисправностей
Перебои в электроснабжении	Нет	
Переключатель не работает из-за механической неисправности	Не работает из-за механической неисправности, если принять во внимание примечание	Все части выключателя должны быть достаточно хорошо закреплены. Механические аспекты см. в приложении А
Короткое замыкание между тремя клеммами переключателя	Нет	—

Таблица D.11 — Неисправности и исключения неисправностей — переключатели — соленоидные клапаны

Рассматриваемая неисправность	Исключение неисправности	Примечания
Не заряжает энергией	Нет	
Не обесточивается	Нет	
Примечание — Перечни неисправностей для механических аспектов пневматических и гидравлических клапанов рассматриваются в приложениях B и C соответственно.		

Таблица D.12 — Неисправности и исключения неисправностей — дискретные электрические компоненты. Трансформаторы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи в одной из обмоток	Нет	
Короткое замыкание между разными обмотками	Короткое замыкание между разными обмотками можно исключить, если принять во внимание примечания 1) и 2)	1) Должны выполняться требования соответствующих разделов IEC 61558. 2) Между разными обмотками применяется двойная или усиленная изоляция или защитный экран. Применяются испытания в соответствии с IEC 61558-1:2005, раздел 18. Соответствующие тестовые напряжения приведены в IEC 61558-1:2005, таблица 8 a). Короткие замыкания в катушках и обмотках необходимо избегать, принимая соответствующие меры, например: пропитка катушек таким образом, чтобы заполнить все полости между отдельными витками, корпусом катушки и сердечника; использование изолированных и выдерживающих максимальные температурные характеристики жил обмотки. 3) В случае вторичного короткого замыкания не должно происходить нагрева выше заданной рабочей температуры
Короткое замыкание в одной обмотке	Короткое замыкание в одной обмотке можно исключить, если принять во внимание примечание 1)	
Изменение эффективного коэффициента трансформации	Изменение эффективного коэффициента трансформации можно исключить, если принять во внимание замечание 1). См. также примечание 3)	

Таблица D.13 — Неисправности и исключения неисправностей — дискретные электрические компоненты — индукторы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи	Нет	—
Короткое замыкание	Короткое замыкание можно исключить, если принять во внимание примечание	Катушка имеет одно из покрытий, эмалированное или из изолирующего материала, и установлена по оси с осевым сращиванием проводов
Случайное изменение значения $0{,}5\ L_N < L < L_N$ + допуск, где L_N — номинальное значение индуктивности	Нет	В зависимости от типа конструкции могут быть рассмотрены и другие диапазоны

Таблица D.14 — Неисправности и исключения неисправностей — дискретные электрические компоненты — резисторы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи	Нет	
Короткое замыкание	Короткое замыкание можно исключить, если принять во внимание примечание 1) или 2)	1) Применяется резистор пленочного или проволочного типа с защитой, предотвращающей в случае поломки от раскручивания проволоки, установленной по оси с осевым сращиванием проводов и лаковым покрытием. 2) Резисторы в технологии поверхностного монтажа должны быть металлическими тонкопленочными в корпусах типа MELF, мини MELF или μMELF. 3) Например, если риск образования «усов» считается высоким, то исключение неисправности «короткое замыкание резистора» бесполезно, поскольку необходимо учитывать короткое замыкание между контактами этого компонента
Случайное изменение значения $0{,}5\ R_N < R < 2\ R_N$, где R_N — номинальное значение сопротивления [см. также примечание 3)]	Нет	В зависимости от типа конструкции могут быть рассмотрены и другие диапазоны

Таблица D.15 — Неисправности и исключения неисправностей — дискретные электрические компоненты — резисторные схемы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи	Нет	—
Короткое замыкание между любыми двумя контактами	Нет	
Короткое замыкание между любыми контактами	Нет	
Случайное изменение значения $0{,}5\ R_N < R < 2\ R_N$, где R_N — номинальное значение сопротивления	Нет	В зависимости от типа конструкции могут быть рассмотрены и другие диапазоны

Таблица D.16 — Неисправности и исключения неисправностей — дискретные электрические компоненты — потенциометры

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи в одном из соединений	Нет	—
Короткое замыкание между всеми соединениями	Нет	
Короткое замыкание между любыми двумя соединениями	Нет	
Случайное изменение значения $0{,}5\ R_p < R < 2\ R_p$, где R_p — номинальное значение сопротивления	Нет	В зависимости от типа конструкции могут быть рассмотрены и другие диапазоны

Таблица D.17 — Неисправности и исключения неисправностей — дискретные электрические компоненты — конденсаторы

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи	Нет	—
Короткое замыкание	Нет	
Случайное изменение значения $0,5\ C_N < C < C_N$ + допуск, где C_N — номинальное значение емкости	Нет	В зависимости от типа конструкции могут быть рассмотрены и другие диапазоны
Изменение значения тангенса, δ	Нет	—

Таблица D.18 — Неисправности и исключения неисправностей — электронные компоненты — дискретные полупроводниковые приборы (например, диоды, полупроводниковые стабилитроны, транзисторы, симисторы, регуляторы напряжения, кварцевые кристаллы, фототранзисторы , светодиоды [LED])

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи в одном из соединений	Нет	—
Короткое замыкание между любыми двумя соединениями	Нет	
Короткое замыкание между всеми соединениями	Нет	
Изменение характеристик	Нет	

Таблица D.19 — Неисправности и исключения неисправностей — электронные компоненты — оптопары

Рассматриваемая неисправность	Исключение неисправности	Примечания
Обрыв цепи в одном из соединений	Нет	—
Короткое замыкание между любыми двумя соединениями на входе	Нет	
Короткое замыкание между любыми двумя соединениями на выходе	Нет	
Короткое замыкание между любыми двумя соединениями на входе и выходе	Короткого замыкания на входе или выходе можно избежать, если выполняется требование	Оптопара построена в соответствии с категорией перенапряжения III согласно IEC 60664-1. Если используется источник питания SELV/PELV, применяется степень загрязнения 2/категория перенапряжения II. Примечание — См. таблицу D.5. Принимаются меры для того, чтобы внутренний отказ оптопары не мог привести к чрезмерному нагреву ее изоляционного материала

Таблица D.20 — Неисправности и исключения неисправностей — электронные компоненты — непрограммируемые интегральные схемы

Рассматриваемая неисправность	Исключения ошибок	Примечания
Обрыв цепи в одном из соединений	Нет	—
Короткое замыкание между любыми двумя соединениями	Нет	
Ошибка типа «постоянная» (т. е. короткое замыкание на 1 и 0 при изолированном входе или отключенном выходе). Статический сигнал «0» и «1» на всех входах и выходах по отдельности или одновременно	Нет	
Побочные колебания на выходах	Нет	
Изменение значений (например, входное/выходное напряжение аналоговых устройств)	Нет	
Примечание — В этой части ISO 13849, ICs с менее чем 1000 элементами и/или менее чем 24 контактами, операционные усилители, сдвиговые регистры и гибридные модули считаются несложными. Это определение произвольно.		

Таблица D.21 — Неисправности и исключения неисправностей — электронные компоненты — программируемые и/или сложные интегральные схемы

Рассматриваемая неисправность	Исключения ошибок	Примечания
Неисправности во всей схеме или в ее отдельной части, включая ошибки программного обеспечения.	Нет	—
Обрыв цепи в одном из соединений	Нет	
Короткое замыкание между любыми двумя соединениями	Нет	
Ошибка типа «постоянная» (т. е. короткое замыкание на 1 и 0 при изолированном входе или отключенном выходе). Статический сигнал «0» и «1» на всех входах и выходах по отдельности или одновременно	Нет	
Побочные колебания на выходах	Нет	
Изменение значения, например, входное/выходное напряжение аналоговых устройств	Нет	
Неустановленные неисправности в аппаратном обеспечении, которые не проявляются из-за сложности интегральных схем	Нет	
Анализ должен выявить дополнительные неисправности, которые следует учитывать, если они влияют на работу функции безопасности		
Примечание — В этой части ISO 13849, IC считается сложной, если она состоит из более чем 1000 элементов и/или более 24 контактов. Это определение произвольно.		

Приложение Е
(справочное)

Пример валидации поведения при неисправности и средства диагностики

Е.1 Общие положения

В этом примере рассматривается проверка PL функции безопасности (SF 1), за исключением требований, относящихся к следующим аспектам PL:

- значения $MTTF_d$;
- отказ по общей причине (CCF);
- программный анализ;
- систематические отказы.

Пример не охватывает валидацию:

- спецификации требований безопасности (см. раздел 7);
- характеристик функций безопасности (см. раздел 8);
- требований окружающей среды (см. раздел 10);
- требований к техническому обслуживанию (см. раздел 11);
- требований к документации (см. раздел 12).

В примере рассматриваются три функции безопасности, SF 1, SF 2 и SF 3.

SF 1 представляет собой связанную с безопасностью функцию останова четырех отдельных приводов машины, инициируемую открытием одного защитного ограждения, и она рассматривается как отдельная функция безопасности для каждого привода (SF 1.0, SF 1.1, SF 1.2 и SF 1.3). Чтобы уменьшить объем примера, проверка была ограничена SF 1.0 и SF 1.3.

В приложении А приведены рекомендации по изучению поведения при неисправности, а также предоставлено диагностическое покрытие данной цепи. Методы, используемые для определения диагностического покрытия, основаны на анализе видов и последствий отказов (FMEA) с учетом ISO 13849-1:2006, приложение Е.

Примечание — Этот пример не охватывает весь процесс валидации SRP/CS. В частности, не рассматривалась необходимая проверка программного обеспечения PLC. Для проверки программного обеспечения, связанного с безопасностью, см. 9.5.

Е.2 Описание машины

Пример основан на сборочном автомате с ручной загрузкой и выгрузкой заготовок. Автомат предназначен для выполнения двух последовательных операций: введения шарика и фиксации винтом на каждой заготовке.

На машине имеется четыре станции: загрузочная, разгрузочная и две рабочие станции (см. рисунок Е.1). Первая рабочая станция представляет собой этап с пневматическим приводом для введения шариков, а второй этап с пневматическим приводом — фиксирующий винт.

Поворотный стол с электроприводом перемещает заготовки вокруг каждой из четырех станций. Заготовки вручную помещаются на держатели заготовок, установленные на поворотном столе, и снимаются с них. Электродвигатель с инверторным управлением приводит в движение планетарную передачу и приводной ремень, который перемещает поворотный стол.

На первой рабочей станции шарик вводится в заготовку с помощью горизонтально установленного пневматического цилиндра, который управляется моностабильным 5/2-ходовым гидрораспределителем (1V1, см. рисунок Е.3). Базовое положение (клапан обесточен) этого цилиндра — отведенное положение. Глубина вставленного шарика контролируется концевым выключателем в полностью выдвинутом положении цилиндра, а приложенное давление прессования контролируется датчиком давления в линии подачи воздуха для выдвижения цилиндра.

