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

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO 13849-1— 2014

Безопасность оборудования

ЭЛЕМЕНТЫ СИСТЕМ УПРАВЛЕНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ

Часть 1

Общие принципы конструирования

(ISO 13849-1:2006, IDT)

Издание официальное

Москва
Стандартинформ
2015

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0—92 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2009 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, применения, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Экспериментальным научно-исследовательским институтом металлорежущих станков (ОАО «ЭНИМС») на основе собственного аутентичного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии (Росстандарт)

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 5 декабря 2014 г. № 46)

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
Азербайджан	AZ	Аэстандарт
Армения	AM	Минэкономики Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Казахстан	KZ	Госстандарт Республики Казахстан
Киргизия	KG	Кыргызстандарт
Молдова	MD	Молдова-Стандарт
Россия	RU	Росстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 3 июня 2015 г. № 549-ст межгосударственный стандарт ГОСТ ISO 13849-1—2014 введен в действие в качестве национального стандарта Российской Федерации с 1 января 2016 г.

5 Настоящий стандарт идентичен международному стандарту ISO 13849-1:2006/Cor.1:2009 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования), включая Поправку 1:2009.

Международный стандарт разработан техническим комитетом по стандартизации CEN/TC 114 «Безопасность машинного оборудования».

Перевод с английского языка (en).

Официальные экземпляры международного стандарта, на основе которого подготовлен настоящий межгосударственный стандарт, и международных стандартов, на которые даны ссылки, имеются в Федеральном агентстве по техническому регулированию и метрологии.

Сведения о соответствии межгосударственных стандартов ссылочным международным стандартам приведены в дополнительном приложении ДА.

Степень соответствия — идентичная (IDT)

6 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты» (по состоянию на 1 января текущего года), а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Содержание

Введение

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

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

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

- стандарты типа В1 — стандарты по конкретным аспектам безопасности (например, по безопасным расстояниям, шумам, безопасной температуре поверхности и т. п.);
- стандарты типа В2 — стандарты по защитным устройствам (например, по двуручным управляющим устройствам, устройствам блокировки, датчикам давления, защитным ограждениям и т. п.);

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

Настоящий стандарт является стандартом типа В1, как установлено в ISO 12100.

Если положения стандарта типа С отличаются от положений, установленных в стандартах типа А или типа В, то положения стандарта типа С имеют преимущество над положениями других стандартов для машин, которые были спроектированы и построены в соответствии с положениями стандарта типа С.

Настоящий стандарт представляет собой руководство для тех, кто занимается проектированием и оценкой систем управления, а также для технических комитетов, разрабатывающих стандарты типа В2 и С, которые должны соответствовать Основным требованиям по безопасности Приложения I к Директиве Совета 98/37/ЕС на машины и механизмы. Стандарт не содержит конкретных указаний в отношении того, каким образом можно достичь соответствия требованиям других директив ЕС.

Как часть общей стратегии сокращения риска при работе на оборудовании конструктор часто выбирает меры сокращения рисков путем применения защитных устройств, выполняющих одну или более функций безопасности.

Элементы систем управления машиной, предназначенные для обеспечения функций безопасности, называются элементами систем управления, связанными с обеспечением безопасности (SRP/CS), и могут состоять из технических средств и программного обеспечения, они могут быть отделены от системы управления машиной или являться ее частью. Кроме выполнения функции безопасности SRP/CS могут также выполнять операционные функции (например, двуручные управляющие устройства как средства включения).

Способность элементов систем управления, связанных с обеспечением безопасности, выполнять функции безопасности в предвиденных обстоятельствах — это один из пяти уровней эффективности защиты (PL). Эти уровни эффективности определены в соответствии с вероятностью опасного отказа в час (см. таблицу 3).

Вероятность опасного отказа функции безопасности зависит от нескольких факторов, включая структуру технических средств и программного обеспечения, диапазон механизмов обнаружения неисправности [диагностический охват (DC)], надежность компонентов [среднее время наработки на опасный отказ ($MTTF_d$), отказ по общей причине (CCF)], процесс конструирования, рабочее напряжение, условия окружающей среды и производственные процессы.

С целью оказания помощи конструктору и облегчения оценки достигнутого PL в этом документе предлагается методика, основанная на классификации структур в соответствии с критериями конструирования и особым поведением станка в условиях сбоя. Категории — это один из пяти уровней, называемых Категориями В, 1, 2, 3 и 4.

Категории и уровни эффективности защиты можно применять к элементам системы управления, связанным с безопасностью, таким как:

- защитные устройства (например, двуручные управляющие устройства, блокирующие устройства), электрочувствительное предохранительное оборудование (например, фотоэлектрические барьеры), устройства, чувствительные к давлению;
- управляющие устройства (например, логический элемент функций контроля, обработка данных, автоматическое слежение и т. д.);
- устройства силового регулирования (например, реле, клапаны и т. д.),

а также к системам управления, выполняющим функции безопасности на всех видах оборудования — от простого (например, кухонные приборы или автоматические двери и ворота) до производственных установок (например, упаковочные машины, печатные станки, прессы).

Цель разработки настоящего стандарта — предоставить четкую основу разработчикам стандартов типа С, на которой конструирование и функционирование любого элемента системы управления, связанного с обеспечением безопасности оборудования, может быть объективно оценено, например, с помощью третьей стороны, собственных (внутренних) средств или независимого испытательного органа.

В настоящем стандарте, как и в [10], устанавливаются требования к конструированию и внедрению элементов систем управления, связанных с обеспечением безопасности. Применение любого из двух вышеупомянутых стандартов в соответствии с областью их применения должно удовлетворять основным требованиям по безопасности. Нижеприведенная таблица 1 содержит области применения [10] и настоящего стандарта.

Таблица 1 — Рекомендуемое применение IEC 62061 [10] и настоящего стандарта

Технология, использующая функцию(и) управления, связанную(ые) с безопасностью	Настоящий стандарт	МЭК 62061 [10]
A Неэлектрическая: например, гидравлика	X	Не входит
B Электромеханическая: например, реле и/или несложная электроника	Ограничена структурными построениями[a] и до PL = *e*	Все структуры и до SIL 3
C Сложная электроника: например, программируемая	Ограничена структурными построениями[a] и до PL = *d*	Все структуры и до SIL 3
D A в сочетании с B	Ограничена структурными построениями[a] и до PL = *e*	X[c]
E C в сочетании с B	Ограничена структурными построениями (см. Примечание 1) и до PL = *d*	Все структуры и до SIL 3
F C в сочетании с A или C в сочетании с A и B	X[b]	X[c]
X показывает, что этот пункт рассматривается в стандарте, указанном в заголовке колонки.		

[a] Структурные построения определены в 6.2, чтобы обеспечить упрощенный подход к квантификации уровня эффективности защиты.

[b] Для сложной электроники: используйте структурные построения в соответствии с настоящим стандартом до PL = *d* или любую структуру в соответствии с [10].

[c] Для неэлектрической технологии используйте элементы в соответствии с настоящим стандартом как подсистемы.

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

Безопасность оборудования

ЭЛЕМЕНТЫ СИСТЕМ УПРАВЛЕНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ

Часть 1

Общие принципы конструирования

Safety of machinery. Safety-related parts of control systems. Part 1. General principles for design

Дата введения — 2016—01—01

1 Область применения

Настоящий стандарт устанавливает требования безопасности и общие принципы конструирования элементов систем управления, связанных с безопасностью (SRP/CS). Стандарт определяет категории SRP/CS и описывает характеристики их функций безопасности. Стандарт распространяется на любые SRP/CS, независимо от вида используемой энергии: например, электрической, гидравлической, пневматической, механической.

Настоящий стандарт не устанавливает, какие функции безопасности и какие категории должны применяться в каждом конкретном случае.

Настоящий стандарт устанавливает специфические требования к SRP/CS, которые используют программируемые системы.

Стандарт не предъявляет особых требований к конструированию изделий, являющихся частью SRP/CS. Тем не менее можно применять некоторые принципы, такие как категории или уровни эффективности защиты (PL).

Примечание 1 — Примеры изделий, являющихся частью элементов систем управления, связанных с безопасностью: реле, соленоидные клапаны, выключатели положения, программируемые путевые выключатели, моторные блоки управления, двуручные управляющие устройства, оборудование, чувствительное к давлению. При разработке такой продукции необходимо соответствие с международными стандартами, такими как [14], [15], [16].

Примечание 2 — Определение термина «требуемый уровень эффективности защиты» см. 3.1.24.

Примечание 3 — Требования, предъявляемые к программируемым системам, совместимы с представленной в [10] методологией конструирования и усовершенствования электрических, электронных и программируемых систем управления, связанных с безопасностью.

Примечание 4 — Для встроенного программного обеспечения, связанного с безопасностью для компонентов с $PL_r = e$, см. раздел 7, IEC 61508-3.

Примечание 5 — Смотри также таблицу 1.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

ISO 12100 Safety of machinery — General principles for design — Risk assessment and risk reduction (Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска)

ISO 13849-2:2003 Safety of machinery — Safety-related parts of control systems — Part 2: Validation (Безопасность машин. Детали систем управления, связанные с обеспечением безопасности. Часть 2. Валидация)

ISO 14121 Safety of machinery — Principles of risk assessment (Безопасность машин. Принципы оценки рисков)

Издание официальное

IEC 60050-191:1990 International electrotechnical vocabulary — Chapter 191: Dependability and quality of service and IEC 60050-191 — am 1:1999 and IEC 60050-191 — am 2:2002 (Международный словарь по электротехнике — Раздел 191: Функциональная надежность и качество обслуживания, и МЭК 60050-191 — поправка 1:1999 и МЭК 60050-191 — поправка 2:2002)

IEC 61508-1 Function safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования)

IEC 61508-3:1998/Corr.1:1999 Functional safety of electrical/electronic/ programmable electronic safety-related systems — Part 3: Software requirements (МЭК 61508-3:1998/Поправка 1:1999 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению)

IEC 61508-4 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definition and abbreviations (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения)

IEC 61511-1:2003 Functional safety — Safety instrumented systems for the process industry sector — Part 1: Framework, definitions, system, hardware and software requirements (Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования)

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины и определения по ISO 12100 и IEC 60050-191, а также следующие термины и определения:

3.1.1 **элемент системы управления, связанный с безопасностью** (safety-related part of a control system, SRP/CS): Часть системы управления, которая реагирует на входные сигналы и вырабатывает выходные сигналы, связанные с обеспечением безопасности.

Примечание 1 — Комбинированные элементы системы управления, связанные с безопасностью, начинают действовать в точке, где возникают сигналы, имеющие отношение к безопасности, например, включающий (рабочий, подталкивающий) кулачок и ролик выключателя положения, и заканчивают на выходе силовых управляющих элементов, например, главные контакты пускателя (контактора).

Примечание 2 — Если системы мониторинга (текущего контроля) используются для диагностики, они также считаются элементами систем управления, связанными с безопасностью.

3.1.2 **категория** (category, Cat.): Классификация элементов системы управления, связанных с обеспечением безопасности, по их устойчивости к неисправностям и последующему поведению при неисправном состоянии, достигаемая структурным построением указанных элементов и/или определяемая их надежностью.

3.1.3 **неисправность** (fault): Состояние оборудования, характеризуемое его неспособностью выполнять требуемую функцию, исключая профилактическое обслуживание или другие планово-предупредительные действия, а также исключая неспособность выполнять требуемую функцию из-за недостатка внешних ресурсов.

Примечание 1 — Неисправность часто является следствием отказа самого оборудования, но может существовать и без предварительного отказа по IEC 60050-191.

Примечание 2 — В стандарте «неисправность» означает случайную неисправность.

3.1.4 **отказ** (failure): Нарушение способности технического объекта (элемента) по выполнению требуемой функции.

Примечание 1 — После отказа технический объект находится в неисправном состоянии.

Примечание 2 — «Отказ» является событием в отличие от «неисправности», которая является состоянием.

Примечание 3 — Это понятие, как оно определено, не применяют к техническим объектам, состоящим только из средств программного обеспечения (IEC 60050-191).

Примечание 4 — Отказы, которые оказывают влияние на процесс управления, рассматриваются вне рамок настоящего стандарта.

3.1.5 **опасный отказ** (dangerous failure): Отказ, который может привести к тому, что система, связанная с безопасностью, перейдет в опасное состояние или в состояние ошибки при выполнении функции.

Примечание 1 — Технический потенциал может зависеть от архитектуры каналов системы; в системах с резервированием менее вероятно, что отказ (сбой) аппаратного обеспечения приведет к всеобщей опасности или угрозе выведения из строя.

Примечание 2 — См. IEC 61508-4, 3.6.7.

3.1.6 **отказ по общей причине** (common cause failures, CCF): Повреждения разных частей машины, произошедшие в результате одного события и не являющиеся следствиями друг друга.

Примечание — «Повреждения по общей причине» не следует путать с «повреждениями общего характера» (см. МЭК 60050-191).

3.1.7 **систематический отказ** (systematic failure): Отказ, вызванный определенной причиной, который может быть устранен только путем изменения конструкции или с помощью технологического приема, операционных процедур, документации или других существенных факторов.

Примечание 1 — Даже восстановительное техническое обслуживание без модификации обычно не устраняет причину отказа.

Примечание 2 — Систематический отказ может быть вызван имитацией причины отказа по МЭК 60050-191.

Примечание 3 — Примеры причин систематических отказов, зависящих от человеческих ошибок при:
- определении спецификации требований безопасности;
- разработке, производстве, монтаже, работе аппаратного обеспечения;
- разработке, реализации и т. д. программного обеспечения.

3.1.8 **приостановка** (muting): Временное автоматическое прекращение выполнения функции безопасности элементами системы управления, связанными с безопасностью.

3.1.9 **возврат в исходное положение вручную** (manual reset): Функция, свойственная элементам системы управления, связанным с безопасностью, и необходимая для восстановления вручную заданных функций безопасности до повторного пуска машины.

3.1.10 **вред здоровью** (harm): Нанесение физической травмы или причинение ущерба здоровью человека.

3.1.11 **опасность** (hazard): Потенциальная угроза нанесения физической травмы или причинения вреда здоровью человека.

Примечание 1 — Термин «опасность» можно квалифицировать в соответствии с причиной его происхождения (например, механическая опасность, электрическая опасность) или характером потенциального повреждения (например, опасность поражения электрическим током, опасность пореза, опасность воздействия токсических веществ, опасность возгорания).

Примечание 2 — Виды опасностей:
- опасности, постоянно присутствующие в процессе использования машины по назначению (например, опасное перемещение подвижных элементов, дуговой разряд в процессе сварки, вредная для здоровья рабочая поза, эмиссия шума, высокая температура);
- опасности, возникающие неожиданно (например, взрыв, опасность раздавливания вследствие неожиданного/непреднамеренного пуска, выбросы вследствие аварии, падение вследствие ускорения или замедления).