Рабочая станция для завинчивания состоит из вертикально установленного бесштокового пневматического цилиндра, на котором закреплен ротационный шуруповерт с пневматическим приводом. Блок шуруповерта поднимается и опускается пневматическим цилиндром, который управляется моностабильным 5/2-ходовым распределительным клапаном (2V1). Базовое положение (клапан обесточен) этого цилиндра — верхнее положение с поднятым блоком шуруповерта. Кроме того, в нижнем штуцере пневматического цилиндра предусмотрен обратный клапан с пилотным управлением (2V2).

Вращательное движение шуруповерта обеспечивается пневматическим двигателем, управляемым моностабильным 5/2-ходовым гидрораспределителем (3V1). Базовым положением (клапан обесточен) этого пневматического двигателя является состояние «ВЫКЛ». Крутящий момент, обеспечиваемый блоком шуруповерта, контролируется датчиком давления в его линии подачи воздуха.

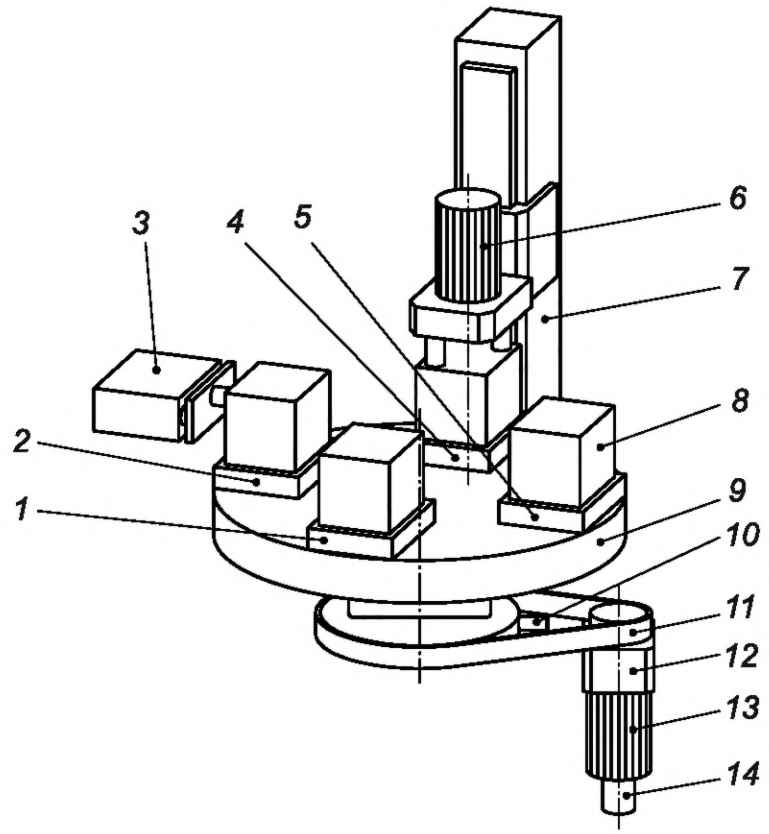
Одиночный цикл машины в автоматическом режиме работы инициируется нажатием кнопки пуска. В начале цикла поворотный стол удерживает три заготовки: (i) только что загруженную заготовку, (ii) частично готовую заготовку (шар вставлен) и (iii) готовую заготовку (шар вставлен и закреплен винтом). Каждый цикл машины состоит из поворота поворотного стола на 90° с последующими одновременными операциями введения шариков и фиксации

винтом вновь загруженных и частично готовых заготовок. Затем машина останавливается, после чего оператор открывает защитное ограждение, чтобы выгрузить готовую заготовку и загрузить новую заготовку. Для завершения обработки заготовки требуется три машинных цикла, чтобы повернуть заготовку на 270° от станции загрузки до станции разгрузки.

Предусмотрены следующие режимы работы:

- автоматический режим с ручной загрузкой и разгрузкой (полный ход машины с закрытым защитным ограждением);
- режим настройки поворотного стола (движение поворотного стола с удерживающим управлением и защитным ограждением в открытом положении).

Станок представляет механическую опасность, возникающую из-за перемещений приводов станка с пневматическим приводом (на рабочих станциях введения шариков и фиксации винтом) и поворотного стола с электрическим приводом. По этой причине он защищен механическими ограждениями, которые являются стационарными, за исключением защитного ограждения, которое обеспечивает доступ к станциям загрузки и разгрузки (опасная зона).



Условные обозначения:

1 — загрузочная станция; *2* — рабочая станция для введения шариков; *3* — цилиндр вставки шарика (A1); *4* — рабочая станция с фиксацией винтом; *5* — разгрузочная станция; *6* — блок шуруповерта (A3); *7* — цилиндр для вставки винта (с вертикальным приводом) (A2); *8* — заготовка; *9* — поворотный стол; *10* — импульсный датчик (G2); *11* — приводной ремень; *12* — планетарная передача; *13* — электродвигатель (M1); *14* — датчик вращения (G1)

Рисунок Е.1 — Машина, используемая в примере: сборочный автомат

Е.3 Спецификация требований к функциям безопасности

В автоматическом режиме работы защита от опасных движений обеспечивается следующей функцией безопасности: SF 1 остановка, связанная с безопасностью, инициированная открытием защитного ограждения и предотвращением неожиданного пуска при открытом защитном ограждении.

Для целей примера это можно рассматривать как отдельную функцию безопасности для каждого из четырех отдельных приводов машины:

SF 1.0 электродвигатель поворотного стола (M1);

SF 1.1 цилиндр вставки шарика (A1);
SF 1.2 цилиндр вставки винта (A2);
SF 1.3 пневмодвигатель шуруповерта (A3).

Примечание — К примеру, связанная с безопасностью остановка и защита от неожиданного пуска считаются одной функцией безопасности, поскольку они реализованы в одной и той же комбинации SRP/CS.

В режиме настройки для поворотного стола с открытым защитным ограждением (механические приводы с пневматическим приводом отключены SF 1.1, SF 1.2 и SF 1.3), безопасное состояние движения поворотного стола достигается комбинацией следующих функций безопасности:
SF 2 безопасно-ограниченная скорость;
SF 3 режим удержания для запуска.

Таблица Е.1 — Активные функции безопасности в зависимости от режима работы

Режим работы	Функция безопасности					
	SF 1.0	SF 1.1	SF 1.2	SF 1.3	SF 2	SF 3
Автоматический режим (блокировочная решетка закрыта)	X	X	X	X		
Режим настройки (защитное ограждение открыто)		X	X	X	X	X
X — активная функция безопасности.						

После проведения оценки риска функциям безопасности были присвоены следующие значения PL_r:
PL_rd для SF1 (безопасная остановка и предотвращение неожиданного пуска);
PL_rd для SF2 (безопасно-ограниченная скорость);
PL_rc для SF3 (режим удержания).

Примечание — Выбор PL_rc для SF3 учитывает его использование в сочетании с SF2, для которого достигается PL d.

Когда запрашивается SF 1, он инициирует следующие действия:
- поворотный стол выполняет контролируемую остановку в соответствии с остановкой категории 2 по IEC 60204-1;
- горизонтально установленный пневматический цилиндр (A1) рабочей станции для введения шариков и вертикально установленный пневматический цилиндр (A2) рабочей станции для фиксации винтом возвращаются в исходное положение и/или остаются в исходном положении (т.е. отведены и подняты соответственно);
- блок шуруповерта (A3) немедленно останавливается.

Примечание — Например, оценка риска показала, что потеря контролируемого замедления поворотного стола в результате неисправности инвертора является допустимой, а перемещение пневматических цилиндров A1 и A2 в исходное положение безопасным.

Минимальное расстояние между защитным ограждением и этими движущимися частями машины было определено в соответствии со стандартом ISO 13855 на основе характеристик остановки машины.

Машина снабжена другими функциями безопасности, такими как аварийная остановка, блокировка повторного пуска, сброс и выбор режимов работы, но они не рассматриваются в примере и, следовательно, соответствующие компоненты не показаны на принципиальных схемах рисунков Е.2 и Е.3.

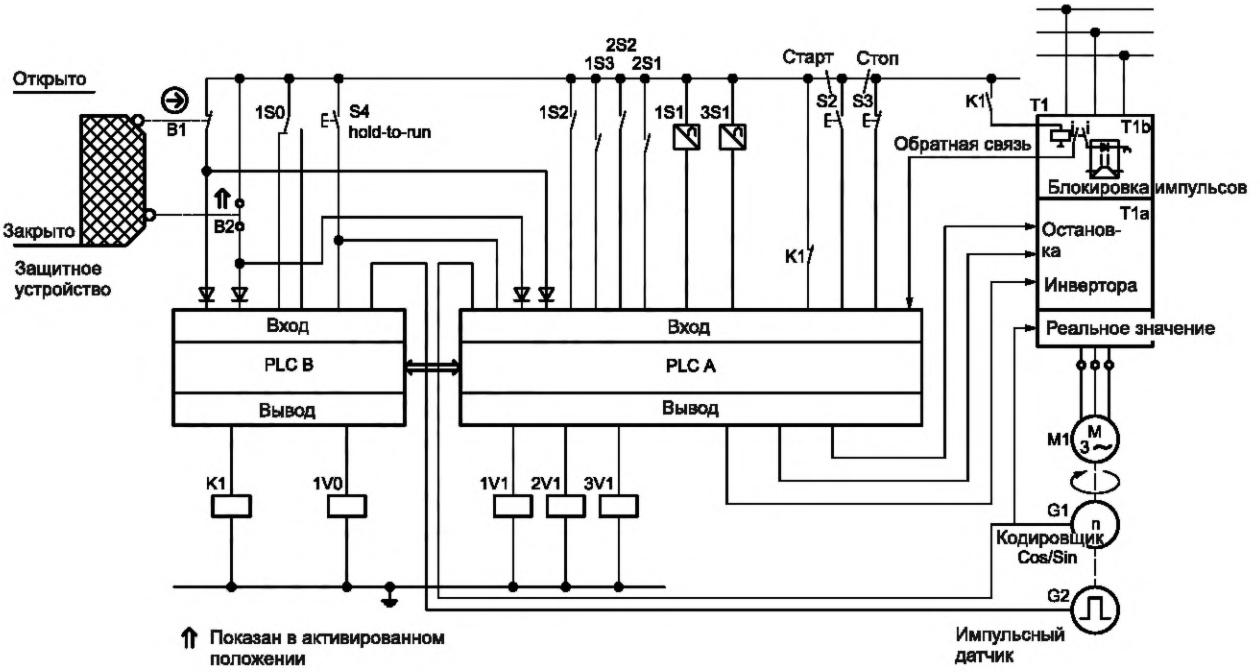


Рисунок E.2 — Автоматическая сборочная машина — принципиальная электрическая схема

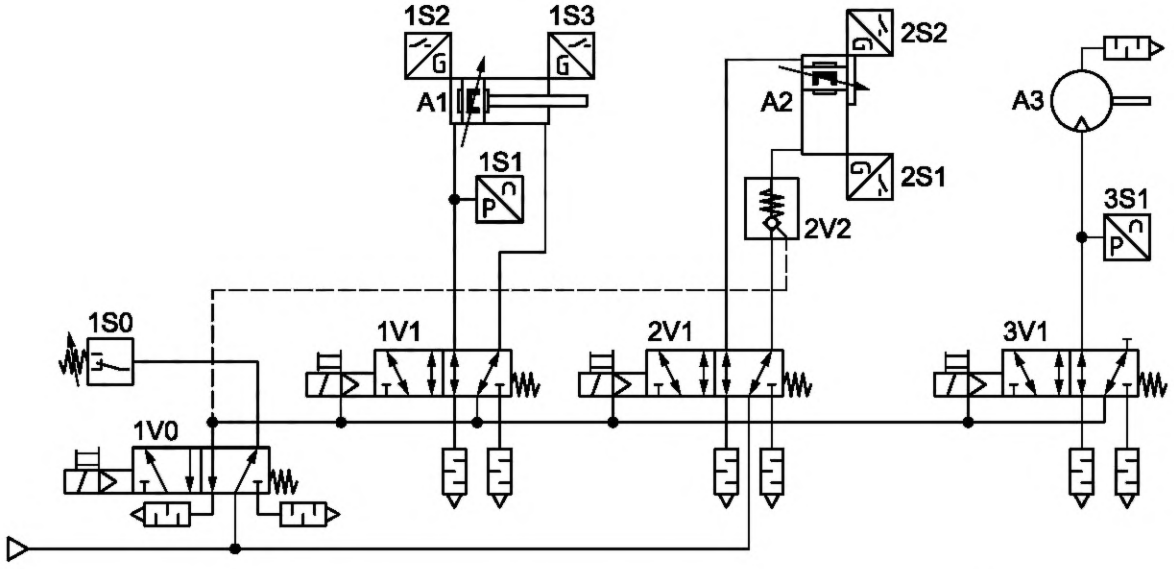


Рисунок E.3 — Автоматическая сборочная машина — схема пневматической цепи

E.4 Проект SRP/CS E.4.1 Общие положения

Система управления для примера была реализована с использованием комбинации электромеханических, электронных и пневматических технологий.

Для достижения PL_r для SF 1 и SF 2 была выбрана категория 3. Поэтому для всех электрических и пневматических частей, связанных с этими функциями безопасности, была принята разнотипная резервная и контролируемая структура (см. рисунки E.2 и E.3).

Для достижения PL_r для SF 3 было выбрано сочетание категорий 2 и 3.

Сигналы от датчиков и механизмов управления (переключатели положения защитной блокировки, кнопка удержания) были продублированы и подключены к двум разным PLC (разные аппаратные средства для PLC A и PLC B), которые обрабатывают их с помощью специальных программных функциональных блоков (SRASW).

Каждый PLC также управляет как инвертором поворотного стола, так и исполнительными механизмами машины с пневматическим приводом через пути переключения, которые не зависят от путей переключения других PLC.

В целях диагностики (перекрестного мониторинга) и синхронизации, два PLC взаимодействуют друг с другом через стандартную шину данных.

Конкретный инвертор в этом примере имеет дополнительное средство (внутреннее реле) для отключения сигналов управления силовыми полупроводниковыми приборами (импульсная блокировка), что можно рассматривать как второй путь отключения [безопасное отключение крутящего момента (STO) в соответствии с IEC 61800-5-2].

Эта функция блокировки импульсов не приводит к быстрой остановке вращающегося двигателя, поскольку отключение инверторного управления двигателем вызывает неконтролируемое замедление. Однако в этом примере блокировка импульсов по-прежнему приводит к остановке поворотного стола до того, как оператор сможет получить доступ к опасной зоне, поэтому контролируемое замедление до состояния покоя, которое обычно предшествует блокировке импульсов, не является обязательной характеристикой SF 1.0.

В пневматической цепи подача воздуха к каждому из приводов машины (A1, A2 и A3) управляется моностабильным 5/2-ходовым направляющим клапаном (1V1, 2V1 и 3V1) электромагнитного типа с пилотным управлением. Импульсный воздух для всех трех клапанов переключается дополнительным клапаном (1V0) того же типа, который обеспечивает резервный канал управления. Состояние этого выпускного клапана контролируется реле давления (1S0). Подача воздуха для A2 осуществляется из основного источника воздуха, а для A1 и A3 — из источника импульсного воздуха (1V0).

Обесточивание приводной камеры от подвижного цилиндра A1 при проникновении в рабочее пространство обеспечивается также двумя каналами:

- стравливания воздуха через 1V1 переключением в нормальное положение;
- обесточивания через 1V0 переключением в нормальное положение. Состояние 1V1 контролируется концевым выключателем (1S2).

Обратный клапан с пилотным управлением (2V2), который также забирает импульсный воздух из 1V0, предусмотрен в нижнем соединении A2 (вертикально установленный бесштоковый пневматический цилиндр). Это обеспечивает резервный канал для остановки движения вниз и удержания привода машины в его основном (верхнем) положении.

Состояние 2V1 контролируется концевым выключателем (2S2).

Подача воздуха для пневматического двигателя A3 (блок шуруповерта) осуществляется из источника импульсного воздуха (1V0), а не из основного источника воздуха. Такое использование 1V0 в дополнение к 3V1 для отключения подачи воздуха к A3 обеспечивает резервный канал управления, который гарантирует, что A3 не будет продолжать вращаться, если 3V1 выйдет из строя во включенном положении. Состояние 3V1 контролируется датчиком давления (3S1), который выдает аналоговый выходной сигнал.

В соответствии с 3 категорией учитываются основные и испытанные принципы безопасности, а также выполняются требования категории B. В частности, требования стандартов IEC 60204 1 и ISO 4414.

Атрибуты компонентов, реализующих SRP/CS, подробно объясняются в таблице E.2.

Таблица E.2 — Атрибуты компонентов, реализующих SRP/CS (список деталей на рисунках E.2 и E.3)

Метка компонента	Функция	Элемент	Атрибут	Испытанный принцип безопасности [a]	Возможное исключение неисправности
B1	Контроль положения защитного ограждения	Блокирующий переключатель	IEC 60947-5-1:2003, включая прямое открытие в соответствии с IEC 60947-5-1:2003, приложение K	Активация принудительного режима	Невозможность размыкания контактов переключателя при срабатывании может быть исключена. Электрические неисправности, так как B1 имеет принудительный режим срабатывания
B2	Контроль положения защитного ограждения	Блокирующий переключатель	IEC 60947-5-1	Нет	Нет
S4	Генерирует удерживающее движение в режиме настройки	Нормально открытый нажимная кнопка		Нет	Нет

Продолжение таблицы Е.2

Метка компонента	Функция	Элемент	Атрибут	Испытанный принцип безопасности [a]	Возможное исключение неисправности
PLCA PLCB	Обработка связанных с безопасностью и не связанных с безопасностью сигналов	Программируемый логический контроллер (PLC)	IEC 61131-1 и IEC 61131-2	Нет	Нет
К1	Генерирует резервный сигнал СТОП для инвертора в случае сбоя в маршруте PLC A	Релейный контактор	IEC 60947-5-1, включая механически соединенные контактные элементы в соответствии с IEC 60947-5-1:2003, приложение L, и EN 50205	Механически соединенные контакты	Нет
Т1	Электродвигатель привода поворотного стола	Инвертор	Инвертор имеет дополнительный маршрут отключения с помощью блокировки импульсов	Реле блокировки с принудительно механически соединенными контактами	Нет
G1	Измеряет скорость электродвигателя поворотного стола	Датчик вращения (кодировщик cos/sin)	—	Нет	Нет
G2	Контролирует движение поворотного стола	Импульсный датчик	—	Нет	Нет
1V0	Воздух системы управления для направляющих клапанов 1V1, 2V1, 3V1 и для обратного клапана 2V2	Электромагнитный клапан управления направлением движения	Пружинный клапан, 5/2-функция, пилотный, внутренняя подача пилотного воздуха, золотниковый клапан с перекрытием	Таблица В.2. Завышение размеров/коэффициент безопасности, безопасное положение (использование испытанной пружины), достаточное принудительное перекрытие в поршневых клапанах	Повышение давления в канале 4 при откачанном канале 5 в нормальном положении, нарушение герметичности из-за выдавливания, перемещение золотника клапана без рабочей мощности
1V1 2V1 3V1	Управление цилиндром вставки шарика А1 Контроль вставки винта цилиндр А2 Управление шуруповертом (пневмодвигатель) А3	См. 1V0	См. 1V0	См. 1V0	См. 1V0

Окончание таблицы Е.2

Метка компонента	Функция	Элемент	Атрибут	Испытанный принцип безопасности [a]	Возможное исключение неисправности
2V2	Устройство защиты от падения для вертикально установленного цилиндра для вставки винта (A2) блока шуруповерта	Обратный клапан	Обратный клапан с управляющим золотником, подпружиненный тарельчатый клапан	Таблица В.2. Клапан закрыт под нагрузкой давление	Открытие без пилотного воздуха
1S0	Контролирует состояние клапана 1V0	Реле давления	Фиксированная точка переключения	Для мониторинга не требуются базовые принципы безопасности (нет функции безопасности)	Нет
1S1 3S1	Контролирует давление, приложенное во время процесса введения шарика. Контролирует крутящий момент (давление), применяемый в процессе завинчивания	Датчик давления	Аналоговый выходной сигнал	Для мониторинга не требуются базовые принципы безопасности (нет функции безопасности)	Нет
1S2, 1S3 2S1, 2S2	Концевые выключатели для цилиндра вставки шарика A1. Концевые выключатели для цилиндра для вставки винта A2	Датчик приближения	Магнитный принцип измерения	Для мониторинга не требуются базовые принципы безопасности (нет функции безопасности)	Нет
A1	Цилиндр вставки шарика	Пневматический цилиндр	Не входит в область действия настоящего стандарта согласно ISO 13849-1:2006, 3.1.1.		
A2	Цилиндр вставки винта	Бесштоковый пневматический цилиндр с внешней направляющей	Не входит в область действия настоящего стандарта согласно ISO 13849-1:2006, 3.1.1.		
A3	Блок шуруповерта	Пневматический двигатель	Не входит в область действия настоящего стандарта в соответствии с ISO 13849-1:2006, 3.1.1.		

[a] Основные принципы безопасности также учитывались при конструировании компонентов (см. таблицу D.1 для электрических компонентов и таблицу В.1 для пневматических компонентов).

Е.4.1 Функция безопасности SF 1 — остановка, связанная с безопасностью, инициируемая открытием защитного ограждения, и предотвращение неожиданного пуска всякий раз, когда защитное ограждение открыто

В соответствии со спецификацией машины, открытие защитного ограждения должно инициировать остановку четырех приводов станка: (i) поворотного стола (приводимого в движение двигателем с инверторным управлением), (ii) цилиндра вставки шарика, (iii) цилиндра вставки винта и (iv) блок шуруповерта. Таким образом, эта функция может быть представлена, как показано на рисунке Е.4.