3.1.12 **опасная ситуация** (hazardous situation): Обстоятельства, при которых человек подвергается по меньшей мере одной или нескольким опасностям.

3.1.13 **риск** (risk): Сочетание вероятности нанесения и степени тяжести возможных травм или другого вреда здоровью.

3.1.14 **остаточный риск** (residual risk): Риск, остающийся после принятия защитных мер, рисунок 2.

Примечание — См. ISO 12100, 3.13.

3.1.15 **оценка риска** (risk assessment): Полный процесс, включающий анализ и оценку степени риска (см. ISO 12100, 3.17).

3.1.16 **анализ риска** (risk analysis): Изучение технических характеристик машины в части ограничений, идентификации опасности и предварительная оценка степени риска (см. ISO 12100, 3.15).

3.1.17 **оценка степени риска** (risk evaluation): Сделанное на основе анализа риска заключение о возможности его снижения (см. ISO 12100, 3.16).

3.1.18 **использование машины по назначению** (intended use of machine): Использование машины в соответствии с информацией, содержащейся в документации для пользователя (см. ISO 12100, 3.23).

3.1.19 **прогнозируемое неправильное применение** (reasonably foreseeable misuse): Использование машины способом, не предусмотренным конструктором, но который может быть результатом легко предсказуемого поведения человека (см. ISO 12100, 3.24).

3.1.20 **функция безопасности** (safety function): Функция машины, сбой которой может привести к немедленному возрастанию риска(ов) (см. ISO 12100, 3.30).

3.1.21 **текущий автоматический контроль (мониторинг)** (monitoring): Функция безопасности, которая гарантирует, что предохранительные меры предусматриваются в том случае, если снижается способность компонента или элемента выполнять свои функции или если изменились условия протекания процесса таким образом, что произошло увеличение рисков.

3.1.22 **программируемая электронная система** (programmable electronic system PES): Система для управления, защиты или мониторинга, основанная на использовании одного или нескольких программируемых электронных устройств, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали данных и другие каналы связи, устройства привода и другие устройства вывода.

Примечание — См. IEC 61508-4, 3.3.2.

3.1.23 **уровень эффективности защиты** (performance level, PL): Дискретный уровень, используемый для определения способности элементов систем управления, связанных с обеспечением безопасности, осуществлять функцию безопасности в прогнозируемых условиях.

Примечание — См. 4.5.1.

3.1.24 **требуемый уровень эффективности защиты** (required performance level PL_r): Уровень эффективности защиты (PL), применяемый для установления предела требуемого снижения риска для каждой функции безопасности (см. рисунок 2 и А.1).

3.1.25 **среднее время наработки на опасный отказ** (mean time to dangerous failure, $MTTF_d$): Ожидаемое среднее время наработки до наступления опасного отказа.

Примечание — см. [10], 3.2.34.

3.1.26 **диагностический охват** (diagnostic coverage, DC): Показатель эффективности диагностики, который может быть определен как отношение между вероятностью обнаружения опасных отказов и вероятностью всех опасных отказов.

Примечание 1 — Диагностический охват может существовать как для всей системы управления, связанной с обеспечением безопасности, так и для ее части. К примеру, показатель эффективности диагностики может существовать для сенсорных устройств, и/или логических систем, и/или конечных элементов.

Примечание 2 — см. IEC 61508-4, 3.8.6.

3.1.27 **защитная мера** (protective measure): Мера, предпринимаемая для адекватного снижения степени риска.

Примеры

1 Меры безопасности, установленные разработчиком: определенная конструкция, основные и дополнительные средства защиты, инструкция по эксплуатации.

2 Меры безопасности, установленные пользователем: организация работы (безопасные технологические процессы, контроль, системы доступа к работе), обеспечение и использование дополнительных средств безопасности, средств индивидуальной защиты работников, обучение.

Примечание — см. ISO 12100, 3.19.

3.1.28 **период эксплуатации** (mission time, T_M): Время планируемого использования SRP/CS.

3.1.29 **тестовый показатель** (test rate, r_t): Частота автоматических тестов для определения ошибок в SRP/CS, обратное значение диагностических тест-интервалов.

3.1.30 **показатель запросов** (demand rate, r_d): Частота запросов на осуществление действий SRP/CS.

3.1.31 **ремонтный коэффициент** (repair rate, r_r): Величина обратная периоду времени между моментом определения опасного отказа с помощью онлайн-теста или появления очевидной неисправности системы и моментом возобновления работы после ремонта или замены системы/компонента.

Примечание — Время ремонта не включает период времени, необходимый для обнаружения отказа.

3.1.32 **система управления машиной** (machine control system): Система, которая отвечает на сигналы ввода от частей элементов оборудования, операторов, оборудования внешнего контроля или любой комбинации вышеприведенных элементов и генерирует сигналы вывода, приводящие машину в действие в заданном порядке.

Примечание — Система управления может использовать любую технику или любую комбинацию различных технических средств (например, электрические/электронные, гидравлические, пневматические, механические).

3.1.33 **уровень полноты безопасности** (safety integrity level, SIL): Дискретный уровень (принимающий одно из четырех возможных значений), определяющий требования к полноте безопасности для функций безопасности, который ставится в соответствие E/E/PE-системам, связанным с безопасностью; уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности; уровень, равный 1, отвечает наименьшей полноте безопасности, см. IEC 61508-4, 3.5.6.

3.1.34 **язык программирования с ограниченной изменчивостью** (limited variability language, LVL): Тип языка, который обеспечивает способность сочетания предопределенных атрибутов, библиотечных функций специализированного применения для выполнения технических требований безопасности.

Примечание 1 — См. IEC 61511-1, 3.2.81.1.2.

Примечание 2 — Типовые примеры LVL (язык многозвеньевой логики, язык функциональных блок-схем) представлены в [39].

Примечание 3 — Типовой пример системы, использующей LVL: PLC.

3.1.35 **язык программирования с полной изменчивостью** (full variability language, FVL): Язык, специально созданный для программистов и позволяющий реализовать широкий диапазон функций и прикладных задач.

Пример — C, C++, Assembler.

Примечание 1 — См. IEC 61511-1, 3.2.81.1.3.

Примечание 2 — Типовой пример систем, использующих FVL: встроенные системы.

Примечание 3 — В области оборудования FVL применяется во встроенном программном обеспечении и реже в прикладном программном обеспечении.

3.1.36 **прикладное программное обеспечение** (application software): Программное обеспечение специального применения, внедренное производителем оборудования и обычно содержащее логические последовательности (ряды), пределы и функции, которые контролируют соответствующие сигналы ввода, вывода, вычисления и решения, необходимые для обеспечения исполнения требований SRP/CS.

3.1.37 **встроенное программное обеспечение (системное)** (embedded software, irmware, system software): Программное обеспечение, которое является частью системы, поставляемой производителем, и которое недоступно для изменения пользователем оборудования.

Примечание — Встроенное программное обеспечение всегда написано на языке FVL.

3.2 Обозначения и сокращения

Обозначения и сокращения приведены в таблице 2.

Таблица 2

Обозначения и сокращения	Характеристика на языке		Появление в тексте
	английском	русском	
a, b, c, d, e	Denotation of performance levels	Обозначение уровней эффективности защиты	Таблица 3
AOPD	Active optoelectronic protective device (e. g. light barrier)	Активное оптоэлектронное защитное устройство	Приложение H
B, 1, 2, 3, 4	Denotation of categories	Обозначение категорий	Таблица 7
B_{10d}	Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components)	Количество циклов наработки до наступления опасного отказа для числа компонентов до 10 % (для пневматических и электромеханических компонентов)	Приложение C
Cat.	Category	Категория	3.1.2
CC	Current converter	Преобразователь тока	Приложение I
CCF	Common cause failure	Отказ по общей причине (независимый)	3.1.6
DC	Diagnostic coverage	Диагностический охват	3.1.26
DC_{avg}	Average diagnostic coverage	Средний диагностический охват (мера диагностики)	E.2
F, F1, F2	Frequency and/or time of exposure to the hazard	Частота и/или время подверженности риску	A.2.2
FB	Function block	Функциональный блок	4.6.3
FVL	Full variability language	Язык программирования с полной изменчивостью (системный)	3.1.35
FMEA	Failure modes and effects analysis	Метод анализа состояний и последствий отказа	7.2
I, I1, I2	Input device, e. g. sensor	Входное устройство, например, датчик	6.2
i, j	Index of counting	Индекс расчетный	Приложение D
I/O	Inputs/outputs	Вход/ выход	Таблица E.1
i_{ab}, i_{bc}	Interconnecting means	Средства соединения	Рисунок 4
K1A, K1B	Contactors	Замыкатель, контактор	Приложение I
L, L1, L2	Logic	Логика, логические элементы	6.2
LVL	Limited variability language	Язык программирования с ограниченной изменчивостью (оперативного программирования)	3.1.34
M	Motor	Двигатель	Приложение I
MTTF	Mean time to failure	Среднее время наработки на отказ	Приложение C

Окончание таблицы 2

Обозначения и сокращения	Характеристика на языке		Появление в тексте
	английском	русском	
$MTTF_d$	Mean time to dangerous failure	Среднее время наработки на опасный отказ, сбой	3.1.25
n, N, $\bar{N}$	Number of items	Количество позиций	6.3, D.1
N_{low}	Number of SRP/CS with PL_{low} in a combination of SRP/CS	Число элементов систем управления, связанных с безопасностью, с нижним уровнем эффективности защиты комбинированных элементов системы управления, связанных с безопасностью	6.3
O, O1, O2, OTE	Output device, e. g. actuator	Выходное устройство, например, привод	6.2
P, P1, P2	Possibility of avoiding the hazard	Вероятность избежать опасности	A.2.3
PES	Programmable electronic system	Программируемая электронная система	3.1.22
PL	Performance level	Уровень эффективности защиты	3.1.23
PLC	Programmable logic controller	Программируемый логический контроллер	Приложение I
PL_{low}	Lowest performance level of a SRP/CS in a combination of SRP/CS	Нижний уровень эффективности защиты комбинированных элементов системы управления, связанных с безопасностью	6.3
PL_r	Requires performance level	Требуемый уровень эффективности защиты	3.1.24
r_d	Demand rate	Показатель запросов	3.1.30
RS	Rotation sensor	Датчик вращения	Приложение I
S, S1, S2	Severity of injury	Тяжесть травмирования	A.2.1
SW1A, SW1B, SW2	Position switches	Положения переключателей	Приложение I
SIL	Safety integrity level	Уровень полноты безопасности	Таблица 4
SRASW	Safety-related application software	Прикладное программное обеспечение функций безопасности	4.6.3
SRESW	Safety-related embedded software	Встроенное программное обеспечение функций безопасности	4.6.2
SRP	Safety-related part	Элемент, отвечающий за безопасность	Общее
SRP/CS	Safety-related part of a control system	Элемент системы управления, связанный с безопасностью	3.1.1
TE	Test equipment	Испытательное оборудование	6.2
T_M	Mission time	Период эксплуатации	3.1.28

4 Вопросы конструирования

4.1 Цели безопасности при конструировании

SRP/CS, следует рассчитывать и конструировать так, чтобы полностью учитывались принципы, изложенные в ISO 12100 и ISO 14121 (см. рисунки 1 и 3). Все возможные преднамеренные злоупотребления и предусмотренное использование должны быть учтены заранее.

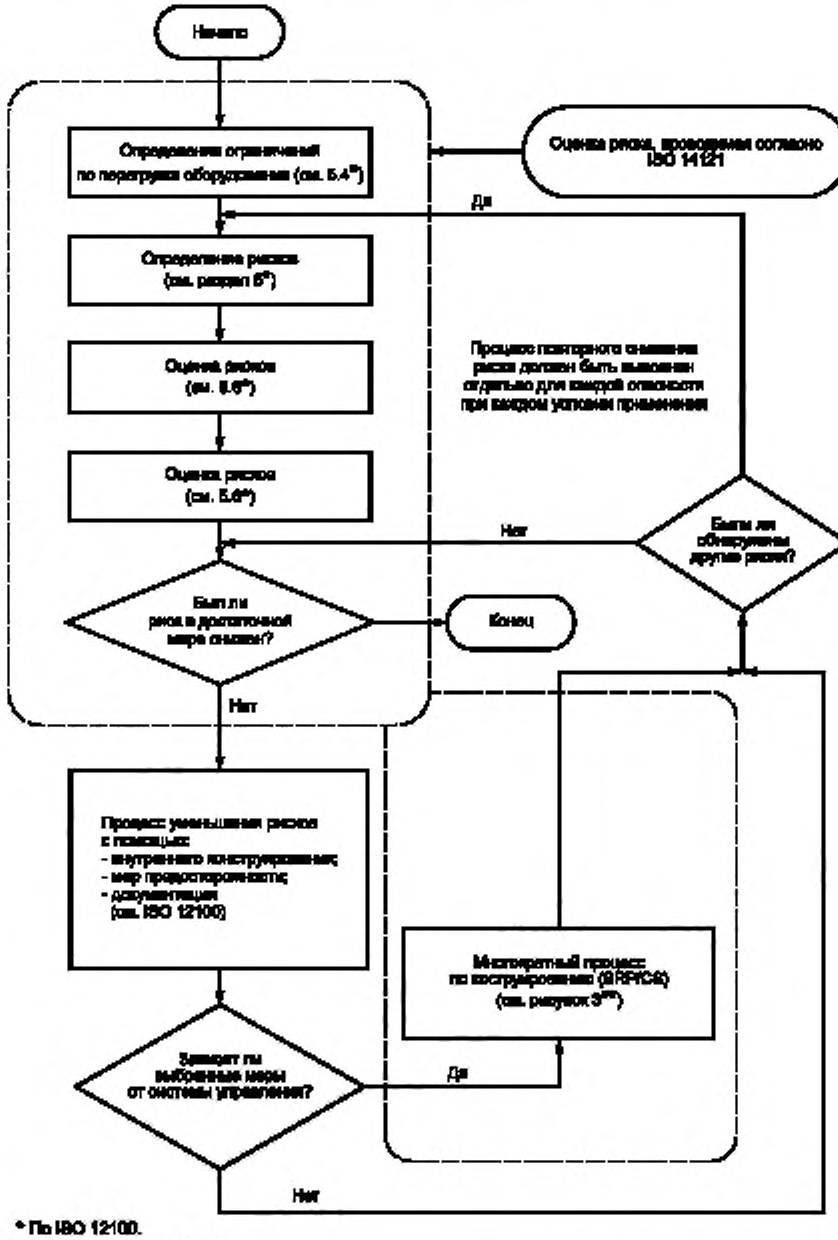


Рисунок 1 — Обзор оценки и снижения риска

4.2 Стратегии по снижению риска

4.2.1 Общие положения

Порядок действий по снижению риска приведен в разделе 4, остальные инструкции содержатся в 6.2 (меры по разработке безопасной конструкции самой машины) и 6.3 (средства защиты и дополнительные защитные меры) ISO 12100. Этот порядок действий учитывает весь жизненный цикл оборудования.