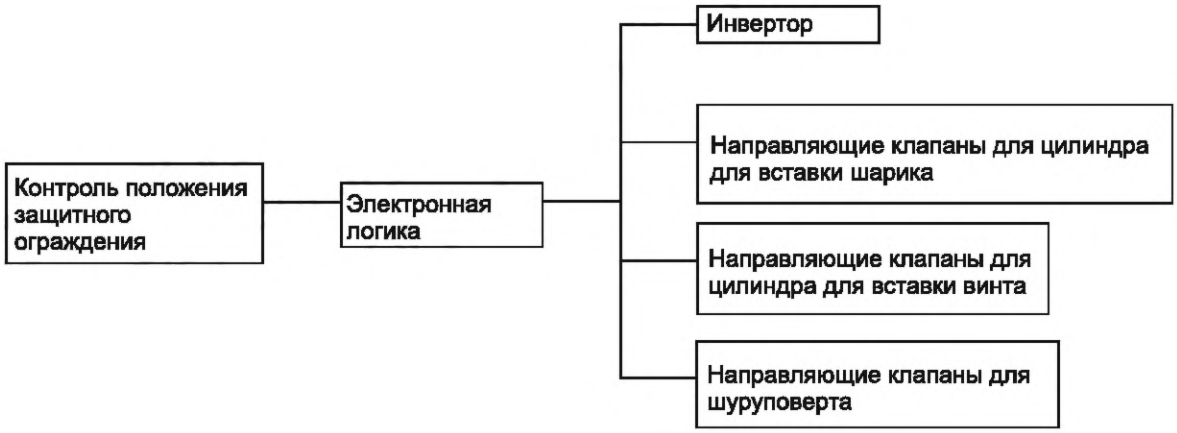


Рисунок Е.4 — Функциональные блоки — SF 1.0, SF 1.1, SF 1.2 и SF 1.3

Когда защитное ограждение открывается, PLC A инициирует остановку поворотного стола, подавая сигнал остановки на инвертор (T1a). PLC B отслеживает результирующее замедление поворотного стола с помощью G2, и когда он обнаруживает, что он достиг полной остановки, он обесточивает K1, чтобы инициировать блокировку импульсов на инверторе (T1b). Если поворотный стол не останавливается из-за ошибки в T1a или PLC A, то PLC B обнаружит эту ошибку и подаст собственный сигнал остановки на инвертор (T1b). Это второй независимый канал для функции остановки. Точно так же выполняется часть функции безопасности, связанная с предотвращением неожиданного пуска.

Открытие защитного ограждения также приводит к тому, что PLC A инициирует первую остановку цилиндра вставки шарика, цилиндра вставки винта и блока шуруповерта путем обесточивания 1V1, 2V1 и 3V1. PLC B инициирует вторую остановку этих трех исполнительных механизмов путем обесточивания 1V0.

Если поворотный стол уже остановлен, но рабочие станции для вставки шариков и фиксации винтов работают, когда защитное ограждение открыто, то PLC A немедленно обесточит 1V1, 2V1 и 3V1, а PLC B немедленно обесточит K1. PLC B также обесточит 1V0 после задержки, чтобы позволить цилиндру вставки шарика (A1) завершить свое перемещение во отведенное положение.

Пока защитное ограждение находится в открытом положении, необходимо убедиться, что неисправность на пути включения PLC A не приведет к неконтролируемому пуску. Это достигается действием PLC B, обесточивающим K1, как только двигатель поворотного стола останавливается, а также обесточивающим 1V0, чтобы предотвратить запуск цилиндра вставки шарика или цилиндра вставки винта.

Оценка PL для SRP/CS, выполняющих SF 1, выполнялась следующим образом:

а) Идентификация элементов безопасности

Элементы безопасности функции остановки SF 1.0 и их разделение на каналы можно проиллюстрировать блок-схемой функции безопасности, показанной на рисунке Е.5.

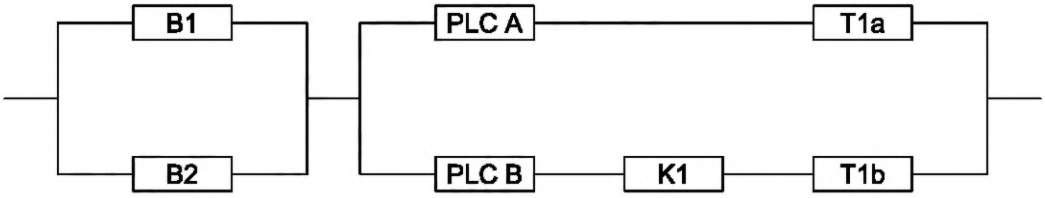
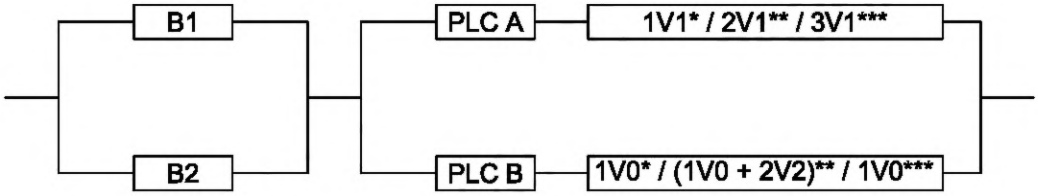


Рисунок Е.5 — Блок-схема функции безопасности — SF 1.0

Точно так же элементы безопасности функций остановки SF 1.1, SF 1.2 и SF 1.3 и их разделение на каналы можно проиллюстрировать блок-схемой функции безопасности, показанной на рисунке Е.6.



* SF 1.1 ** SF 1.2 *** SF 1.3

Рисунок Е.6 — Блок-схема функции безопасности — SF 1.1, SF 1.2 и SF 1.3

Каждая из двух частей схем на рисунках Е.5 и Е.6 может быть сопоставлена с назначенной архитектурой для категории 3, поэтому схемы могут быть упрощены как две SRP/CS (вход, логика/выход), показаны на рисунке Е.7.

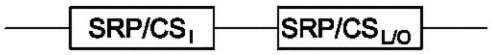


Рисунок Е.7 — Комбинация SRP/CS, выполняющих функции безопасности

Для каждого SRP/CS, PL был оценен с применением упрощенной процедуры, описанной в ISO 13849-1:2006, 4.5.4.

b) Оценка $MTTF_d$ каждого канала

Для оценки значений $MTTF_d$ компонентов использовались данные о надежности, предоставленные производителями.

Для оценки $MTTF_d$ канала был применен метод подсчета частей (см. ISO 13849-1:2006, приложение D). Разнотипная резервная структура приводит к разным значениям $MTTF_d$ для каждого канала, поэтому применение уравнения симметризации дает средний результат 25 лет (средний) для $MTTF_d$ каждого канала как SRP/CSi, так и $SRP/CS_{I/o}$ SF 1.0, SF 1.1, SF 1.2 и SF 1.3 (см. ISO 13849-1:2006, D.2).

c) Оценка DC_{avg}

DC_{avg} был рассчитан как для SRP/CS на основе DC внутреннего теста, так и по способам мониторинга, применяемым к различным компонентам.

Проверка правдоподобия защитных блокирующих переключателей B1 и B2 с помощью PLC A и PLC B в соответствии с ISO 13849-1:2006, приложение Е, приводит к высокому значению DC_{avg} (99 %) для SRP/CS i SF 1.0, SF 1.1, SF 1.2 и SF 1.3.

В SRP/CSI/o SF 1.0, SF 1.1, SF 1.2 и SF 1.3 предусмотрены следующие диагностические мероприятия:

- контроль контактора реле К1 с помощью SF A по положению контактов К1;
- перекрестный мониторинг между SF A и SF B;
- косвенный мониторинг T1a и PLC A с помощью PLC B через G2;
- косвенный контроль самой платы выхода SF A через 1S2, 2S2, 3S1 и G1;
- контроль выполнения программы внутренним «сторожевым» устройством в PLC A и PLC B;
- косвенный мониторинг T1a с помощью PLC от A до G1;
- контроль T1b PLC A по положению контакта реле блокировки импульсов;
- косвенный контроль PLC B со стороны PLC A через положение контактов К1;
- косвенный контроль платы выхода PLC B через 1S0;
- косвенный контроль 1V1 с помощью PLC A через 1S2;
- косвенный контроль 2V1 с помощью PLC A через 2S2;
- косвенный контроль 3V1 с помощью PLC A через 3S1;
- косвенный контроль 1V0 с помощью PLC B через 1S0;
- обнаружение неисправностей PLC A, T1a и 1V1, 2V1 и 3V1 посредством наблюдения за процессом.

В соответствии с ISO 13849-1:2006, приложение Е, эти диагностические меры обеспечивают DC_{avg} средний результат (90 %) для $SRP/CS_L/_O$ SF 1.0, SF 1.1, SF 1.2 и SF 1.3.

d) Оценка мер против отказа по общей причине (CCF)

Подсчитано, что были приняты адекватные меры против отказов по общей причине (разделение, разнообразие, защита от избыточного давления, воздействия окружающей среды) для обоих SRP/CS SF 1.0, SF 1.1, SF 1.2 и SF 1.3, что в соответствии с ISO 13849-1:2006, приложение F дает 75 баллов за каждый SRP/CS.

e) Определение PL для каждого SRP/CS

PL для каждого SRP/CS определяется следующим образом:

- SRP/CS_I SF 1.0, SF 1.1, SF 1.2 и SF 1.3:
- категория 3;
- среднее $MTTF_d$ каждого канала;
- высокий DC_{avg};
- 75 баллов за меры против CCF.

Применение этих значений к ISO 13849-1:2006, Рисунок 5, но с ограничением DC_{avg} средним значением (категория 3), дает результат PL d.

- $SRP/CS_{L/O}$ SF 1.0, SF 1.1, SF 1.2 и SF 1.3:
- категория 3;
- среднее $MTTF_d$ каждого канала;
- средний DC_{avg};
- 75 баллов за меры против CCF.

Применение этих значений к ISO 13849-1:2006, рисунок 5, дает результат PL d.

f) Определение PL для комбинации SRP/CS, выполняющих SF 1.0, SF 1.1, SF 1.2 и SF 1.3.

Согласно ISO 13849-1:2006, 6.3, и принимая во внимание, что отдельные SRP/CS для SF 1.0, SF 1.1, SF 1.2 и SF 1.3 имеют одинаковые значения PL, PL общей комбинации SRP/CS для SF 1.0, SF 1.1, SF 1.2 и SF 1.3 определяется следующим образом:

$$PL_{iow} = d$$

$$M_{ow} = 2$$

Таким образом, PL для комбинации SRP/CS для каждого из SF 1.0, SF 1.1, SF 1.2 и SF 1.3 равен PL d.

Примечание — Расчет результирующего PL путем сложения значений PFH всех подсистем приведет к более точному результату.

g) Систематические отказы

Подсчитано, что к SRP/CS для SF 1.0, SF 1.1, SF 1.2 и SF 1.3 были применены адекватные меры против систематических отказов в соответствии с ISO 13849-1:2006, приложение G.

E.4.2 Функция безопасности SF 2 — безопасное ограничение скорости (SLS)

Когда машина находится в режиме настройки и защитное ограждение находится в открытом положении, поворотный стол может двигаться только с безопасно ограниченной скоростью (SLS), которая измеряется как G1, так и G2. PLC A отслеживает сигнал от G1, а PLC B отслеживает сигнал от G2, при этом оба PLC независимо выполняют сравнение желаемой и фактической скорости. Если скорость не была успешно снижена до предельного значения инвертором T1a, то PLC A может отреагировать, подав сигнал остановки на инвертор (T1a), а PLC B может отреагировать, активировав блокировку импульсов с задержкой на инверторе (T1b) через K1.

a) Идентификация элементов безопасности

Элементы функции безопасности SF 2 и ее разделение на каналы можно проиллюстрировать блок-схемой функции безопасности, показанной на рисунке E.8.

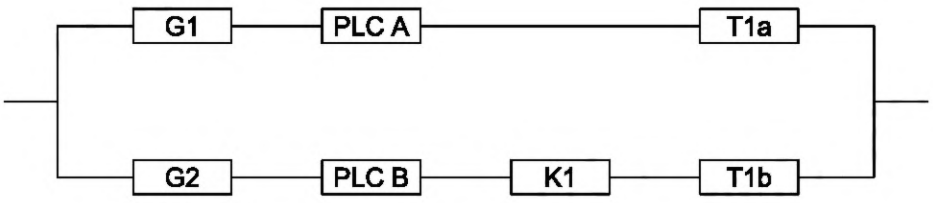


Рисунок E.8 — Блок-схема функции безопасности — SF 2

Для SRP/CS, PL был оценен с применением упрощенной процедуры, описанной в ISO 13849-1:2006, 4.5.4.

Схему можно сопоставить с назначенной архитектурой для категории 3, чтобы функция безопасности выполнялась одним SRP/CS, как показано на рисунке E.9.

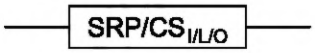


Рисунок E.9 — SRP/CS, выполняющие функцию безопасности SF 2

Для SRP/CS, PL был оценен с применением упрощенной процедуры, описанной в ISO 13849-1:2006, 4.5.4.

b) Оценка $MTTF_d$ каждого канала

Для оценки значений $MTTF_d$ компонентов использовались данные о надежности, предоставленные производителями.

Для оценки $MTTF_d$ канала был применен метод подсчета частей (см. ISO 13849-1:2006, приложение D). Разнотипная резервная структура приводит к неодинаковым значениям $MTTF_d$ для каждого канала, поэтому применение уравнения симметрирования дает средний результат среднего $MTTF_d$ (более 25 лет) для каждого канала SRP/CS.

c) Оценка DC_{avg}

DC_{avg} был рассчитан для SRP/CS на основе DC внутренних испытаний и мер мониторинга, применяемых к различным компонентам.

Предусмотрены следующие диагностические мероприятия:

- контроль контактора реле K1 с помощью PLC A по положению контактов K1;
- перекрестный мониторинг между SF A и SF B;
- косвенный контроль G1, T1a и PLC A с помощью PLC B через G2;
- контроль T1b PLC A по положению контакта реле блокировки импульсов;
- контроль выполнения программы внутренним «сторожевым» устройством в PLC A и PLC B;
- косвенный контроль G2 и PLC B со стороны PLC A через положение контактов K1;
- мониторинг G1 с помощью PLC A;
- мониторинг G1 и T1a (правдоподобие информации sin/cos);
- контроль G2 PLC B (после нажатия S4 PLC B проверяет наличие импульсов от G2, если их нет, PLC B останавливает T1b).

Согласно ISO 13849-1:2006, приложение E, эти диагностические меры обеспечивают средний результат DC_{avg} (90 %) для SRP/CS.

d) Оценка мер против отказа по общей причине (CCF)

Подсчитано, что для SRP/CS были приняты адекватные меры против отказа по общей причине (разделение, разнообразие, защита от избыточного давления, воздействия окружающей среды), что в соответствии с ISO 13849-1:2006, приложение F, приводит к оценке 75 баллов по SRP/CS.

e) Определение PL для SRP/CS

PL для SRP/CS определяется следующим образом:

- категория 3;
- среднее $MTTF_d$ каждого канала;
- средний DC_{avg};
- 75 баллов за меры против CCF.

Применение этих значений к ISO 13849-1:2006, рисунок 5, но с ограничением DC_{avg} средним значением (категория 3), дает результат PL d.

f) Систематические отказы

Подсчитано, что адекватные меры против систематических отказов были применены к SRP/CS в соответствии с ISO 13849-1:2006, приложение G.

E.4.3 Функция безопасности SF 3 — режим автоматического возврата в исходное состояние

Движение поворотного стола (с безопасно ограниченной скоростью) с открытым защитным ограждением начинается и продолжается, пока нажата кнопка S4, и останавливается, когда кнопку отпускают. Когда кнопка находится в отпущенном положении, необходимо предотвратить неожиданный запуск. Сигнал от кнопки S4 обрабатывается обоими PLC.

a) Идентификация элементов безопасности

Элементы функции безопасности SF 3 и их разделение на каналы можно проиллюстрировать с помощью блок-схемы функции безопасности, показанной на рисунке E.10.

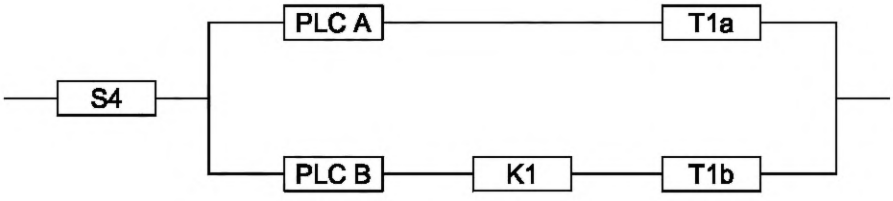


Рисунок E.10 — Блок-схема функции безопасности — SF 3

Каждая из двух частей схемы может быть сопоставлена с назначенной архитектурой для категории 1 и категории 3, поэтому схему можно упростить как две SRP/CS (вход, логика/выход), показанные на рисунке Е.11.

Рисунок Е.11 — Комбинация SRP/CS, выполняющая функцию безопасности SF 3

Для каждого SRP/CS был оценен PL с применением упрощенной процедуры, описанной в ISO 13849-1:2006, 4.5.4.

b) Оценка $MTTF_d$ каждого канала

$MTTF_d$ для SRP/CS_i (кнопка удержания и запуска) рассчитывается с использованием значения производителя #10d, что дает результат высокого $MTTF_d$.

Оценка $MTTF_d$ SRP/CSl/o дает, как и SRP/CSl/o SF 1.0, средний результат 25 лет (средний) для $MTTF_d$ (более 25 лет) каждого канала.

c) Оценка DC_{avg}

DC_{avg} был рассчитан как для SRP/CS, так и для SRP/CS, исходя из DC внутреннего теста и мер мониторинга, выполненных на различных компонентах.

Мониторинг времени удержания кнопки S4 (чередование низкого и высокого уровня в окне временных рамок) с помощью PLC A и PLC B в соответствии с ISO 13849-1:2006, приложение E, приводит к низкому DC_{avg} (75 %) для SRP/CS_I.

Меры мониторинга в соответствии с SRP/CSl/o SF 1.0 предусмотрены в SRP/CS_I/o SF 3, что приводит к среднему значению постоянного тока (90 %) для $SRP/CS_L/_O$.

d) Оценка мер против отказа по общей причине (CCF)

Подсчитано, что для каждого SRP/CS были предприняты адекватные меры против отказа по общей причине (разделение, разнесение, защита от перенапряжения, окружающая среда), что, согласно ISO 13849-1:2006, приложение F, приводит к оценке 75 баллов для обоих SRP/CS.

e) Определение PL для каждого SRP/CS

PL для каждого SRP/CS определяется следующим образом:

- SRP/CS_I:
- Категория 1;
- Высокий $MTTF_d$ канала.

Применение этих значений к ISO 13849-1:2006, рисунок 5, дает результат PL c.

- SRP/CSl/o:
- Категория 3;
- Среднее $MTTF_d$ каждого канала;
- Средний DC_{avg};
- 75 баллов за меры против CCF.

Применение этих значений к ISO 13849-1:2006, рисунок 5, дает результат PL d.

f) Определение PL комбинации SRP/CS, выполняющей SF 3

Согласно ISO 13849-1:2006, 6.3, и принимая во внимание как SRP/CS SF 3, PL общей комбинации SRP/CS определяется следующим образом:

$$PL_{low} = c;$$

$$M_{ow} = 1.$$

Таким образом, PL для комбинации SRP/CS SF 3 является PL c.

g) Систематические отказы

Подсчитано, что для SRP/CS SF 3 были приняты адекватные меры против систематических отказов в соответствии с ISO 13849-1:2006, приложение G.

Е.5 Валидация

Е.5.1 Общие положения

Как указано в Е.1, пример был сведен к валидации поведения при неисправности и средствам диагностики функций безопасности SF 1.0 и SF 1.3.

В соответствии с 9.2 и 9.3, валидация поведения при неисправности и средств диагностики выполняется путем рассмотрения проектной документации, анализа отказов и дополнительных испытаний с вводом отказа.

Выполняются следующие шаги:

a) Определить диагностические меры и устройства (компоненты, блоки), которые они проверяют/контролируют.

b) Проверить значение DC, присвоенное каждому диагностическому показателю (DC) для конкретного устройства.

c) Проанализировать поведение системы при сбоях и определите тестовые примеры.

d) Проверить правильность расчета DC_{avg} для каждого SRP/CS.

e) Провести необходимые тесты для подтверждения значений DC.

E.5.2 Валидация поведения при неисправности и Dc_{avg}

Проверка проектной документации (блок-схема безопасности и перечень мероприятий по диагностике SRP/CS) подтверждает, что блоки (компоненты), относящиеся к каждому SRP/CS и комбинации SRP/CS на блок-схемах безопасности, диагностические мероприятия и контролируемые устройства, принятые в обосновании проекта, верны для всех функций безопасности.

FMEA используется для проверки значений DC, назначенных каждому контролируемому устройству каждого SRP/CS, а также поведения системы в случае неисправности.

Поскольку функция безопасности SF 1 должна выполнять как безопасную остановку, так и последующее предотвращение неожиданного пуска, анализ неисправностей для каждого связанного компонента рассматривается в отдельной строке для каждого из этих требований.

Для анализа использовались соответствующие списки неисправностей, приведенные в приложениях A, B, C и D. Теперь рассматривается FMEA для функций безопасности SF 1.0 и SF 1.3, включая тестовые примеры.

E.5.3 FMEA и DC_{avg} для SF 1.0 и SF 1.3

E.5.3.1 SF 1.0

Для того, чтобы облегчить анализ SF 1.0, его блок-схема функции безопасности воспроизведена на рисунке E.12.