Процесс устранения или понижения рисков на машине связывается с принятием следующих мер:

- устранение или снижение рисков с помощью конструирования (6.2, ISO 12100);
- обеспечение безопасности при помощи мер предосторожности и дополнительных защитных мер (6.2, ISO 12100);
- снижение рисков с помощью предоставления документации по остаточным рискам (6.6, ISO 12100).

4.2.2 Влияние уменьшения риска на системы управления

Целью всего конструирования в целом является достижение безопасности (см. 4.1). Конструирование SRP/CS и снижение рисков являются лишь частью процедуры конструирования машины. SRP/CS обеспечивает функцию безопасности в PL, который достигает требуемого снижения риска. В процессе выполнения функции безопасности — будь то сама часть системы, управление ограждением или предохранительным устройством, конструирование SRP/CS — это всего лишь часть методики уменьшения рисков. Это многократный процесс, и он проиллюстрирован на рисунках 1 и 3.

Для каждой функции безопасности необходимо специфицировать и документировать ее свойства (см. раздел 5) и требуемые уровни эффективности защиты, согласно перечню требований.

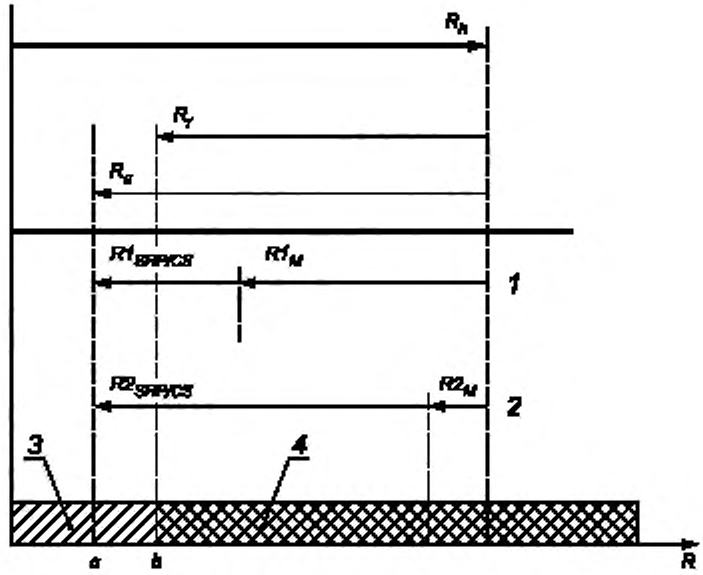
В настоящем стандарте уровни эффективности защиты определены в единицах вероятности возникновения опасного отказа в час (наработка на отказ). Пять уровней эффективности защиты (от *a* до *e*) представлены с интервалами значений вероятности возникновения опасного отказа в течение часа в таблице 3.

Таблица 3 — Уровень эффективности защиты

Уровень эффективности защиты (PL)	Средняя вероятность возникновения опасного отказа в час
a	$\geq 10^{-5}$ до $< 10^{-4}$
b	$\geq 3\times10^{-6}$ до $< 10^{-5}$
c	$\geq 10^{-6}$ до $< 3\times10^{-6}$
d	$\geq 10^{-7}$ до $< 10^{-6}$
e	$\geq 10^{-8}$ до $< 10^{-7}$
Примечание — Кроме среднего значения вероятности возникновения опасного отказа в течение часа для достижения необходимого PL нужно также учитывать и другие критерии.	

Исходя из оценки риска (см. ISO 14121) для данной машины, конструктор должен определить вклад в снижение риска, который необходимо обеспечить с помощью каждого SRP/CS. Этот вклад не включает общий риск управляемой машины, например связанный с эксплуатацией механического пресса или стиральной машины, а только часть риска, снижение которого обеспечивается применением определенных функций безопасности. Примером таких функций является функция останова, выполняемая путем использования электрочувствительного предохранительного устройства механического пресса, или функция блокирования двери стиральной машины.

Снижение риска может быть достигнуто применением различных мер (как SRP/CS, так и другими) с достижением в итоге безопасных условий (см. рисунок 2).



R_h — определенный для каждой опасной ситуации риск, возникший до принятия мер безопасности; R_r — необходимые меры по снижению риска; R_a — текущее состояния снижения риска, достигнутое путем применения мер безопасности; *1* — решение 1 — существенная часть мер по снижению риска, не относящихся к *SRP/CS* (механические меры), остальная часть относится к *SRP/CS*; *2* — решение 2 — существенная часть мер по снижению риска, относящихся к *SRP/CS* (световая завеса), остальная часть не относится к *SRP/CS*; *3* — риск, сниженный в достаточной мере; *4* — недостаточно сниженный риск; *R* — риск; a — остаточный риск после выполнения решений 1 или 2; *b* — риск снижен в достаточной мере; $R1_{SRP/CS}$ $R2_{SRP/CS}$ — уменьшение риска за счет использования функции безопасности, реализованной *SRP/CS*; $R1_M$, $R2_M$ — уменьшение риска за счет использования защитных мер, отличных от *SRP/CS* (например, механической защиты)

Примечание — Для получения подробной информации об уменьшении риска см. ISO 12100.

Рисунок 2 — Обзор процесса снижения риска для каждой опасной ситуации

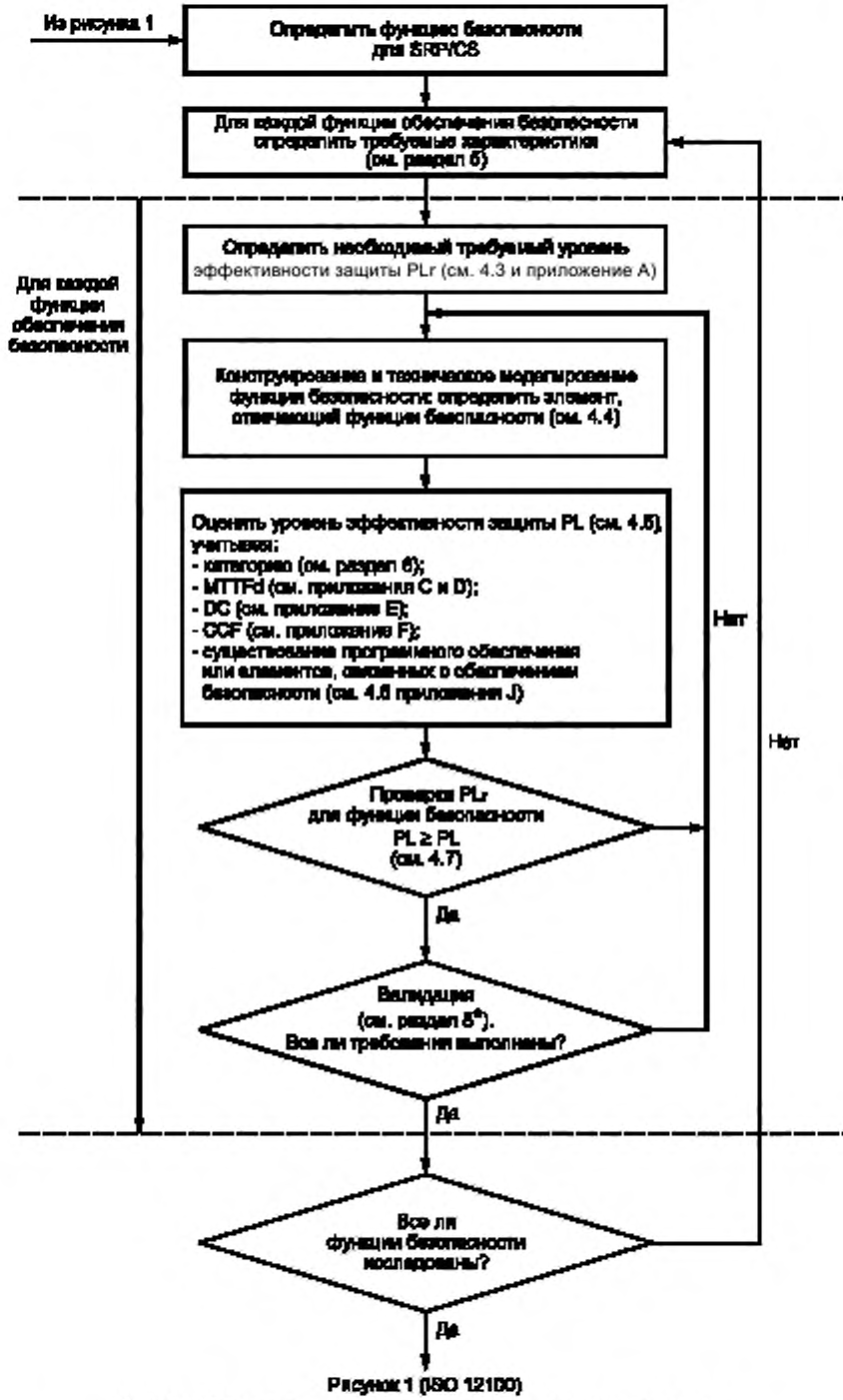


Рисунок 1 (ISO 12100)

*ISO 13849-2 предоставляет дополнительную помощь по валидации.

Рисунок 3 — Многократный (интерактивный) подход к процессу конструирования элементов системы управления, отвечающих за обеспечение безопасности

4.3 Выбор требуемого уровня эффективности защиты (PL_r)

Для каждой функции безопасности, выполняемой SRP/CS, должен быть выбран и задокументирован PL_r (см. приложение А относительно определения PL_r). Выбор требуемого уровня эффективности защиты — это результат оценки риска и анализа степени уменьшения риска, выполненных элементами систем управления, связанными с безопасностью.

Чем больше требуется снизить риск применением SRP/CS, тем выше должен быть PL_r (рисунок 2).

4.4 Конструирование элементов системы управления, связанных с безопасностью (SRP/CS)

Элементы, снижающие риск, определяют безопасность функционирования машин. Элементы, обеспечивающие безопасность, обеспечивают безопасность управления, блокируя, в частности, непредусмотренный запуск в работу.

Функция безопасности может быть реализована с помощью одного или нескольких SRP/CS, в то же время несколько функций безопасности могут относиться к одному SRP/CS (например, логическое устройство, регулятор мощности). Также возможно, что один SRP/CS реализует функцию безопасности и стандартную функцию управления. Конструктор может использовать любые доступные технологии, по одной или в сочетании друг с другом. SRP/CS может также выполнять и эксплуатационную функцию (например, в AOPD как средство включения цикла).

На рисунке 4 представлена диаграмма функции безопасности, отражающая комбинации SRP/CS для:

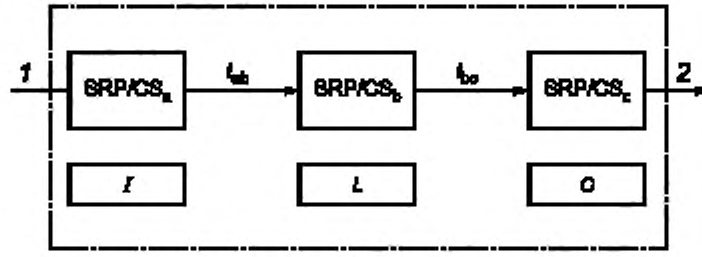
- входных устройств (SRP/CS_a);
- логических блоков/обработки (SRP/CS_b);
- выходных/силовых управляющих элементов (SRP/CS_c) и
- средств соединения (интерфейсов: например, электрических, оптических) (i_{ab}, i_{bc}).

Примечание 1 — Для одной и той же машины необходимо проводить различие между различными функциями безопасности и связанными с ними SRP/CS, реализующими определенную функцию безопасности.

Определяя функцию безопасности для системы управления, конструктор должен определить и элемент обеспечения безопасности (см. рисунки 1 и 3) и, где это необходимо, привязать ее ко входу, логической схеме и выходу и в случае резервирования к отдельным каналам, а затем оценить уровень эффективности защиты PL (см. рисунок 3).

Примечание 2 — Указанная структура представлена в разделе 6.

Примечание 3 — Все интерфейсы включены в элементы обеспечения безопасности.



I — ввод, *L* — логический элемент; *O* — вывод; *1* — событие инициации (например, ручная активация нажимной кнопки, открытие предохранительного приспособления, прерывание пучка AOPD); *2* — силовой привод механизма (например, тормоз двигателя)

Рисунок 4 — Схематическое изображение комбинации элементов системы управления, связанных с безопасностью, для осуществления типичной функции безопасности

4.5 Оценка достигнутого уровня эффективности защиты (PL) и его соотношение с уровнем полноты безопасности (SIL)

4.5.1 Уровень эффективности защиты (PL)

Способность узлов, связанных с осуществлением безопасности, выполнять функцию безопасности выражается посредством определения уровня эффективности защиты.

Для каждого выбранного SRP/CS и/или комбинации SRP/CS, которые выполняют функцию безопасности, должна быть выполнена оценка PL.

PL узла SRP/CS должен определяться посредством оценки следующих аспектов:

- значений $MTTF_d$ для отдельных компонентов (см. приложение C и D);
- DC (см. приложение E);
- CCF (см. приложение F);
- структуры (см. раздел 6);
- работы функции безопасности в условиях неисправности (см. раздел 6);
- программного обеспечения, связанного с обеспечением безопасности (см. 4.6 и приложение J);
- систематических отказов (см. приложение G);
- способностей выполнять функцию безопасности при ожидаемых условиях окружающей среды.

Примечание 1 — Могут иметь определенное влияние другие параметры, например, аспекты эксплуатации, коэффициент (частота) запросов, коэффициент тестирования.

Аспекты могут быть сгруппированы по двум методам, касающимся процедуры оценки:

a) выражаемые количественно аспекты (значение $MTTF_d$ для отдельных компонентов, DC, CCF, структура);

b) не выражаемые количественно качественные аспекты, которые влияют на работу SRP/CS (режим работы функции безопасности в условиях неисправности; программное обеспечение, связанное с обеспечением безопасности; систематический отказ и условия окружающей среды).

Среди выражаемых количественно аспектов вклад надежности (например, $MTTF_d$, структура) может варьироваться в используемых технологиях. Например, возможно (в определенных рамках), что один канал узлов высокой надежности, связанных с обеспечением безопасности, в одной технологии дает такой же или выше PL, что и отказоустойчивая конструкция более низкой надежности в другой технологии.