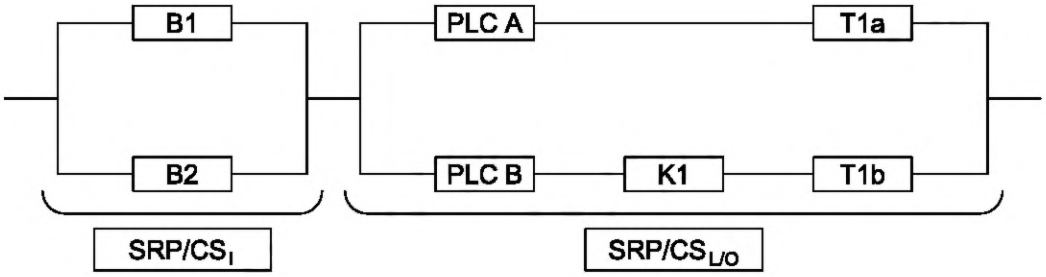


Рисунок E.12 — Блок-схема функции безопасности — SF 1.0

См. таблицы E.3 и E.4.

Из анализа можно сделать вывод, что любые одиночные неисправности в SRP/CS_i будут обнаружены либо немедленно, либо при следующем запросе функции безопасности. При возникновении одиночной неисправности всегда выполняется функция безопасности и предотвращается повторный запуск.

В результате анализа считается, что принятые значения DC (высокий) при конструировании для B1 и B2 являются адекватными. Поскольку DC обоих компонентов одинаков (99 %), DC_{avg} SRP/CS_i высок (99 %), как и предполагалось при конструировании.

Эти характеристики типичны для категории 3, выбранной при конструировании (см. E.4.1) для того, чтобы соответствовать спецификации требований безопасности, приведенной в E.3 (PL_r).

Для проверки правильности выполнения диагностических мероприятий могут применяться тесты, описанные в последнем столбце таблицы E.3.

Таблица Е.3 — FMEA и оценка DC для компонентов SRP/CS_I SF 1.0

	Компонент/ блок	Возможная неисправность	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F1	Блокирующий переключатель B1	Контакт не размыкается при открытии защитного ограждения (механическая неисправность) [a]	Неисправность распознается независимо PLC A и PLC B посредством изменения сигнала в B2, когда запрашивается функция безопасности (открытие защитного ограждения, проверка правдоподобия)	Электродвигатель M1 останавливается через T1a PLC A и через K1 и T1b PLC B, и повторный запуск предотвращается	Подайте статический высокий уровень на соответствующий вход обоих PLC, прежде чем защитное ограждение будет открыто
F2		Отсутствие опасной неисправности при открытом ограждении (исключение неисправности)	—	—	—
Проверка правдоподобия B1 и B2 с помощью PLC A и PLC B дает DC 99 % для B1 (см. ISO 13849-1:2006, таблица Е.1).					
F3	Блокирующий переключатель B2	Контакт не размыкается при открытии защитного ограждения (электрическая или механическая неисправность)	Неисправность распознается независимо PLC A и PLC B посредством изменения сигнала в B1, когда запрашивается функция безопасности (открытие защитного ограждения, проверка достоверности)	Электродвигатель M1 останавливается через T1a PLC A и через K1 и T1b PLC B, и повторный запуск предотвращается	Подайте статический высокий уровень на соответствующий вход обоих PLC, прежде чем защитное ограждение будет открыто
		Самопроизвольное замыкание контактов при открытом ограждении (механические неисправности)	Неисправность распознается независимо и немедленно PLC A и PLC B в результате отсутствия соответствующего изменения сигнала в B1	Электродвигатель M1 останавливается через T1a PLC A и через K1 и T1b PLC B, и повторный запуск предотвращается	Подайте статический высокий уровень на соответствующий вход обоих PLC, пока защита открыта
Проверка правдоподобия B1 и B2 с помощью PLC A и PLC B дает DC 99 % для B2 (см. ISO 13849-1:2006, таблица Е.1).					
Примечание — Проводники не включаются в анализ неисправностей, поскольку считается, что они выходят из строя только по систематическим причинам.					
[a] Электрические неисправности могут быть исключены, поскольку B1 имеет прямой режим срабатывания (см. IEC 60947-5-1:2003, приложение K).					

Таблица E.4 — FMEA и оценка DC компонентов для SRP/CS $_{L}/_{O}$ SF 1.0

	Компонент/ блок	Потенциальные неисправности	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F1	PLC A	Неисправность плат ввода/вывода, зависание, неправильное кодирование или отсутствие выполнения в CPU, что предотвращает отправку PLC A команды остановки на T1a до или во время открытия ограждения	Неисправность распознается PLC B посредством считывания G2 для сравнения его сигнала, зависящего от времени, с ожидаемым изменением числа оборотов. Некоторые неисправности (например, выходные карты) распознаются PLC A посредством считывания G1 при рабочей остановке электродвигателя M1 или при запросе функции безопасности. Другие неисправности могут быть обнаружены заранее с помощью встроенной функции «сторожевого» устройства (WD [a]) PLC A	Электродвигатель M1 останавливается PLC B через K1 и T1b после временной задержки, когда защитное ограждение открывается, и повторный запуск предотвращается. В случае неисправности, обнаруженной PLC A посредством считывания G1 во время рабочей остановки, PLC A информирует PLC B. В результате сообщения PLC B электродвигатель M1 останавливается, а повторный пуск предотвращается PLC B. В случае неисправности, обнаруженной WD, PLC A пытается остановить электродвигатель M1 и предотвратить повторный запуск через T1a до срабатывания функции безопасности, или до того, как электродвигатель M1 остановится, а затем проинформирует об этом PLC B	Подайте статический высокий уровень на стоп-выход PLC A перед тем, как защитное ограждение откроется
F2		Залипание с ошибкой на платах ввода/вывода, или застревание, или неправильное кодирование или отсутствие выполнения в CPU, который удаляет команду остановки PLC A из T1a, когда защита открыта	Ошибки не могут быть распознаны PLC B посредством считывания G2, поскольку двигатель M1 остается приостановленным. PLC B через K1 и T1b, когда защита открыта. Некоторые неисправности (например, карты выходов) распознаются PLC A посредством считывания G1 при закрытии ограждения. Вышеуказанные и дополнительные неисправности обнаруживаются оператором через наблюдение за процессом при закрытии ограждения или с помощью PLC B, когда в следующий раз потребуется функция безопасности (открытие защитного ограждения). Другие неисправности могут быть обнаружены заранее с помощью WD через функцию PLC A	Электродвигатель M1 остается приостановленным PLC B через K1 и T1b, пока защитное ограждение открыто. В случае неисправности, обнаруженной PLC A посредством считывания G1 при закрытии ограждения, PLC A информирует PLC B. В результате отчета PLC B, непреднамеренный запуск электродвигателя M1 предотвращается PLC B. В случае неисправности, обнаруженной WD, PLC A пытается остановить электродвигатель M1 и предотвратить повторный запуск через T1a, а также сообщить об этом PLC B	Передача пускового сигнала на инвертор, когда защитное ограждение открыто

Продолжение таблицы Е.4

[a] Некоторые внутренние неисправности PLC, которые априори не приводят к отказу функции безопасности (например, неспособность PLC отправить команду остановки на привод или клапан, или неспособность удерживать команду остановки на приводе или на клапане) могут быть обнаружены функцией WD.

В результате косвенного контроля PLC A с помощью PLC B через G2, косвенного контроля PLC A своей собственной выходной карты через G1, контроля последовательности выполнения программы внутренним «сторожевым» устройством и обнаружения ошибок посредством наблюдения за процессом, PLC A считается имеющим неисправность DC 90 % (см. ISO 13849-1:2006, таблица Е.1).

Вышеупомянутые меры можно рассматривать как относящиеся к ISO 13849-1:2006, таблица Е.1, примечание 2.

Примечание — Считается, что большинство сбоев PLC происходит на платах ввода/вывода и относится к типу «постоянные» (90 % всех сбоев в PLC), но функция WD PLC может обнаруживать только некоторые сбои, влияющие на последовательность выполнения программы.

	Компонент/ блок	Потенциальные неисправности	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F3	Инвертор T1a	Устойчивая неисправность и другие сложные внутренние неисправности в управляющей и силовой электронике инвертора, которые не позволяют T1a остановить двигатель до или при открытии защитного ограждения	Неисправность распознается PLC B посредством считывания G2, когда запрашивается функция безопасности. Неисправность также распознается PLC A посредством считывания G1 при рабочей остановке электродвигателя M1 или когда требуется срабатывание функции безопасности	Электродвигатель M1 останавливается PLC B через K1 и T1b после временной задержки, когда защитное ограждение открывается, и повторный запуск предотвращается. PLC A информирует PLC B, когда неисправность распознается во время рабочей остановки. В результате оповещения PLC B, электродвигатель M1 останавливается, а повторный запуск предотвращается PLCB	Установите вход остановки инвертора на высокий уровень до или во время открытия защитного ограждения
F3	Инвертор T1a	Устойчивая неисправность и другие сложные внутренние неисправности в управляющей и силовой электронике инвертора, которые не позволяют T1a остановить двигатель до или при открытии защитного ограждения	Неисправность распознается PLC B посредством считывания G2, когда запрашивается функция безопасности. Неисправность также распознается PLC A посредством считывания G1 при рабочей остановке электродвигателя M1 или когда требуется срабатывание функции безопасности	Электродвигатель M1 останавливается PLC B через K1 и T1b после временной задержки, когда защитное ограждение открывается, и повторный запуск предотвращается. PLC A информирует PLC B, когда неисправность распознается во время рабочей остановки. В результате оповещения PLC B, электродвигатель M1 останавливается, а повторный запуск предотвращается PLC B	Установите вход остановки инвертора на высокий уровень до или во время открытия защитного ограждения

Продолжение таблицы Е.4

	Компонент/ блок	Потенциальные неисправности	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F4		Устойчивая неисправность и другие сложные внутренние неисправности в управляющей и силовой электронике инвертора, которая выдает стробирующие сигналы на силовые полупроводники T1a при открытом защитном ограждении	Неисправность не может быть распознана PLC B посредством считывания G2, поскольку двигатель M1 остается приостановленным PLC B через K1 и T1b, когда защита открыта. Неисправность будет обнаружена оператором посредством наблюдения за процессом при закрытии ограждения. Неисправность также распознается PLC A посредством считывания G1 при закрытии ограждения	Электродвигатель M1 остается приостановленным PLC B через K1 и T1b, пока ограждение открыто. При закрытии ограждения происходит непреднамеренный пуск двигателя (неопасно). PLC A информирует PLC B, когда обнаруживается ошибка. В результате уведомления PLC B, непреднамеренный запуск электродвигателя M1 предотвращается, а повторный запуск предотвращается PLC B	Передача пускового сигнала на инвертор, когда защитное ограждение открыто
В результате косвенного контроля T1a с помощью PLC B до G2, косвенного контроля T1a с помощью PLC от A до G1 и обнаружения неисправностей посредством наблюдения за процессом считается, что T1a имеет DC 99 % [a] Некоторые внутренние неисправности PLC, которые априори не приводят к отказу функции безопасности (например, неспособность PLC отправить команду остановки на привод или клапан, или неспособность удерживать команду остановки на приводе или на клапане) могут быть обнаружены функцией WD.					
F5	PLC B	Устойчивая неисправность на платах ввода/вывода, или ошибка типа «постоянная», или неправильное кодирование, или отсутствие выполнения в CPU, который предотвращает отключение PLC B K1 до или во время открытия защитного ограждения	Неисправность распознается PLC A, контролирующим механически связанный контакт обратной связи K1, когда запрашивается функция безопасности. Некоторые неисправности могут быть обнаружены на ранней стадии с помощью WD как функции PLC B	Электродвигатель M1 немедленно останавливается PLC A через T1a, когда защитное ограждение открывается и повторный пуск предотвращается. В случае неисправности, обнаруженной WD, PLC B пытается сообщить об этом PLC A, а затем остановить электродвигатель M1 и предотвратить повторный запуск через T1b до того, как будет затребована функция безопасности	Держите K1 в положении питания при открытии защитного ограждения