Существует несколько методов оценки выражаемых количественно аспектов PL для любого типа системы (например, комплексная конструкция), таких как модель Маркова, обобщенная стохастическая сеть Петри (GSPN), блок-схема надежности (см., например, IEC 61508).

Для облегчения оценки количественных аспектов PL предоставлен упрощенный порядок, основанный на определении пяти указанных структур, которые отвечают специфическим критериям разработки и работают в условиях неисправности (см. 4.5.4).

Для SRP/CS или комбинации SRP/CS, разработанных в соответствии с требованиями, данными в разделе 6, средняя вероятность опасного отказа может определяться посредством рисунка 5 и процедуры, данной в приложениях A — H, J и K.

Для SRP/CS, которое отклоняется от указанного построения, должен быть проведен детальный расчет, чтобы продемонстрировать достижение PL_r.

В прикладных программах, в которых SRP/CS может считаться простым и необходимый уровень эффективности защиты — от *a* до *c*, качественная оценка PL может быть подтверждена расчетным логическим обоснованием.

Примечание 2 — Для разработки сложных систем управления, таких как PES, предназначенной для выполнения функций безопасности, может оказаться приемлемым применение других стандартов (например, [5], [6], [7], [8], [9], [10] и [2], [3], [4]).

Достижение качественных аспектов PL может быть продемонстрировано применением рекомендованных мероприятий, приведенных в 4.6 и приложении G.

В соответствии с серией стандартов IEC 61508 способность систем управления, связанных с обеспечением безопасности, выполнять функцию безопасности дается через SIL. Таблица 4 демонстрирует отношение между двумя понятиями (PL и SIL).

PL *a* не имеет соответствия на шкале SIL и в основном используется для снижения риска легкой, обычно обратимой травмы. Поскольку SIL 4 предназначен для катастрофических событий, возможных в перерабатывающей промышленности, этот диапазон не является существенным для оценки рисков механизмов. Следовательно, PL *e*, соответствующий SIL 3, определяется как самый высокий уровень.

Таблица 4 — Отношение между уровнем эффективности защиты PL и уровнем полноты безопасности SIL

PL	SIL (IEC 61508-1, для информации) интенсивный/непрерывный режим работы
a	Нет соответствия
b	1
c	1
d	2
e	3

Принципиально должны применяться следующие защитные меры по снижению риска:

- снижение вероятности возникновения неисправностей на компонентном уровне. Цель — снизить вероятность возникновения неисправностей или отказов, которые влияют на функцию безопасности. Это может быть сделано посредством увеличения надежности компонентов, например, отбором успешно испытанных компонентов, и/или применения хорошо проверенных принципов безопасности, чтобы минимизировать или исключить опасные неисправности или нарушения (отказ) (см. ISO 13849-2);

- улучшение конструкции SRP/CS. Цель — избежать опасных последствий неисправности. Некоторые неисправности могут быть выявлены, и потребуется резервирование и/или мониторинг конструкции.

Обе меры могут применяться отдельно или в комбинации. В некоторых технологиях снижение риска может быть достигнуто посредством отбора надежных компонентов и исключением неисправностей; но в других технологиях снижение риска может потребовать дополнительной и/или мониторинговой системы. В дополнение должны суммарно учитываться отказы по общей причине (CCF) (см. рисунок 3).

Особенности структурных построений см. в разделе 6.

4.5.2 Среднее время наработки на опасный отказ каждого канала ($MTTF_d$)

Значение $MTTF_d$ каждого канала дано по трем уровням (см. таблицу 5) и должно браться в расчет для каждого канала (например, одиночный канал, каждый канал дополнительной системы) отдельно.

В соответствии с $MTTF_d$ в расчет может приниматься максимальное значение 100 лет.

Таблица 5 — Среднее время наработки на опасный отказ каждого канала ($MTTF_d$)

$MTTF_d$	
Обозначение каждого канала	Диапазон времени каждого канала
Низкое	3 года ≤ $MTTF_d$ < 10 лет
Среднее	10 лет ≤ $MTTF_d$ < 30 лет
Высокое	30 лет ≤ $MTTF_d$ < 100 лет

Примечание 1 — Выбор диапазонов $MTTF_d$ каждого канала основан на интенсивности (частоте) отказов в области существующих технологий, образуя нечто вроде логарифмической шкалы, соответствующей логарифмической PL-шкале. Значение $MTTF_d$ каждого канала существующего SRP/CS менее трех лет предположительно нельзя найти, поскольку это бы означало, что после одного года около 30 % всех систем на рынке сломались бы, и их необходимо бы было заменить. Значение $MTTF_d$ каждого канала более 100 лет неприемлемо, т. к. SRP/CS для крупных рисков не должен зависеть от надежности только одних компонентов. Чтобы защитить SRP/CS от систематических и случайных неисправностей, должны понадобиться дополнительные средства, такие как резервирование. Для использования на практике количество диапазонов было сокращено до трех. Ограничение значений $MTTF_d$ каждого канала до максимума 100 лет относится к SRP/CS, которые выполняют функцию безопасности. Более высокие значения $MTTF_d$ могут использоваться для одинарных компонентов (см. таблицу D.1).

Примечание 2 — Указанные в данной таблице границы имеют точность 5 %.

Для оценки $MTTF_d$ компонента необходима последовательная процедура в следующем порядке:

a) использование данных производителя;

b) использование методов, приведенных в приложении C и D;

c) выборка в диапазоне 10 лет.

4.5.3 Диагностический охват (DC)

Значение DC распределено по четырем уровням (см. таблицу 6).

Для оценки DC в большинстве случаев могут использоваться метод анализа состояния и последствий отказа (FMEA, см. [32]) или подобные методы. В этом случае должны рассматриваться все характерные неисправности и/или виды отказов, и должен быть проверен PL комбинации SRP/CS, выполняющих функцию безопасности, в сравнении с PL_r. Упрощенный подход к оценке DC см. в приложении Е.

Таблица 6 — Мера диагностического охвата (DC)

DC	
Обозначение	Диапазон
Никакое	DC < 60 %
Низкое	60 % ≤ DC < 90 %
Среднее	90 % ≤ DC < 99 %
Высокое	99 % ≤ DC

Примечание 1 — Для SRP/CS, состоящего из нескольких частей, используется средний диагностический охват DC_{avg} вместо DC, изображенного на рисунке 5, раздел 6 и Е.2.

Примечание 2 — Выбор диапазонов DC основан на ключевых значениях 60, 90 и 99 %, также используемых в других стандартах (например, IEC 61508), имеющих дело с тестами оценки диагностического охвата. (1 — DC) для ключевых значений 60, 90 и 99 % образует нечто вроде логарифмической шкалы, соответствующей логарифмической PL-шкале. Значение DC менее 60 % оказывает лишь небольшое влияние на надежность тестируемой системы и, следовательно, называется «никакое». Значения DC свыше 99 % для сложных систем очень сложно достичь. Для практичности количество диапазонов было сокращено до четырех. Указанные в данной таблице границы имеют точность 5 %.

4.5.4 Упрощенный порядок оценки уровня эффективности защиты (PL)

PL может быть оценен посредством учета всех существенных параметров и соответствующих методов для расчета (см. 4.5.1).

Данный пункт описывает упрощенную процедуру оценки PL узлов SRP/CS, основанную на регламентированных построениях. Некоторые другие построения с подобной структурой могут трансформироваться в данные регламентированные построения для того, чтобы осуществить оценку PL.

Регламентированные построения представлены в виде блок-схем и перечислены в контексте каждой категории в 6.2. Информация о методе блок-схем и блок-схемах, связанных с обеспечением безопасности, дана в 6.2. и приложении В.

Регламентированные построения демонстрируют логическое представление о структуре системы для каждой категории. Техническая реализация или, например, принципиальная схема функционирования могут выглядеть совершенно по-другому.

Регламентированные построения вычерчены для комбинированных SRP/CS, начинающихся в точках, в которых возникают сигналы, связанные с обеспечением безопасности, и заканчивающихся на выводе элементов включения-выключения питания (см. также ISO 12100, приложение А). Регламентированные построения могут также использоваться, чтобы описывать часть или подчасть системы управления, которая отвечает на входящие сигналы и генерирует выходные сигналы, связанные с обеспечением безопасности. Элемент «ввода» может представлять собой, например, световую завесу (AOPD), также как и входные цепи логических элементов управления или входные переключатели. «Вывод» может также представлять собой, например, переключающее устройство выходного сигнала (OSSD) или выводы лазерных сканеров.

Для регламентированных построений сделаны следующие типовые допущения:

- заданная продолжительность работы — 20 лет (см. раздел 10);
- частота отказов постоянная в течение заданной продолжительности работы;
- для категории 2 частота (коэффициент) запросов ≤ 1/100 частоты (коэффициента) тестирования;
- для категории 2 $MTTF_{d,\ TE\ (контрольно\text{-}измерительный\ прибор)}$ больше половины $MTTF_{d,\ L\ (логический\ элемент)}$.

Примечание — Когда блоки каждого канала не могут быть разделены, может применяться следующее допущение: $MTTF_d$ суммированного тестового канала (TE, OTE) больше половины $MTTF_d$ суммируемого рабочего канала (I — входное устройство, L — логический элемент, O — устройство вывода).

Методика рассматривает категории как построения с определенным DC_{avg}. PL каждого узла SRP/CS зависит от структуры, среднего времени наработки на опасный отказ каждого канала ($MTTF_d$) и от DC_{avg}.

Отказ по общей причине (CCF) также должен приниматься в расчет (инструкцию см. в Приложении F).

Для SRP/CS с программным обеспечением применяются требования из 4.6.

Если количественные данные недоступны или не используются (например, системы низкой сложности), должен быть выбран самый худший показатель всех существенных параметров.

Комбинация SRP/CS или одинарный SRP/CS могут иметь PL. Комбинация нескольких SRP/CS с различными PL рассматривается в 6.3.

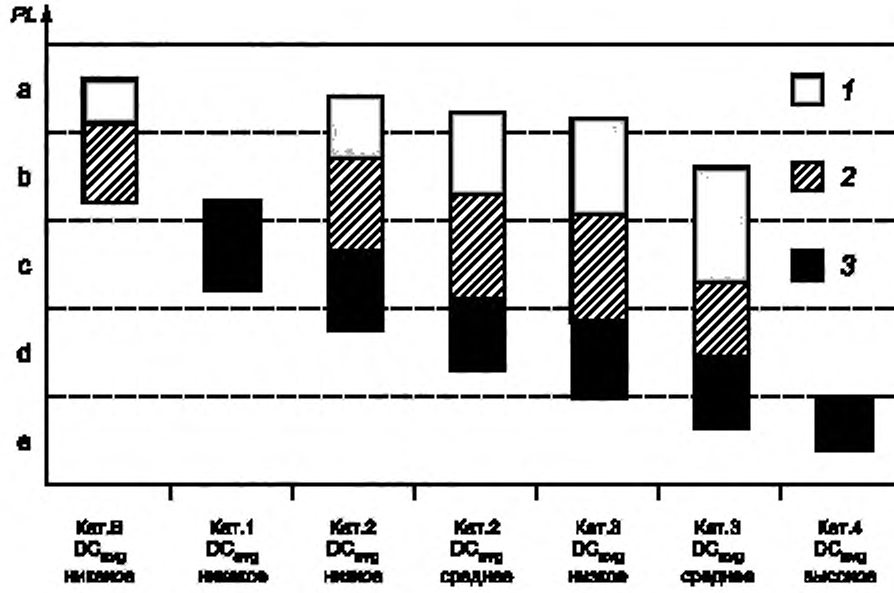
В случае применений PL_r от *a* до *c* меры по избеганию неисправностей могут быть достаточными; при применении большего риска PL_r — от *d* до *e* конструкция SRP/CS может обеспечить меры по избеганию, обнаружению или преодолению неисправностей. Практические меры включают избыточность, разнообразие, контроль (см. также ISO 12100, раздел 3 и IEC 60204-1).

На рисунке 5 демонстрируется процедура выбора категорий в комбинации с $MTTF_d$ каждого канала и DC_{avg} для достижения необходимого PL функции безопасности.

Для оценки PL на рисунке 5 демонстрируются различные возможные комбинации категории с DC_{avg} (горизонтальная ось) и $MTTF_d$ каждого канала (столбцы). Столбцы на диаграмме представляют собой три диапазона $MTTF_d$ каждого канала (низкий, средний и высокий), которые могут быть выбраны для достижения необходимого PL.

До использования упрощенного подхода на рисунке 5 (который представляет результаты различных моделей Маркова, основанных на указанных построениях раздела 6) должна быть определена категория SRP/CS, также как DC_{avg} и $MTTF_d$ каждого канала (см. раздел 6 и приложения C — E).

Для категорий 2, 3 и 4 должны быть предприняты достаточные меры против отказов по общей причине (инструкцию см. в приложении F). Учитывая эти параметры в сумме, рисунок 5 представляет графический метод определения PL, достигнутого SRP/CS. Комбинация категории (включая отказ по общей причине) и DC_{avg} определяет, какая колонка на рисунке 5 должна быть выбрана. В соответствии с $MTTF_d$ каждого канала должна быть выбрана одна из трех различных закрашенных областей соответствующей колонки.



PL — уровень эффективности защиты; *1* — $MTTF_d$ каждого канала — низкое; *2* — $MTTF_d$ каждого канала — среднее; *3* — $MTTF_d$ каждого канала — высокое

Рисунок 5 — Отношения между категориями DC_{avg}, $MTTF_d$ каждого канала и PL

Расположение данной области по вертикали определяет достигнутый PL, который может быть считан по вертикальной оси. Если область охватывает два или три PL_S, то достигнутый PL дан в таблице 7. Для более точного выбора показателя PL, зависящего от точного значения $MTTF_d$ каждого канала, см. приложение К.