Продолжение таблицы Е.4

	Компонент/ блок	Потенциальные неисправности	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F6		Устойчивая неисправность на платах ввода/вывода, или ошибка типа «постоянная», или неправильное кодирование, или отсутствие выполнения в CPU, который снимает команду остановки PLC B с К1, когда защитное ограждение открыто	Неисправность немедленно распознается PLC A, контролирующим механически связанный контакт обратной связи К1. Некоторые неисправности могут быть обнаружены на ранней стадии с помощью WD как функции PLC B	Электродвигатель М1 останавливается PLC A через T1a, пока защитное ограждение открыто, и повторный запуск невозможен. В случае неисправности, обнаруженной WD, PLC B пытается остановить электродвигатель М1 и предотвратить повторный запуск через T1b, и сообщить PLC A	Переключите К1 в его положение питания, когда защита открыта
В результате косвенного контроля PLC B со стороны PLC A через положение контакта обратной связи К1 и контроля последовательности выполнения программы внутренним сторожевым устройством считается, что PLC B имеет DC 90 %					
Примечание — Считается, что большинство сбоев PLC происходят на платах ввода-вывода и относятся к типу «постоянные» (90 % всех сбоев в PLC), но функция WD PLC может обнаруживать только некоторые сбои, влияющие на последовательность выполнения программы.					
F7	Релейный контактор К1	Контакт не размыкается при открытии защитного ограждения (электрическая неисправность, например, приварены контакты)	Неисправность распознается PLC A, контролирующим механически связанный контакт обратной связи К1, когда запрашивается функция безопасности	Электродвигатель М1 немедленно останавливается PLC A через T1a, когда защитное ограждение открывается и повторный пуск предотвращается	Держите контакт К1 в положении ВКЛ при открытии защитного ограждения
F8		Отсутствие опасной неисправности при открытом ограждении (исключение неисправности)			
Контроль релейного контактора К1 с помощью PLC A посредством положения механически связанного контакта обратной связи К1 дает DC 99 % для К1					
[a] Некоторые внутренние неисправности PLC, которые *априори* не приводят к отказу функции безопасности (например, неспособность PLC отправить команду остановки на привод или клапан, или неспособность удерживать команду остановки на приводе или на клапане), могут быть обнаружены функцией WD.					
F9	Инвертор T1b	Неоткрытие внутреннего релейного контакта при открытии ограждения	Неисправность распознается PLC A, контролирующего механически связанный контакт обратной связи для внутреннего реле T1b, когда срабатывает функция безопасности	Электродвигатель М1 немедленно останавливается PLC A через T1a, когда защитное ограждение открывается и повторный пуск предотвращается	Держите вход катушки реле блокировки в T1b на высоком уровне, когда ограждение открыто

Окончание таблицы Е.4

	Компонент/ блок	Потенциальные неисправности	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F10		Отсутствие опасной неисправности при открытом ограждении (исключение неисправности)			
Контроль внутреннего (блокирующего импульсы) реле T1b с помощью PLC A дает DC 99 % для T1b					
[a] Некоторые внутренние неисправности PLC, которые *априори* не приводят к отказу функции безопасности (например, неспособность PLC отправить команду остановки на привод или клапан, или неспособность удерживать команду остановки на приводе или на клапане), могут быть обнаружены функцией WD.					

Из анализа можно сделать вывод, что одиночные неисправности в SRP/CS будут обнаруживаться либо сразу, либо при оперативной остановке электродвигателя M1, либо при следующем запросе на функцию безопасности. При возникновении одиночной неисправности всегда выполняется функция безопасности. Повторный запуск возможен только с одним каналом в случае необнаруженной неисправности в PLC A и PLC B.

Анализ определяет, что значения DC, принятые при конструировании SRP/CSI/o, являются адекватными. Принимая во внимание расчетные значения $MTTF_d$ и значения DC для различных компонентов, используемых в $SRP/CS_I/o$, достигается среднее значение DC среднего (90 %), как и предполагалось при конструировании.

Эти характеристики типичны для категории 3, выбранной при конструировании (см. Е.4.1) для того, чтобы соответствовать спецификации требований безопасности, приведенной в Е.3 (PL_r).

Для проверки правильности выполнения диагностических мероприятий могут применяться тесты, описанные в последнем столбце таблицы Е.4.

Е.5.3.2 SF 1.3

Чтобы облегчить анализ SF 1.3, его блок-схема функции безопасности воспроизведена на рисунке Е.13.

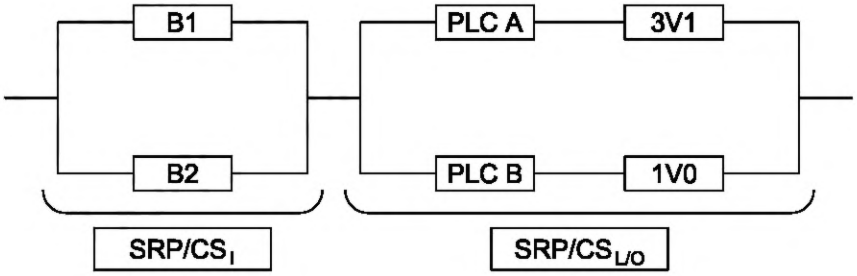


Рисунок Е.13 — Блок-схема функции безопасности для SF 1.3

Для SRP/CSi из SF 1.3, диагностические меры и проверенные/отслеживаемые устройства идентичны таковым для SF 1.0, поэтому DC_{avg} SRP/CS_I также высок (99 %).

См. таблицу Е.5.

Таблица E.5 — FMEA SRP/$CS_{L/O}$ SF 1.3

	Компонент/ блок	Возможные неисправности/сбои	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F1	PLC A	Устойчивая неисправность на платах ввода/вывода, или ошибка типа «постоянная», или неправильное кодирование, или отсутствие выполнения в CPU, который предотвращает отключение PLC A 3V1 до или при открытии защитного ограждения	Некоторые неисправности (например, карты выходов) распознаются PLC A посредством считывания показаний датчика давления 3S1 при рабочей остановке пневматического двигателя A3 или при запросе функции безопасности. Другие неисправности могут быть обнаружены заранее с помощью WD как функции PLC A	Пневматический двигатель A3 останавливается PLC B через 1V0 после временной задержки, когда защитное ограждение открывается. В случае ошибок, обнаруженных PLC A посредством считывания 3S1 во время рабочей остановки, PLC A информирует об этом PLC B. В результате уведомления PLC B, пневматический двигатель A3 останавливается через 3V1 и повторный запуск предотвращается PLC B. При ошибках, обнаруженных WD, PLC A пытается остановить пневматический двигатель A3 и предотвратить повторный пуск через 3V1 до того, как будет запрошена функция безопасности или до того, как пневматический двигатель A3 останавливается, а затем информирует PLC B	Примените статический высокий уровень на выход 3V1 PLC A перед открытым защитным ограждением
F2		Устойчивая неисправность на платах ввода/вывода, или ошибка типа «постоянная», или неправильное кодирование, или отсутствие выполнения в CPU, который приводит к тому, что PLC A включает 3V1, когда защитное ограждение открыто	Некоторые неисправности (например, карты выходов) распознаются PLC A посредством считывания показаний датчика давления 3S1 при закрытии ограждения. Другие неисправности могут быть обнаружены на ранней стадии с помощью функции WD. PLC A	Пневматический двигатель A3 останавливается PLC B через 1V0, пока ограждение открыто. При закрытии ограждения, PLC B подает питание 1V0, и пневматический двигатель A3 перезапускается (безопасно). В случае неисправности, обнаруженной PLC A посредством считывания 3S1 при закрытии ограждения, PLC A информирует PLC B. В результате уведомления PLC B, непреднамеренный пуск пневматического двигателя A3 предотвращается, а повторный пуск предотвращается PLC B. При неисправностях, обнаруженных WD, PLC A пытается остановить пневматический двигатель A3 и предотвратить повторный запуск через 3V1, а также сообщить об этом PLC B	Измените выход 3V1 PLC A на высокий уровень, пока защитное ограждение открыто
В результате косвенного контроля PLC A своей собственной платы вывода через 3S1 и контроля последовательности выполнения программы внутренним сторожевым устройством считается, что PLC A имеет DC 90 %					
Примечание — Считается, что большинство сбоев PLC происходят на платах ввода/вывода и относятся к типу «постоянные» (90 % всех сбоев в ПЛК), но функция WD PLC может обнаруживать только некоторые сбои, влияющие на последовательность выполнения программы.					