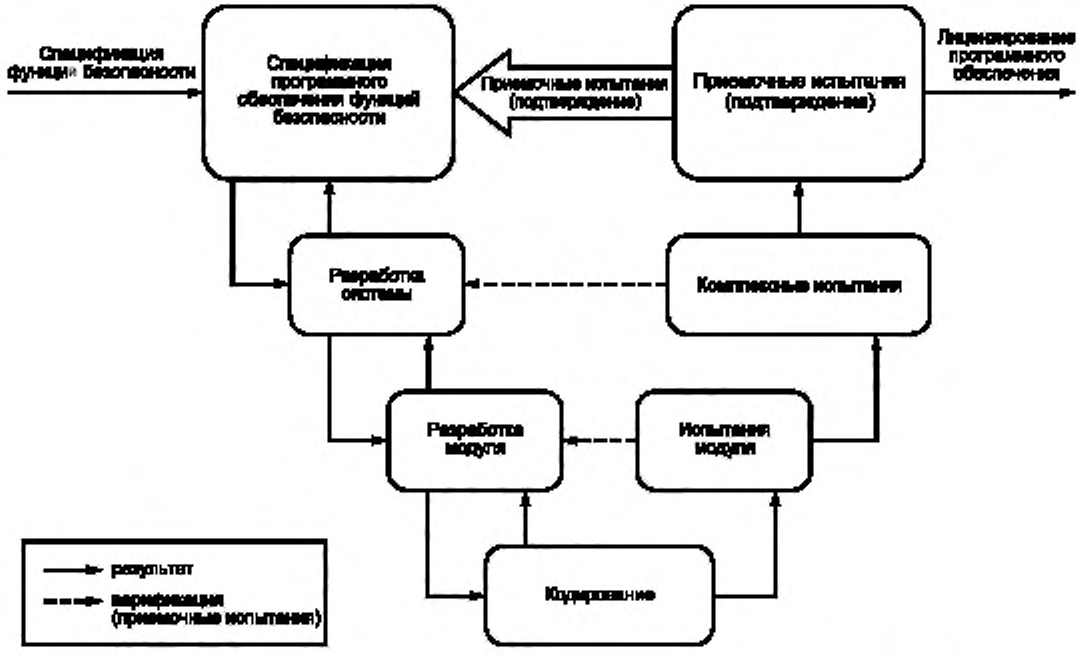
Таблица 7 — Упрощенная процедура оценки уровня эффективности защиты PL, достигнутого узлом SRP/CS

Категория	B	1	2	2	3	3	4
DC_{avg}	никакое	никакое	низкое	среднее	низкое	среднее	высокое
$MTTF_d$ каждого канала							
Низкое	*a*	Не покрывается	*a*	*b*	*b*	*c*	Не покрывается
Среднее	*b*	Не покрывается	*b*	*c*	*c*	*d*	Не покрывается
Высокое	Не покрывается	*c*	*c*	*d*	*d*	*d*	*e*

4.6 Требования к безопасности программного обеспечения

4.6.1 Общие принципы

Вся работа на протяжении срока службы встроенного или прикладного программного обеспечения функций безопасности должна быть в первую очередь направлена на повышение надежности самого программного обеспечения во время срока службы (см. рисунок 6). Основная цель следующих требований — иметь читабельное, понятное, тестируемое и ремонтируемое программное обеспечение.



Примечание — Приложение J дает детальные рекомендации по работе в течение срока службы.

Рисунок 6 — Упрощенная V-модель срока службы программного обеспечения функций безопасности

4.6.2 Встроенное программное обеспечение функций безопасности (SRESW)

Для компонентов SRESW с PL_r от *a* до *d* должны применяться следующие основные меры:

- срок службы программного обеспечения с верификацией и приемочными испытаниями, см. рисунок 6;
- документирование спецификации и конструкции;
- модульная и структурная разработка и кодирование;
- контроль систематических отказов (см. G.2);
- использование мер, основанных на программном обеспечении, для контроля случайных отказов аппаратных средств, проверки правильного применения;
- функциональные испытания, например, испытание черного ящика;
- соответствующие работы по безопасности программного обеспечения в течение срока службы после модификаций.

Для компонентов SRESW с PL_r от *c* до *d* должны применяться следующие дополнительные меры:

- менеджмент качества сопоставляемых систем при конструировании, например, в соответствии с IEC 61508 или [18];
- документирование всей деятельности, взаимосвязанной с жизненным циклом программного обеспечения;
- менеджмент по идентификации всех форм и документов, связанных с реализацией SRESW;
- структурированные технические требования, включая требования по безопасности, и конструирование;
- использование подходящих языков программирования и компьютерных средств;
- модульное и структурное программирование, разделение в области программных способов и средств обеспечения безопасности, модули ограниченного размера с полностью заданным интерфейсом, применение стандартов конструирования и кодирования;
- проверка кодирования сквозным контролем/пересмотром, включая анализ потока управления;
- расширенное функциональное тестирование, например тестирование методом серого ящика, испытание для определения рабочих характеристик или моделирование;
- анализ воздействий и проведение соответствующих работ по безопасности программного обеспечения в течение срока службы после внесения изменений.

Компоненты SRESW с $PL_r = e$ должны соответствовать IEC 61508, раздел 7, с подходящим SIL 3. С учетом отличий в области технических требований, конструирования и кодирования для двух каналов, применяемых в SRP/CS с категориями 3 или 4 и $PL_r = e$, оценка может быть проведена с помощью вышеупомянутых критериев для $PL_r = c$ или *d*.

Примечание 1 — Для более подробного описания данных критериев см. IEC 61508-7.

Примечание 2 — Для SRESW с отличиями в области конструирования и кодирования, а также для компонентов, используемых в SRP/CS с категориями 3 или 4, затраты на принятие мер с целью исключения систематических отказов могут быть сокращены, например, проверкой компонентов программного обеспечения с учетом только структурных аспектов вместо проверки каждой строки кода.

4.6.3 Прикладное программное обеспечение функций безопасности (SRASW)

Срок службы программного обеспечения, связанного с безопасностью (см. рисунок 6) также относится к SRASW (см. приложение J).

SRASW, написанные на языке LVL и отвечающие следующим требованиям, могут иметь PL от *a* до *e*. Если SRASW написано на языке FVL, то должны применяться требования к SRESW, уровень PL от *a* до *e* может быть достигнут. Если элемент SRASW в пределах одной компоненты имеет какое-либо влияние (например, по причине модификации) на несколько функций безопасности с различными PL, то следует применять требования, относящиеся к высшим уровням PL. Следующие основные критерии должны применяться к компонентам SRASW с PL_r от *a* до *e*:

- цикл разработки с процессами контроля и подтверждения, см. рисунок 6;
- документирование технических требований и разработки;
- модульное и структурное программирование;
- функциональное испытание;
- соответствующие опытно-конструкторские работы после модификаций.

Для компонентов SRASW с PL_r от *c* до *e* необходимо или рекомендовано применение следующих мер с целью повышения эффективности (низкая эффективность $PL_r = c$, средняя эффективность $PL_r = d$, высокая эффективность $PL_r = e$):

a) спецификация программного обеспечения функций безопасности должна быть проверена (см. приложение J), доступна каждому человеку, участвующему в жизненном цикле, а также должна содержать описание:

1) функций безопасности с требуемым уровнем PL и связанных с ними рабочих режимов;

2) критериев эффективности, например, времени срабатывания;

3) структуры комплекса аппаратных средств с интерфейсом внешних сигналов;

4) выявления и контроля внешнего отказа;

b) выбора инструментов, библиотек, языков:

1) подходящие инструменты: для уровня PL = *e*, достигнутого одним компонентом и его инструментом, инструмент должен отвечать соответствующим требованиям безопасности; если используются два различных компонента с различными инструментами, то может быть достигнут достаточный уровень достоверности. Должны учитываться технические параметры, определяющие условия возникновения систематической ошибки (такие как несоответствие типов данных, неопределенное размещение динамического запоминающего устройства, незавершенный интерфейс, рекурсия, адресная арифметика с указателями). Проверки должны проводиться главным образом во время компиляции, а не только во время рабочего цикла. Инструменты должны вводить в действие подмножества языка и директивы кодирования или, по крайней мере, контролировать и направлять пользователя, использующего их;

2) при условии целесообразности и практической применимости должны использоваться утвержденные библиотеки функциональных блоков (FB), или библиотеки FB, связанные с безопасностью и обеспеченные производителем инструмента (особо рекомендовано для уровня PL = *e*), или утвержденные библиотеки прикладных специальных FB в соответствии с настоящим стандартом;

3) для модульного подхода должно применяться утвержденное LVL-подмножество, например, принятое подмножество языков [39]. Особо рекомендовано использование графических языков (например, функциональная блок-схема, релейная диаграмма);

c) разработка программного обеспечения должна содержать в себе:

1) полуформальные методы описания данных и потока управляющих сигналов, например, диаграмма состояний или блок-схема программы;

2) модульное и структурное программирование, осуществленное преимущественно функциональными блоками, входящими в состав утвержденных библиотек функциональных блоков, связанных с обеспечением безопасности;

3) функциональные блоки ограниченного размера кодирования;

4) запуск программного кода внутри функционального блока, который должен иметь один вход и один выход;

5) архитектурную трехступенчатую модель, Входные сигналы => Обработка => Выходные сигналы (см. рисунок 7 и приложение J);

6) размещение выходного сигнала безопасности только в одном месте программы;

7) использование методов выявления внешнего отказа и защитного программирования в пределах блоков входного сигнала, обработки и выходного сигнала, что приводит к безопасному состоянию;

Рисунок 7 — Общая архитектурная модель программного обеспечения

d) когда SRASW и не SRASW объединены в один компонент:

1) SRASW и не SRASW должны быть закодированы в разных функциональных блоках с четко определенными каналами передачи данных;

2) не должно быть логического объединения данных, связанных и не связанных с обеспечением безопасности, что может привести к снижению полноты сигналов, связанных с безопасностью, например, объединение связанных и не связанных с безопасностью сигналов логическим «ИЛИ», когда результат управляет сигналами, связанными с обеспечением безопасности;

e) внедрение/кодирование программного обеспечения:

1) код должен быть четким, понятным и тестируемым, поэтому должны использоваться символьные переменные (вместо подробного описания адресов технических средств);

2) должны использоваться подтвержденные или принятые рекомендации по выполнению кодирования;

3) должны применяться проверки целостности и достоверности данных (например, проверка попадания в интервал), доступные на прикладном уровне (защитное программирование);

4) код должен быть проверен моделированием;

5) верификация должна проводиться посредством контроля и анализа потока данных для уровня PL = *d* или *e*;

f) тестирование:

1) подходящим методом подтверждения является тестирование функционального поведения, а также критериев эффективности (например, эффективность использования рабочего времени) методом черного ящика;

2) для PL = *d* или *e* рекомендуется использование тестовых вариантов, полученных на основе анализа граничных значений;

3) рекомендуется проводить планирование испытаний, причем планирование должно включать в себя тестовые варианты с критериями завершения и требуемыми программными средствами;

4) тестирование входов/выходов должно гарантировать, что сигналы, связанные с безопасностью, правильно использованы в рамках SRASW;

g) документирование:

1) весь жизненный цикл программного обеспечения, а также работы, связанные с модификацией, должны быть снабжены документацией;

2) документация должна быть полной, доступной, четкой и ясной;

3) документация системы кодирования в пределах исходного текста должна содержать заголовки модулей, указывающие на область применения, описание функциональных задач и входов/выходов, информацию о версии системы кодирования и версии используемых функциональных блоков библиотек, а также необходимые ссылки на интернет-ресурсы/официальные отчеты и строки-описания;

h) верификация[1]

Пример — Анализ, проверка, сквозной контроль или другие подходящие меры.

i) управление конфигурацией

Настоятельно рекомендуется ввести резервные копии данных и процедур с целью последующей идентификации и архивирования документов, программных модулей, результатов верификации/валидации, а также конфигурации программных средств, относящихся к особой версии SRASW;

j) модификации

После модификации SRASW должен быть проведен анализ воздействий с целью обеспечения технических требований. Также после модификации должны быть проведены соответствующие работы, касающиеся жизненного цикла программного обеспечения. Права доступа к модификациям должны находиться под контролем, история модификаций должна быть задокументирована.

Примечание — Модификации не затрагивают уже используемые системы.

4.6.4 Параметризация на основе программного обеспечения

Программная параметризация показателей, связанных с обеспечением безопасности, должна рассматриваться в качестве аспекта безопасности конструкции SRP/CS, которые должны быть описаны в спецификации требований по безопасности программного обеспечения. Параметризация должна проводиться при использовании предназначенных для этого программных средств, предусмотренных поставщиком SRP/CS. Эти программные средства должны иметь свои параметры для идентификации (название, номер версии и т. д.), а также предотвращать несанкционированные изменения, например, с помощью защиты паролем.

[1] Верификация необходима только для программы специального назначения, а не для утвержденных библиотечных функций.

Полнота данных, используемых для параметризации, должна поддерживаться на необходимом уровне, что может быть достигнуто применением мер по отношению к контролю:

- диапазона допустимых входных данных;
- искажения данных перед их передачей;
- влияния ошибок, начиная с процесса передачи параметров;
- влияния неполной передачи параметров;
- влияния сбоев и отказов технических средств и программного обеспечения средств, используемых для параметризации.

Средства параметризации должны отвечать всем требованиям, установленным для SRP/CS в соответствии с настоящим стандартом. В качестве альтернативы должна использоваться особая процедура для определения параметров, связанных с безопасностью. Данная процедура должна включать подтверждение входных параметров по отношению к элементам SRP/CS или

- повторной передачей измененных параметров к инструменту параметризации, или
- другими подходящими средствами подтверждения полноты параметров,

также как и последующее подтверждение, например, с привлечением подготовленного специалиста или средствами автоматической проверки инструментом параметризации.

Примечание 1 — Особенно важно в тех случаях, когда параметризация проводится средствами, не предназначенными для этого (например, с помощью персонального компьютера или аналогичного средства).

Для того чтобы избежать систематических отказов, программные модули для кодирования/декодирования в процессе передачи/повторной передачи данных, а также модули для визуализации параметров, связанных с безопасностью, должны как минимум иметь различия внутри функции(й).

Документы на параметризацию, основанную на программном обеспечении, должны содержать используемые данные (например, предопределенные наборы параметров), а также информацию, необходимую для идентификации параметров, связанных с SRP/CS, специалистом(ми), выполняющим(ми) параметризацию, наряду с другой значимой информацией, такой как дата проведения параметризации.

Следующие мероприятия по верификации должны применяться к параметризации, основанной на программном обеспечении:

- проверка правильности настройки каждого параметра, связанного с безопасностью (минимум, максимум и характерные значения);
- подтверждение того, что параметры, связанные с безопасностью, проверены на достоверность, например, использованием недопустимых значений и т. д.;
- проверка защиты от несанкционированных изменений параметров, связанных с безопасностью;
- проверка того, что данные/сигналы параметризации сформированы и обработаны так, что отказы не приведут к потере функции безопасности.

Примечание 2 — Особенно важно в тех случаях, когда параметризация проводится средствами, не предназначенными для этого (например, с помощью персонального компьютера или аналогичного средства).

4.7 Проверка достигнутого уровня эффективности защиты (PL) соответствующему требуемому уровню эффективности защиты (PL_r)

Для каждой конкретной функции безопасности PL, связанный с SRP/CS, должен соответствовать PL_r, установленному в пункте 4.3 (см. рисунок 3). Если это не так, то необходимо повторение в процессе, описанном на рисунке 3.

PL различных SRP/CS, которые являются элементами функции безопасности, должен быть больше или равен PL_r этой функции безопасности.

4.8 Эргономические принципы конструирования

Взаимодействие между операторами и SRP/CS должно проектироваться и устанавливаться так, чтобы никто не подвергался опасности при всех режимах предназначенного использования и возможных случаях неправильного использования машины (см. также ISO 12100, [19], [20], [21], раздел 10 [29], [30], [38], [41], [44]).

Эргономические принципы следует применять так, чтобы машину и систему управления, включая элементы, обеспечивающие безопасность, можно было легко использовать и не провоцировать оператора работать опасным способом.

Следует применять требования безопасности для соблюдения эргономических принципов, указанных в 6.2.8 ISO 12100.

5 Функции безопасности

5.1 Спецификация функций безопасности

В настоящем разделе приведен перечень и характеристики функций безопасности, которые могут быть соблюдены с помощью SRP/CS. Конструктор (или разработчик стандарта типа С) должен выбирать необходимые функции безопасности из этого перечня, чтобы получить требуемые меры безопасности от системы управления для заданного применения.

Пример — Функция останова, предотвращение внезапного пуска, ручной возврат, приостановка, ручная приостановка функций безопасности.

Примечание — Системы управления оборудованием обеспечивают операционные функции и/или функции безопасности. Операционные функции (например, пуск, нормальный останов) также могут быть функциями безопасности, но это может быть установлено только после полной оценки риска на используемом оборудовании.

В таблицах 8 и 9 перечислены типовые функции безопасности, некоторые их характеристики и параметры, связанные с обеспечением безопасности, а также приведены ссылки на другие международные стандарты, в которых изложены требования, относящиеся к функциям безопасности, их характеристикам и параметрам. Конструктор (или разработчик стандарта типа С) должен гарантировать, что требования этих стандартов удовлетворяются для функций безопасности, приведенных в таблицах.

В данном разделе приведены дополнительные требования к некоторым характеристикам функций безопасности.

При необходимости характеристики функций должны быть адаптированы для использования при питании от разных источников энергии.

Так как большинство ссылок, содержащихся в таблицах 8 и 9, относятся к стандартам электротехники, то необходимо, чтобы требования были адаптированы для использования другого вида оборудования (например, гидравлического, пневматического).

При идентификации функции(й) безопасности должны учитываться следующие условия:

a) результаты оценки риска, связанного с каждой опасностью или опасной ситуацией;

b) эксплуатационные характеристики машины, в том числе:

- предназначенное использование машины (включая возможные случаи неправильного использования);
- режимы работы (например, автономный режим, автоматический режим, режимы, относящиеся к конкретной зоне или части машины);
- продолжительность цикла;
- время срабатывания;

c) аварийный режим работы;

d) описание взаимодействия различных рабочих процессов и работ, выполняемых вручную (ремонт, наладка, диагностика неисправностей и т. д.);

e) режим работы машины, который должен быть обеспечен или предотвращен функцией безопасности;

f) условие(я) (например, рабочий режим), при котором(ых) машина будет находиться в рабочем или нерабочем состоянии;

g) частота эксплуатации;

h) приоритет тех функций, которые могут действовать одновременно и вызвать противоречивые действия.

5.2 Элементы функций безопасности

5.2.1 Функция останова

Функция останова (например, включаемая защитным устройством) (см. в таблице 8) должна сразу после его срабатывания переводить машину в безопасное состояние. Такой останов должен пользоваться приоритетом перед остановом машины по операционным причинам.

При совместной работе группы машин в согласованном режиме необходимо предусмотреть подачу сигнала в диспетчерское управление и/или на другие машины о существовании такого состояния останова.

Примечание — Такой останов может вызывать операционные проблемы и трудности повторного пуска, например, при электродуговой сварке. С целью уменьшения вероятности отмены функции останова ее выпол-

нение может быть начато с останова машины по операционным причинам для завершения текущей операции и подготовки к быстрому и свободному повторному пуску из позиции останова (например, без ущерба произведенной продукции). Единственное решение — это применение блокировочных устройств с защитными фиксаторами, причем защитный фиксатор отключается, когда рабочий цикл достигает определенного состояния, при котором возможно свободное выполнение повторного пуска.

Таблица 8 — Международные стандарты, относящиеся к типовым функциям безопасности машин и некоторым их характеристикам

Функция безопасности/ характеристика	Требование(я)		Дополнительная информация
	Настоящий стандарт	ИСО 12100	
Функция останова, включаемая защитным устройством[a)]	5.2.1	3.28.8, 6.2.11.3	9.2.2, 9.2.5.3, 9.2.5.5 [29]
Ручной возврат	5.2.2	—	9.2.5.3, 9.2.5.4 [29]
Пуск и повторный пуск	5.2.3	6.2.11.3, 6.2.11.4	9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6 [29]
Функция местного управления	5.2.4	6.2.11.8, 6.2.11.10	10.1.5 [29]
Приостановка	5.2.5	—	—
Ручная приостановка функций безопасности		перечисление b) 6.2.11.8	9.2.6.1 [29]
Управление разблокированием		—	9.2.6.3, 10.9 [29]
Предотвращение внезапного пуска	—	6.2.11.4	[27], 5.4 [29]
Освобождение и спасение заблокированных людей	—	6.3.5.3	—
Отключение и рассеяние энергии	—	6.3.5.4	[27], 5.3, 6.3.1 [29]
Режимы управления и выбор режима	—	6.2.11.8, 6.2.11.10	9.2.3, 9.2.4 [29]
Взаимодействие между разными элементами систем управления, связанными с обеспечением безопасности	—	6.2.11.1 (последнее предложение)	9.3.4 [29]
Контроль параметризации входных величин, связанных с обеспечением безопасности	4.6.4	—	—
Функция аварийного останова[b)]	—	6.3.5.2	[13], 9.2.5.4 [29]
[a)] Включая ограждения с блокировкой и ограничители (например, на превышение скорости, температуры, давления). [b)] Дополнительные меры защиты смотрите в ISO 12100.			

Таблица 9 — Международные стандарты, содержащие требования к некоторым функциям безопасности и параметрам, связанным с обеспечением безопасности

Функция безопасности/параметр, связанный с обеспечением безопасности	Требование		Дополнительная информация
	Настоящий стандарт	ISO 12100	
Время срабатывания	5.2.6	—	3.2, A.3, A.4 [26]
Параметры, связанные с обеспечением безопасности (скорость, температура или давление)	5.2.7	перечисление e) 6.2.11.8	7.1, 9.3.2, 9.3.4 [29]
Колебания, отключение и восстановление источников питания	5.2.8	перечисление e) 6.2.11.8	4.3, 7.1, 7.5 [29]
Сигналы и устройства предупреждения	—	6.2.8	[10], [17], [22], [23], 10.3, 10.4 [29], [38], [39]

5.2.2 Ручной возврат

После подачи предохранительным устройством команды «Останов» состояние останова должно поддерживаться до тех пор, пока не будут созданы безопасные условия для повторного пуска.

Восстановление функции безопасности путем возврата предохранительного устройства отменяет команду «Останов». Отмена команды «Останов» должна быть подтверждена вручную, отдельным и преднамеренным действием (ручным возвратом) (см. в таблице 8).

Функция ручного возврата:

- должна быть обеспечена с помощью отдельного и вручную управляемого устройства в пределах SRP/CS;
- должна быть выполнена только в случае, если действуют все функции безопасности и предохранительные устройства;
- не должна сама инициировать движение или создавать опасную ситуацию;
- должна исполняться преднамеренным действием;
- должна подготавливать систему управления для приема отдельной команды «Останов»;
- должна применяться только путем выключения исполнительного механизма, находящегося в положении «включено».

Уровень эффективности безопасности элементов, связанных с обеспечением безопасности и выполняющих функцию ручного возврата, должен выбираться так, чтобы включение функции ручного возврата не снижало требуемый уровень безопасности соответствующей функции.

Исполнительный механизм возврата должен находиться за пределами опасной зоны и в безопасном положении, из которого хорошо видно, что в пределах опасной зоны никого нет.

Требуется отдельная процедура возврата, когда нет полной видимости в пределах опасной зоны.

Примечание — Единственное решение — это применение второго исполнительного механизма возврата. Функция возврата запускается в пределах опасной зоны первым исполнительным механизмом в сочетании со вторым, расположенным за пределами опасной зоны (около предохранительного устройства). Необходимо, чтобы данная процедура возврата была реализована за ограниченное время перед тем, как система контроля примет отдельную команду «Пуск».

5.2.3 Пуск и повторный пуск

Повторный автоматический запуск должен осуществляться только в том случае, если опасная ситуация больше не существует. В частности, для блокировочных устройств с функцией пуска следует применять 6.3.3.2.5 ISO 12100.

Требования к пуску и повторному пуску (см. в таблице 8) должны также применяться к машинам, которые имеют дистанционное управление.

Примечание — Сигнал с датчика обратной связи, поступающий в систему управления, может включить автоматический повторный пуск.

Пример — В автоматическом режиме работы сигналы с датчика обратной связи, поступающие в систему управления, часто применяются для контроля технологического процесса. Если заготовка вышла из позиции, то происходит останов технологического процесса. Если мониторинг блокировочных устройств не превосходит автоматическое регулирование процесса, то может возникнуть опасность повторного пуска машины в то время, когда оператор меняет заготовку. Поэтому повторный пуск от пульта дистанционного управления не должен выполняться до тех пор, пока предохранительное устройство снова не включится и оператор не покинет опасную зону. Содействие функции предотвращения внезапного пуска, обеспеченного системой управления, зависит от результатов оценки риска.

5.2.4 Функция местного управления

При местном управлении машиной (см. в таблице 8), например с помощью переносного устройства управления или подвесного пульта, должны выполняться следующие требования:

- средства, выбранные для местного управления, должны быть расположены за пределами опасной зоны;
- запуск опасных условий эксплуатации в локальной зоне с оцененным риском должен быть возможен только от одного устройства местного управления;
- переключение управления между местным и главным не должно создавать опасную ситуацию.

5.2.5 Приостановка

Приостановка (см. в таблице 8) не должна приводить к опасным для человека ситуациям. Во время приостановки безопасные условия должны быть обеспечены другими средствами.

В конце приостановки должны быть восстановлены все функции безопасности SRP/CS.

Уровень эффективности безопасности элементов, связанных с безопасностью и выполняющих функцию приостановки, должен выбираться таким, чтобы включение функции приостановки не снижало требуемый уровень безопасности соответствующей функции.

Примечание — При некоторых применениях требуется сигнал, указывающий на приостановку.

5.2.6 Время срабатывания

Должно быть указано время срабатывания SRP/CS (см. в таблице 9), если это необходимо, исходя из оценки риска.

Примечание — Время срабатывания системы управления — это часть общего времени срабатывания машины. Необходимое общее время срабатывания машины может влиять на конструкцию элементов, связанных с обеспечением безопасности, например, вызывать необходимость в обеспечении системы торможения.

5.2.7 Параметры, связанные с обеспечением безопасности

Если параметры SRP/CS, например расположение, скорость, температура, давление (см. в таблице 9), отклоняются от заданных пределов, то система управления должна инициировать соответствующие действия, например, включение останова, сигнала предупреждения, аварийного сигнала.

Если ошибки ручного ввода данных по обеспечению безопасности в программируемые электронные системы ведут к возникновению опасной ситуации, то в этом случае в пределах системы управления, связанной с обеспечением безопасности, должна устанавливаться система проверки данных, например проверка пределов ограничений, формата и/или логических входных значений.

5.2.8 Колебания, отключение и восстановление источников питания

Дополнение к требованиям, приведенным в таблице 9.

Если возникают колебания, выводящие энергетические уровни за пределы расчетного рабочего диапазона, в том числе внезапное отключение энергоснабжения, то элементы системы управления, связанные с безопасностью, должны продолжать выдавать или инициировать передачу выходного(ых) сигнала(ов), который(ые) позволяет(ют) другим машинам поддерживать безопасное состояние (см. в таблице 9).

6 Категории и их связь со средним временем наработки на опасный отказ ($MTTF_d$) каждого из каналов, средним диагностическим охватом (DC_{avg}) и отказом по общей причине (CCF)

6.1 Общие положения

SRP/CS должны соответствовать требованиям одной или нескольких из пяти категорий, установленных в 6.2.

Категории являются основными параметрами, используемыми для достижения определенного PL.

Категория B является основной. Возникновение неисправности может повлечь за собой потерю функции безопасности. Для категории 1 повышенная стойкость к неисправностям достигается преимущественно путем выбора и применения компонентов. Для категорий 2, 3 и 4 улучшение рабочих характеристик в отношении заданной функции безопасности достигается преимущественно путем совершенствования структуры SRP/CS. Для категории 2 это обеспечивается периодической проверкой выполнения функции заданной безопасности. Для категорий 3 и 4 совершенствование структуры обеспечивается тем, что одиночная неисправность не ведет к потере функции безопасности. Для категории 4 и там, где практически целесообразно для категории 3, такие неисправности будут обнаружены. Для категории 4 устанавливается стойкость элементов к накоплению неисправностей.

В таблице 10 дан обзор по категориям SRP/CS, приведены требования и поведение системы управления в случае неисправности.

При рассмотрении причин отказа некоторых компонентов можно исключать возникновение определенных неисправностей (см. раздел 7).

Выбор категорий для конкретного SRP/CS главным образом зависит от:

- снижения риска, которое достигается за счет функции безопасности, выполняемой элементом системы управления;

- требуемого уровня эффективности защиты (PL_r);
- применяемых технологий;
- возникновения риска в случае неисправности(ей) элемента;
- возможности избежать неисправности(ей) элемента (систематические ошибки);
- возможности возникновения неисправности(ей) элемента и соответствующих параметров;
- среднего времени наработки на опасный отказ ($MTTF_d$);
- диагностического охвата (DC);
- отказа по общей причине (CCF) в случае применения категорий 2, 3 и 4.

6.2 Характеристики категорий

6.2.1 Общие положения

Каждый SRP/CS должен соответствовать требованиям категорий, см. 6.2.3—6.2.7.

Нижеприведенная структура отвечает требованиям соответствующей категории.

Нижеприведенные рисунки являются не примерами, а общими структурами. Всегда возможно отклонение от данных структурных построений, но любое отклонение должно быть подтверждено аналитическими методами (например, моделированием Маркова, анализом диагностического дерева отказов) и система управления должна соответствовать PL_r.

Структурные построения не должны рассматриваться только в качестве принципиальных схем, поскольку они также являются и логическими схемами. Для категорий 3 и 4 это означает, что не все элементы обязательно являются резервными, однако существуют резервные средства обеспечения того, что неисправность не приведет к потере функции безопасности.