Продолжение таблицы Е.5

	Компонент/ блок	Возможные неисправности/сбои	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F3	Электромагнитный клапан управления направлением движения 3V1	Непереключение (залипание в конечном положении) или неполное переключение (залипание в произвольном промежуточном положении) или изменение времени переключения до или во время открытия ограждения	Неисправность распознается PLC A посредством считывания показаний датчика давления 3S1 при рабочей остановке пневматического двигателя A3 или при запросе функции безопасности. Неисправности также выявляет оператор через наблюдение за процессом	Пневматический двигатель A3 останавливается PLC B через 1V0 после временной задержки, когда защитное ограждение открывается. PLC A информирует PLC B при обнаружении неисправности. По результатам этого сообщения, PLC B останавливает посредством 1V0 пневматический двигатель A3, и любой повторный запуск предотвращается	Держите электрические и пневматические управляющие сигналы для 3V1 на высоком уровне при открытии ограждения
F4		Самопроизвольное изменение начального положения переключения (без входного сигнала) при открытом ограждении. ПРИМЕЧАНИЕ: Эту неисправность можно исключить, поскольку 3V1 имеет испытанные пружины, а также применяются нормальные условия монтажа и эксплуатации	—	—	—
В результате косвенного контроля 3V1 PLC A через 3S1 и обнаружения неисправностей с помощью наблюдения за процессом считается, что 3V1 имеет DC 99 %					
F5	PLC B	Устойчивая неисправность на платах ввода/вывода, или ошибка типа «постоянная», или неправильное кодирование, или отсутствие выполнения в CPU, что не позволяет PLC B отключить 1V0 до или при открытии защитного ограждения	Некоторые сбои (например, карты выходов) распознаются PLC B посредством считывания реле давления 1S0, когда требуется функция безопасности. Другие могут быть обнаружены на ранней стадии с помощью функции WD [a]. PLC B	Пневмодвигатель A3 немедленно останавливается PLC A через 3V1 при открытии защитного ограждения. В случае ошибок, обнаруженных PLC B посредством считывания реле давления 1S0, PLC B сообщает PLC A и держит K1 деактивированным. В результате уведомления, PLC A предотвращает повторный запуск. Для неисправностей, обнаруженных WD, PLC B пытается проинформировать PLC A, а затем остановить пневматический двигатель A3 через 1V0 и предотвратить повторный запуск до срабатывания функции безопасности.	Подайте статический высокий уровень на выход 1V0 PLC B перед открытым защитным ограждением

Продолжение таблицы Е.5

	Компонент/ блок	Возможные неисправности/сбои	Обнаружение неисправностей	Эффект/реакция	Тесты для подтверждения
F6		Устойчивая неисправность на платах ввода/вывода, или ошибка типа «постоянная», или неправильное кодирование, или отсутствие выполнения на CPU, что заставляет PLC B включать 1V0, когда защитное ограждение открыто	Некоторые неисправности (например, платы вывода) немедленно распознаются PLC B путем считывания реле давления 1S0. Другие могут быть обнаружены на ранней стадии с помощью функции WD [a]. PLC B		
В результате косвенного контроля PLC B собственной выходной платы через 1S0, косвенного контроля PLC B PLC A через положение контакта обратной связи K1 и контроля последовательности выполнения программы внутренним сторожевым устройством, считается, что PLC B имеет DC 90 %					
Примечание — Считается, что большинство сбоев PLC происходят на платах ввода-вывода и относятся к типу «постоянные» (90 % всех сбоев в PLC), но функция WD PLC может обнаруживать только некоторые сбои, влияющие на последовательность выполнения программы.					
F7	Электромагнитный клапан управления направлением движения 1V0	Непереключение (залипание в конечной позиции) или неполное переключение (залипание в произвольном промежуточном положении) или изменение времени переключения до или во время открывания защитного ограждения	Неисправность распознается PLC B посредством считывания реле давления 1S0, когда срабатывает функция безопасности	Пневмодвигатель A3 немедленно останавливается PLC A через 3V1 при открытии защитного ограждения. В случае ошибок, обнаруженных PLC B посредством считывания реле давления 1S0, PLC B сообщает PLC A и держит K1 обесточенным. В результате уведомления, PLC A предотвращает повторный запуск	Подайте статический высокий уровень на выход 1V0 PLC B перед открытым защитным ограждением
F8	Магнитный клапан 1V0	Самопроизвольное изменение исходного положения переключения (без входного сигнала), во время открытия защитного ограждения. Примечание — Эта неисправность может быть исключена, так как 1V0 имеет испытанные пружины и применяются нормальные условия установки и эксплуатации	—	—	—
Косвенный контроль 1V0 с помощью PLC B через 1S0 дает DC 99 % для 1V0					

Окончание таблицы Е.5

[a] Некоторые внутренние неисправности PLC, которые априори не приводят к отказу функции безопасности (например, неспособность PLC отправить команду остановки на привод или клапан, или неспособность удерживать команду остановки на приводе или на клапане), могут быть обнаружены функцией WD.

Из анализа можно сделать вывод, что большинство одиночных отказов в SRP/CS будут обнаружены либо немедленно, либо при рабочей остановке пневматического двигателя А3, либо при следующем запросе функции безопасности. При возникновении одиночной неисправности всегда выполняется функция безопасности. Повторный запуск возможен только с одним каналом в случае необнаруженной неисправности в PLC A и PLC B.

Анализ определяет, что значения DC, принятые при конструировании SRP/CSI/o, являются адекватными. Принимая во внимание расчетные значения $MTTF_d$ и значения DC для различных компонентов, используемых в $SRP/CS_I/o$, достигается среднее значение DC среднего (90 %), как и предполагалось при конструировании.

Эти характеристики типичны для категории 3, выбранной при конструировании (см. Е.4.1) для того, чтобы соответствовать спецификации требований безопасности, приведенной в Е.3 (PL_r).

Для проверки правильности выполнения диагностических мероприятий могут применяться тесты, описанные в последнем столбце таблицы Е.5.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO 12100:2010	IDT	ГОСТ ISO 12100—2013 «Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска»
ISO 13849-1:2006	IDT	ГОСТ ISO 13849-1—2014 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования»

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

- IDT — идентичные стандарты.

Библиография

[1] ISO 4079-1 Rubber hoses and hose assemblies — Textile-reinforced hydraulic types — Specification — Part 1: Oil-based fluid applications (Рукава и рукава в сборе резиновые. Рукава с текстильными прокладками для гидравлических жидкостей. Технические условия. Часть 1. Применение для жидкостей на нефтяной основе)

[2] ISO 4413:2010 Hydraulic fluid power — General rules and safety requirements for systems and their components (Гидравлика. Общие правила и требования безопасности, касающиеся систем и их компонентов)

[3] ISO 4414:2010 Pneumatic fluid power — General rules and safety requirements for systems and their components (Пневматика. Общие правила и требования безопасности, касающиеся систем и их компонентов)

[4] ISO 4960 Cold-reduced carbon steel strip with a mass fraction of carbon over 0,25 % (Сталь углеродистая полосовая, обжатая в холодном состоянии, с содержанием углерода свыше 0,25%)

[5] ISO 5598:2008 Fluid power systems and components — Vocabulary (Приводы гидравлические и пневматические и их элементы. Словарь)

[6] ISO 11161 Safety of machinery — Integrated manufacturing systems — Basic requirements (Безопасность машин и механизмов. Интегрированные производственные системы. Основные требования)

[7] ISO 13850 Safety of machinery — Emergency stop — Principles for design (Безопасность машин. Аварийный останов. Принципы проектирования)

[8] ISO 13851 Safety of machinery — Two-hand control devices — Functional aspects and design principles (Безопасность машин. Двуручные устройства управления. Принципы проектирования и выбора)

[9] ISO 13855 Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body (Позиционирование защитного оборудования с учетом скорости сближения частей человеческого тела)

[10] ISO 13856 (все части) Safety of machinery — Pressure-sensitive protective devices (Безопасность машин. Сенсорные защитные устройства)

[11] ISO 14118:2000 Safety of machinery — Prevention of unexpected start-up (Безопасность машин. Предупреждение неожиданных пусков)

[12] ISO 14119:1998 Safety of machinery — Interlocking devices associated with guards — Principles for design and selection (Безопасность машин. Блокировочные устройства для ограждений. Принципы конструкции и выбора)

[13] IEC 60204-1:2005 Safety of machinery — Electrical equipment of machines — Part 1: General requirements (Безопасность машин. Электрооборудование промышленных машин. Часть 1. Общие требования)

[14] IEC 60269-1 Low-voltage fuses — Part 1: General requirements (Предохранители плавкие низковольтные. Часть 1. Общие требования)

[15] IEC 60529 Degrees of protection provided by enclosures (IP code) (Степени защиты, обеспечиваемые оболочками (код IP))

[16] IEC 60664 (все части) Insulation coordination for equipment within low-voltage systems (Координация изоляции для оборудования в низковольтных системах)

[17] IEC 60812 Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA) (Техника анализа надежности систем. Метод анализа вида и последствий отказа (FMEA))

[18] IEC 60893-1 — Insulating materials — Industrial rigid laminated sheets based on thermosetting resins for electrical purposes — Part 1: Definitions, designations and general requirements (Материалы изоляционные. Материалы промышленные жесткие слоистые листовые на основе термореактивных смол электротехнического назначения. Часть 1. Определения, обозначения и общие требования)

[19] IEC 60947 (все части) — Low-voltage switchgear and controlgear (Аппаратура распределения и управления низковольтная)

[20] IEC 61025 — Fault tree analysis (FTA) (Анализ диагностического дерева неисправностей (FTA))

[21] IEC 61078 — Analysis techniques for dependability — Reliability block diagram and boolean methods (Методы анализа общей надежности. Метод блок-схемы и булев метод)

[22] IEC 61131-1 — Programmable controllers — Part 1: General information (Контроллеры программируемые. Часть 1. Общие сведения)

[23] IEC 61131-2 — Programmable controllers — Part 2: Equipment requirements and tests (Контроллеры программируемые. Часть 2. Требования к оборудованию и испытания)

[24] IEC 61165 — Application of Markov techniques (Применение методики Маркова)

[25] IEC 61249 (все части) — Materials for printed boards and other interconnecting structures (Материалы для печатных плат и других структур меж-соединений)

[26] IEC 61508 — Functional safety of electrical/electronic/programmable electronic safety-related systems (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью)

[27] IEC 61558 (все части) — Safety of power transformers, power supplies, reactors and similar products (Трансформаторы силовые, блоки питания и аналогичные изделия)

[28] IEC 61800-5-2 — Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional (Системы силовых электроприводов с регулируемой скоростью. Часть 5-2. Функциональные требования безопасности)

[29] IEC 61810 (все части) — Electromechanical elementary relays (Реле логические электромеханические)

[30] EN 952:1996 — Safety of machinery — Safety requirements for fluid power systems and their components — Hydraulics (Безопасность машин. Требования безопасности для гидравлических систем и их компонентов. Гидравлика)

[31] EN 953:1996 — Safety of machinery — Safety requirements for fluid power systems and their components — Pneumatics (Безопасность машин. Требования безопасности для гидравлических систем и их компонентов. Пневматика)

[32] EN 50205 — Relays with forcibly guided (mechanically linked) contacts (Реле с принудительно управляемыми (механически связанными) контактами)

[33] EN 60730 (все части) — Automatic electric controls for household and similar use (Автоматическое электрическое управление для бытового и аналогичного использования)

[34] JESD22A121.01 — Test Method for Measuring Whisker Growth on Tin and Alloy Surfaces Finishes (Метод испытаний для измерения роста «усов» на поверхностях из олова и сплавов)[1)]

[35] JESD201 — Environmental Acceptance Requirements for Tin Whisker Susceptibility of Tin and Alloy Surface Finishes (Требования к приемлемости для окружающей среды в отношении восприимчивости поверхностей олова и сплавов к образованию оловянных «усов»)[1)]

[1)] JEDEC Solid State Technology Association, 2500 Wilson Boulevard, Arlington, VA 22201-3834, www.jedec.org/download/search/22a1121-01.pdf

УДК 62.93:006.354 МКС 13.110 IDT

Ключевые слова: процесс валидации, принципы валидации, план валидации, блок-схема функции, валидация функций безопасности, валидация на соответствие категорий, валидация требований окружающей среды

Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 21.11.2025. Подписано в печать 23.12.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 9,30. Уч.-изд. л. 7,91.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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