Линии и стрелки на рисунках 8—12 являются средствами логической связи и средствами логической диагностики.

6.2.2 Структурные построения

Структура SRP/CS является ключевой характеристикой, оказывающей большое влияние на PL. Даже если существует множество возможных структур, то основные принципы построения все равно часто похожи. Таким образом, большинство структур, присутствующих в сфере оборудования, могут быть сопоставлены с одной из категорий. Типовым представлением каждой категории является представление в виде структурной схемы. Такое типовое представление называется структурным построением и содержится в описании каждой категории.

Важно отметить, что PL, показанный на рисунке 5 и зависящий от категории $MTTF_d$ каждого канала и DC_{avg}, основан на структурном построении. Если рисунок 5 применяется для оценки PL, то структура SRP/CS должна быть представлена в соответствии со структурным построением требуемой категории. В целом схемы, отображающие характеристики категорий, эквивалентны соответствующим структурным построениям категорий.

Примечание — В некоторых случаях, исходя из особых технических решений или рекомендаций, установленных стандартом типа С, эффективность SRP/CS может быть достигнута только категорией без дополнительного PL_r. В таких особых случаях безопасность обеспечивается структурой, и требования к $MTTF_d$, DC и CCF не применяются.

6.2.3 Категория B

SRP/CS должны быть, как минимум, разработаны, сконструированы, выбраны, смонтированы и соединены согласно соответствующим стандартам с использованием основных принципов безопасности для конкретного применения с тем, чтобы они могли выдерживать:

- ожидаемые эксплуатационные нагрузки, например, надежность в отношении отключающей способности и частоты;
- влияние обрабатываемого материала, например, стойкость стиральной машины к воздействию моющих средств;
- другие соответствующие внешние воздействия, например, механическую вибрацию, электромагнитные помехи, отключение или другие нарушения в области электроснабжения.

В пределах систем с категорией B не существует среднего диагностического охвата ($DC_{avg} = 0$) и $MTTF_d$ каждого канала может быть снижено до среднего уровня. В таких структурах (обычно одноканальных системах) CCF не является значимым.

Максимально возможный PL достигается категорией B — PL = *b*.

Примечание — Возникновение неисправности может привести к потере функции безопасности.

Специальные требования к электромагнитной совместимости можно найти в соответствующих стандартах на продукцию, например, в [35] для систем силовых приводов. Требования по устойчивости относятся, в частности, и к функциональной безопасности SRP/CS. Если таких стандартов на продукцию нет, то во всяком случае должны быть соблюдены требования [34].

i_m — средства связи; *I* — входное устройство, например, датчик; *L* — логический блок; *O* — выходное устройство, например, главный контактор

Рисунок 8 — Структурное построение для категории B

6.2.4 Категория 1

Для категории 1 следует применять требования категории B согласно 6.2.3 и требования, приведенные далее.

SRP/CS, которым присвоена категория 1, разрабатывают и конструируют с использованием успешно испытанных компонентов и хорошо проверенных принципов безопасности (см. ISO 13849-2).

«Успешно испытанный компонент» для применений, связанных с обеспечением безопасности, — это компонент, который или

a) широко использовался в прошлом с успешными результатами в подобных применениях, или

b) изготовлен и проверен с использованием принципов, которые демонстрируют его пригодность и надежность для применений, связанных с обеспечением безопасности.

Вновь разработанные компоненты и принципы безопасности могут считаться эквивалентом «успешно испытанного компонента», если они удовлетворяют условиям перечисления b).

Решение о приемке индивидуального компонента как «успешно испытанного» зависит от конкретного применения.

Примечание — Многофункциональные электронные компоненты (например, PLC, микропроцессор, интегральная схема специального назначения) не могут считаться эквивалентами «успешно испытанных компонентов».

Значение $MTTF_d$ для каждого канала должно быть большим.

Максимально возможный PL с категорией 1 — PL = *c*.

Примечание 1 — В пределах систем с категорией 1 не существует среднего диагностического охвата (DC_{avg} = 0). В таких структурах (обычно одноканальных системах) CCF не является значимым.

Примечание 2 — Возникновение неисправности может привести к потере функции безопасности. Однако значение $MTTF_d$ каждого канала с категорией 1 больше, чем для элементов, которым присвоена категория B. Следовательно, потеря функции безопасности менее вероятна.

Важно иметь четкое различие между «успешно испытанными компонентами» и «исключением неисправностей» (см. раздел 7). Проверка компонента на принадлежность к «успешно испытанным» зависит от его применения. Например, позиционный выключатель с принудительным размыканием контактов может считаться «успешно испытанным компонентом» станка, в то время как в пищевой промышленности он не может считаться таковым: например, в молочной промышленности выключатель будет разрушаться после нескольких месяцев взаимодействия с молочной кислотой. Исключение неисправностей может привести к очень высокому уровню эффективности защиты, однако необходимые меры по исключению неисправностей должны проводиться на протяжении всего жизненного цикла устройства. Для того чтобы гарантировать высокий PL, необходимо применение дополнительных мер за пределами системы управления. Для позиционного выключателя приведены некоторые примеры подобных мер, средства:

- обеспечения фиксации выключателя после его настройки;
- обеспечения фиксации кулачка;
- обеспечения поперечной устойчивости кулачка;
- предотвращения смещения позиционного выключателя из рабочего положения, например, обеспечение достаточной прочности крепления демпфера и установочных приспособлений;
- защиты от внешнего воздействия.

i_m — средства связи; I — входное устройство, например, датчик; L — логический блок; O — выходное устройство, например, главный контактор

Рисунок 9 — Структурное построение для категории 1

6.2.5 Категория 2

Для категории 2 следует применять требования категории B согласно 6.2.3. Необходимо соответствовать «хорошо проверенным принципам безопасности» согласно 6.2.4 и требованиям, приведенным далее.

SRP/CS категории 2 должны быть разработаны так, чтобы их функции проверялись системой управления машины через соответствующие интервалы. Проверку функций безопасности следует осуществлять:

- при пуске машины;
- до возникновения любой опасной ситуации, например при запуске нового цикла и/или периодически в процессе работы, если оценка риска и характер работы указывают на ее необходимость.

Запуск процедуры проверки может осуществляться автоматически. Любая проверка функции(й) безопасности должна:

- разрешать работу, если не было обнаружено никаких неисправностей;
- вырабатывать выходной сигнал, который вызывает соответствующее управляющее воздействие, если обнаружена неисправность.

Когда это возможно, выходной сигнал должен обеспечивать безопасное состояние. Безопасное состояние должно поддерживаться до момента устранения неисправности. При невозможности соблюдения безопасного состояния (например, сварка контакта в конечном устройстве коммутации) выходной сигнал должен обеспечивать предупреждение об опасности.

Для структурного построения категории 2, как показано на рисунке 10, при расчете значений $MTTF_d$ и DC_{avg} следует учитывать только блоки функциональных каналов (т. е. I, L и O на рисунке 10) и не учитывать блоки каналов испытаний (т. е. TE и OTE на рисунке 10).

Значение DC_{avg} SRP/CS, включая обнаружение неисправностей, должно быть малым. $MTTF_d$ каждого канала должно находиться в диапазоне от малого до большого в зависимости от PL_r. Должны быть приняты меры, направленные на предотвращение CCF (см. приложение F).

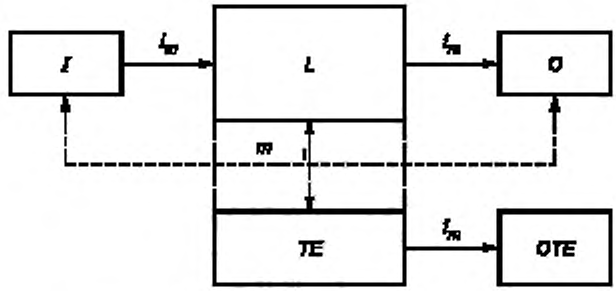
Сама проверка не должна создавать опасную ситуацию (например, вследствие увеличения времени срабатывания). Контролирующие устройства могут быть неотъемлемой частью или находиться отдельно от элемента(ов), выполняющего(их) функцию безопасности.

Максимально возможный уровень эффективности защиты с категорией 2 — PL = *d*.

Примечание 1 — В некоторых случаях категория 2 неприменима, потому что нельзя применять проверку функции безопасности ко всем элементам.

Примечание 2 — Поведение системы управления категории 2 допускает, что:
- возникновение неисправности может вызывать потерю функции безопасности между проверками;
- потерю функции безопасности обнаруживают проверкой.

Примечание 3 — Принцип, который обеспечивает действие функции категории 2, заключается в том, что принятое техническое обеспечение, например выбор частоты проведения контроля, может снизить вероятность возникновения опасной ситуации.



Пунктирные линии означают обнаружение неисправности, целесообразное с практической точки зрения.

i_m — средства связи; *I* — входное устройство, например, датчик, *L* — логический блок; *m* — мониторинг; *O* — выходное устройство, например, главный контактор; *TE* — испытательное оборудование; *OTE* — выходные сигналы испытательного оборудования

Рисунок 10 — Структурное построение для категории 2

6.2.6 Категория 3

Для категории 3 следует применять требования категории B согласно 6.2.3. Необходимо соответствовать «хорошо проверенным принципам безопасности» согласно 6.2.4 и требованиям, приведенным далее.

SRP/CS категории 3 должны быть разработаны так, чтобы одиночная неисправность в любом из этих элементов не приводила к потере функции безопасности. Когда практически целесообразно, одиночная неисправность должна быть обнаружена во время или до следующего требования по функции безопасности.

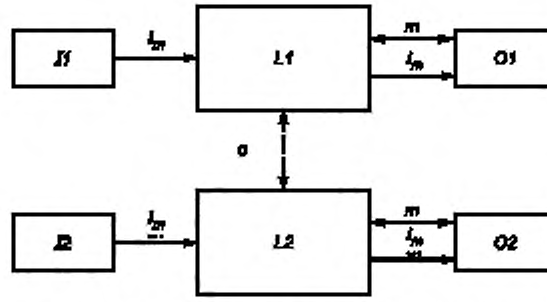
Значение DC_{avg} всех SRP/CS, включая обнаружение неисправностей, должно быть малым. $MTTF_d$ резервированных каналов должно находиться в диапазоне от малого до большого в зависимости от PL_r. Должны быть приняты меры, направленные на предотвращение CCF (см. приложение F).

Примечание 1 — Требование обнаружения одиночной неисправности не означает, что все неисправности будут обнаружены. Следовательно, накопление необнаруженных неисправностей может привести к появлению непреднамеренного выходного сигнала и возникновению опасной ситуации в машине. Типовыми примерами практических мер по обнаружению неисправности является применение обратной связи контактов реле с механическим управлением и контроль резервных электрических выходных сигналов.

Примечание 2 — Если необходимо по причинам технологии и применения, то разработчики стандарта типа C должны более подробно характеризовать обнаружение неисправностей.

Примечание 3 — Поведение системы управления категории 3 допускает, что:
- при возникновении одиночной неисправности функция безопасности всегда выполняется;
- некоторые, но не все неисправности будут обнаружены;
- накопление необнаруженных неисправностей может привести к потере функции безопасности.

Примечание 4 — Используемая технология будет влиять на возможность осуществления мер по обнаружению неисправностей.



Пунктирные линии означают обнаружение неисправности, целесообразное с практической точки зрения.

i_m — средства связи; *c* — перекрестный мониторинг; *I1*, *I2* — входное устройство, например, датчик; *L1*, *L2* — логический блок; *m* — контроль, *O1*, *O2* — выходное устройство, например, главный контактор

Рисунок 11 — Структурное построение для категории 3

6.2.7 Категория 4

Для категории 4 следует применять требования категории B согласно 6.2.3. Необходимо соответствовать «хорошо проверенным принципам безопасности» согласно 6.2.4 и следующим требованиям.

SRP/CS категории 4 должны быть разработаны так, чтобы:

- одиночная неисправность в любом из этих элементов не приводила к потере функции безопасности;
- одиночная неисправность обнаруживалась во время или до следующего требования по функции безопасности, например, сразу при включении, при окончании рабочего цикла машины.

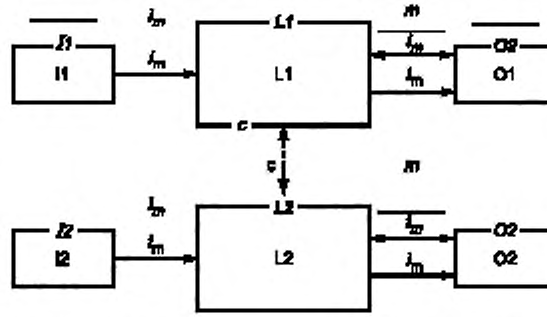
Если такое обнаружение невозможно, то накопление неисправностей не должно приводить к потере функции безопасности.

Значение DC_{avg} всех SRP/CS, включая накопление неисправностей, должно быть большим. $MTTF_d$ каждого из резервированных каналов должно быть большим. Должны быть приняты меры, направленные на предотвращение CCF (см. приложение F).

Примечание 1 — Поведение системы управления категории 4 допускает, что:
- при возникновении неисправностей функция безопасности всегда выполняется;
- неисправности будут обнаруживаться своевременно, чтобы предотвратить потерю функции безопасности;
- учтено накопление необнаруженных неисправностей.

Примечание 2 — Различие категорий 3 и 4 заключается в более высоком значении DC_{avg} для категории 4, а также в том, что требуемое значение $MTTF_d$ каждого канала должно быть строго большим.

На практике рассмотрение комбинации из двух неисправностей может являться достаточным.



Сплошные линии означают диагностический охват, значение которого для категории 4 больше, чем в структурном построении для категории 3.

i_m — средства связи; *c* — перекрестный мониторинг; *I1*, *I2* — входное устройство, например, датчик; *L1*, *L2* — логический блок; *m* — контроль; *O1*, *O2* — выходное устройство, например, главный контактор

Рисунок 12 — Структурное построение для категории 4

Таблица 10 — Краткое изложение требований для категорий

Категория	Краткое изложение требований	Поведение системы	Принципы достижения безопасности	$MTTF_d$ каждого канала	DC_{avg}	CCF
B (см. 6.2.3)	SRP/CS и/или их предохранительные устройства, а также их компоненты должны быть разработаны, сконструированы, выбраны, смонтированы и соединены согласно соответствующим стандартам с тем, чтобы они выдерживали ожидаемые воздействия. Должны применяться основные требования безопасности	Возникновение неисправности может привести к потере функции безопасности	В основном характеризуются выбором компонентов	От малого до среднего	—	Не значимо
1 (см. 6.2.4)	Должны применяться требования категории B. Необходимо использовать успешно испытанные компоненты и хорошо проверенные принципы безопасности	Возникновение неисправности может привести к потере функции безопасности, но вероятность неисправности ниже, чем для категории B	В основном характеризуются выбором компонентов	Большое	—	Не значимо
2 (см. 6.2.5)	Должны применяться требования категории B и хорошо проверенные принципы безопасности. Функция безопасности должна проверяться через соответствующие интервалы системой управления машины	Возникновение неисправности может привести к потере функции безопасности между проверками. Потеря функции безопасности обнаруживается в ходе проверки	В основном характеризуются структурой	От малого до большого	От малого до среднего	См. приложение F
3 (см. 6.2.6)	Должны применяться требования категории B и хорошо проверенные принципы безопасности. SRP/CS должны разрабатываться так, чтобы: - одиночная неисправность в любом из этих элементов не приводила к потере функции безопасности; - там, где практически возможно, одиночная неисправность должна обнаруживаться	При одиночной неисправности функция безопасности всегда выполняется. Некоторые, но не все неисправности будут обнаружены. Накопление невыявленных неисправностей может приводить к потере функции безопасности	В основном характеризуются структурой	От малого до большого	От малого до среднего	См. приложение F
4 (см. 6.2.7)	Должны применяться требования категории B и хорошо проверенные принципы безопасности. SRP/CS должны разрабатываться так, чтобы: - одиночная неисправность в любом из этих элементов не приводила к потере функции безопасности; - одиночная неисправность обнаруживалась во время или до следующего запроса функцией безопасности, однако если это сделать невозможно, то тогда накопление неисправностей не должно приводить к потере функции безопасности	При возникновении одиночной неисправности функция безопасности выполняется всегда. Обнаружение накопленных неисправностей сокращает вероятность потери функции безопасности (большое значение DC). Неисправности будут обнаруживаться своевременно, чтобы предотвращать потерю функции безопасности	В основном характеризуются структурой	Большое	Большое, включая накопление неисправностей	См. приложение F
Примечание — Для ознакомления со всеми требованиями см. раздел 6.						

6.3 Комбинирование элементов системы управления, связанных с безопасностью (SRP/CS), с целью достижения уровня эффективности защиты (PL)

Функция безопасности может быть реализована комбинированием нескольких SRP/CS: входная система, блок обработки сигналов, выходная система. Этим элементам может быть присвоена одна и/или разные категории. Согласно 6.2 категории следует выбирать для всех SRP/CS. Для всех комбинирований этих элементов общий PL может быть установлен по таблице 11. В этом случае требуется оценка достоверности комбинирования (см. рисунок 3).

Согласно 6.2 комбинированные SRP/CS начинают работу на позиции, где включаются сигналы безопасности, и завершают на выходе элементов регулирования мощности. Однако комбинированные SRP/CS могут состоять из элементов, соединенных последовательно или параллельно. Приведена оценка последовательного соединения SRP/CS для того, чтобы не проводить новую комплексную оценку PL, достигнутого совмещенными SRP/CS, когда отдельные значения PL всех элементов уже рассчитаны.

Примем N отдельных SRP/CS_i при их последовательном соединении и совместно выполняющих функцию безопасности. Для каждого элемента уже проведена оценка PL_i. Этот пример показан на рисунке 13 (см. также рисунок 4 и рисунок Н.2).

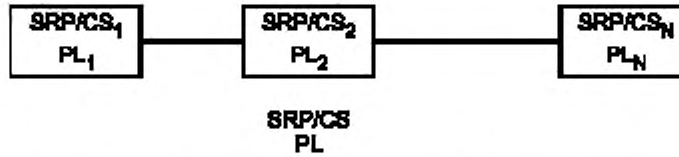


Рисунок 13 — Комбинирование SRP/CS с целью достижения общего PL

Приведенный метод позволяет рассчитать PL всего совмещенного элемента, выполняющего функцию безопасности:

a) определить самый малый PL_i как PL_{low};

b) определить номер $N_{low} \leq N$ для SRP/CS_i, имеющего $PL_i = PL_{low}$;

c) найти PL в таблице 11.

Таблица 11 — Расчет PL последовательного соединения SRP/CS

PL_{low}	N_{low}	⇒	PL
a	>3	⇒	Не допускается
	≤3	⇒	*a*
b	>2	⇒	*a*
	≤2	⇒	*b*
c	>2	⇒	*b*
	≤2	⇒	*c*
d	>3	⇒	*c*
	≤3	⇒	*d*
e	>3	⇒	*d*
	≤3	⇒	*e*

Примечание — Значения, рассчитанные для данной справочной таблицы, основаны на средних показателях надежности для каждого PL.

7 Рассмотрение и исключение неисправностей

7.1 Общие положения

В соответствии с выбранной категорией SRP/CS должны быть разработаны так, чтобы они могли обеспечить PL_r. Должна быть проведена оценка их способности противостоять неисправностям.

7.2 Рассмотрение неисправностей

В настоящем стандарте перечислены некоторые значительные неисправности и отказы для разных технологий. Перечень неисправностей не является исключительным, и при необходимости дополнительные неисправности должны быть рассмотрены и внесены в перечень. В таких случаях должен быть также четко изложен метод оценки. Для новых компонентов, которые не упоминаются в стандарте ISO 13849-2, должен быть проведен анализ видов и последствий отказов (FMEA, см. [32]) с целью определения неисправностей, которые будут рассмотрены для данных компонентов.

В общем случае следует учитывать следующие критерии неисправности:

- если как следствие неисправности из строя выходят другие элементы, то первая неисправность и последующие неисправности должны рассматриваться как одиночная неисправность;
- две или более независимые неисправности, имеющие общую причину возникновения, рассматриваются как одиночная неисправность;
- одновременное возникновение двух и более неисправностей, имеющих независимые причины, считается в высшей степени маловероятным и поэтому не рассматривается.

7.3 Исключение неисправностей

Нецелесообразно оценивать SRP/CS без допущения, что определенные неисправности могут быть исключены. Для получения более подробной информации об исключении неисправностей см. ISO 13849-2.

Такие неисправности могут быть исключены на основе компромисса между техническими требованиями обеспечения безопасности и теоретической вероятностью их возникновения.

Исключение неисправности может быть основано на:

- отсутствии вероятности возникновения определенных неисправностей;
- общепризнанном техническом опыте, который может быть использован независимо от конкретно рассматриваемого применения;
- технических требованиях, установленных для данного применения и рассмотренного конкретного риска.

Если неисправности исключены, то должно быть приведено обоснование в технической документации.

8 Оценка достоверности

Структурная комбинация SRP/CS должна быть оценена на достоверность (см. рисунок 3). Эта оценка должна показывать, что структурная комбинация элементов, связанных с обеспечением безопасности и выполняющих каждую функцию безопасности, отвечает всем требованиям настоящего стандарта.

Для получения более подробной информации об оценке достоверности см. ISO 13849-2.

9 Техническое обслуживание

Планово-предупредительное или внеплановое техническое обслуживание обычно необходимо для поддержания заданных рабочих характеристик SRP/CS. Отклонения от заданных рабочих характеристик со временем могут привести к снижению уровня обеспечения безопасности или даже к опасной ситуации. Информация по использованию SRP/CS должна включать инструкции по техническому обслуживанию (включая периодические проверки) этих элементов.

Положения о ремонтопригодности SRP/CS должны соответствовать принципам, изложенным в 6.2.7 ISO 12100. Вся информация по техническому обслуживанию должна быть в соответствии с перечислением e) 6.4.5.1, ISO 12100.

10 Техническая документация

При разработке SRP/CS конструктор должен включить в документацию нижеприведенную информацию, относящуюся к конкретному элементу:

- функция(и) безопасности, выполняемая(ые) элементом;
- характеристики каждой функции безопасности;
- точное расположение точек, в которых начинает(ют) и завершает(ют) свою работу элемент(ы) обеспечения безопасности;
- условия окружающей среды;
- уровень эффективности защиты (PL);
- выбранная категория или категории;
- параметры, связанные с надежностью ($MTTF_d$, DC, CCF и T_M);
- меры по устранению систематических ошибок;
- применяемая технология или технологии;
- все учтенные неисправности, связанные с безопасностью;
- обоснование исключения неисправностей (см. ИСО 13849-2);
- обоснование структурной комбинации (например, учтенные неисправности, исключенные неисправности);
- документация по программному обеспечению;
- меры, направленные на предотвращение предсказуемой неправильной эксплуатации.

Примечание — Данная документация считается предназначенной для внутреннего использования производителем, а не для распространения среди пользователей.

11 Информация для пользователя

Следует применять принципы, изложенные в 6.4.5.2 ISO 12100, а также в соответствующих разделах других, относящихся к этому вопросу документов (например, в разделе 17 [29]). В частности, информация, важная для надежного использования SRP/CS, должна предоставляться пользователю. Информация включает в себя, но не ограничивается только этим, следующее:

- пределы зоны действия элементов обеспечения безопасности по выбранной(ым) категории(ям) и любые исключения неисправностей;
- если пределы зоны SRP/CS и любые исключения неисправностей (см. 7.3) являются существенными для сохранения выбранной категории или категорий и характеристик безопасности, то соответствующая информация (например, для модификации, технического обслуживания и ремонта) должна быть предоставлена для гарантии последующего обоснования исключения неисправности(ей);
- влияние отклонений от заданных рабочих характеристик на функцию(и) безопасности;
- четкое описание мест сопряжения с SRP/CS и предохранительными устройствами;
- время срабатывания;
- ограничения при эксплуатации (включая условия окружающей среды);
- обозначения и сигналы опасности;
- приостановка и прекращение функций безопасности;
- режимы управления;
- техническое обслуживание (см. раздел 9);
- контрольный перечень технического обслуживания;
- удобство доступа и замены внутренних компонентов;
- средства для легкого и безопасного поиска неисправностей;
- информация, поясняющая использование, связанное с категорией, на которую дана ссылка;
- периодичность контрольных испытаний, где это необходимо.

Должна быть предоставлена информация о категории или категориях и уровне эффективности защиты SRP/CS, как показано ниже:

- ссылка на настоящий стандарт;
- категория B, 1, 2, 3 или 4;
- уровень эффективности защиты, *a, b, c, d* или *e*.

Пример — В соответствии с ГОСТ ISO 13849-1 SRP/CS с категорией B и уровнем эффективности защиты a будет обозначен следующим образом:

ГОСТ ISO 13849-1 категория B PL a.

Приложение А
(справочное)

Определение требуемого уровня эффективности защиты (PL_r)

А.1 Выбор PL_r

В настоящем приложении описан упрощенный метод, который касается вклада в снижение риска, вносимого SRP/CS. Этот метод обеспечивает только оценку снижения риска и предназначен для того, чтобы конструктор и разработчик стандартов могли выбирать PL_r для каждого SRP/CS.

Оценка снижения риска предполагает ситуацию до предоставления предполагаемой функции безопасности.

Снижение рисков с помощью других технических мер независимой системы управления (например, механизированные ограждения) или дополнительные функции безопасности, которые могут быть учтены при определении PL_r — в этом случае начальная точка (рисунок А.1) может быть выбрана после осуществления этих мер (см. также рисунок 2).Тяжесть травмирования (S) относительно легко поддается оценке, например: рваная рана, ампутация, летальный исход. При определении частоты появления опасного события используют вспомогательные параметры, чтобы повысить уровень оценки. К таким параметрам относят:

- частоту и время подверженности данному риску (F);
- возможность избежать опасности или ограничение вреда (P).

Опыт показал, что эти параметры можно совместить, как показано на рисунке А.1, чтобы продемонстрировать градацию от низкой до высокой степени риска. Этим подчеркивается, что только качественный процесс дает оценку риска.

А.2 Руководство для подбора параметров S, F и P для оценки рисков

А.2.1 Тяжесть травмирования видов S1 и S2

При оценке риска, связанного с неисправностями в элементах системы управления, имеющих отношение к безопасности, рассматривают легкие (обычно обратимые) и серьезные травмы (как правило, необратимые, включая летальный исход).

Чтобы сделать выбор, необходимо принимать во внимание обычные обстоятельства несчастных случаев и нормальные процессы лечения: например, ушибы и/или рваные раны следует классифицировать как S1, в то время как ампутацию или летальный исход — как S2.

А.2.2 Частота и/или время подверженности риску видов F1 и F2

Как правило, действительный период времени, в течение которого должны выбираться параметры F1 и F2, не может быть задан. Однако следующее объяснение может помочь в правильном решении при сомнительных случаях.

Параметр F2 следует выбирать в том случае, если человек (лицо, оператор) кратковременно или длительно подвергается опасности. Не имеет значения, подвергается ли последовательно опасностям один и тот же или разные люди (операторы), например, при пользовании лифтами.

Когда проектировщику известно требование к функции безопасности, параметры частоты и продолжительности этого требования могут быть выбраны вместо параметров частоты и продолжительности доступа к объекту риска. В настоящем стандарте параметр частоты в требованиях к функции безопасности принимается чаще, чем раз в год.

Продолжительность подверженности опасности следует оценивать на основе среднего значения, которое можно представить как отношение к общему периоду времени, в течение которого используют данное оборудование. Например, если в течение рабочего цикла необходимо регулярно просовывать руку между механизмами машины для того, чтобы загружать и снимать детали, то тогда следует выбирать параметр F2. Если доступ к детали требуется время от времени, то тогда можно выбирать параметр F1.

Примечание — В случае отсутствия обоснования используется F2, если частота чаще, чем раз в час.

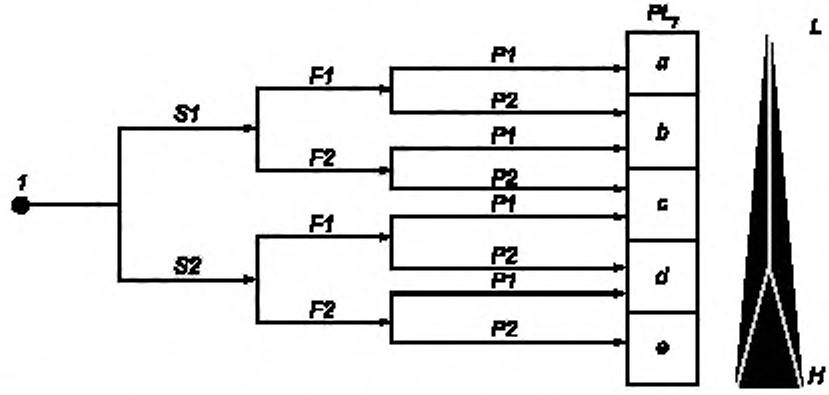
А.2.3 Вероятность избежать опасности вида P1 и P2

При возникновении опасности важно знать, можно ли ее распознать или ее можно избежать прежде, чем она приведет к несчастному случаю. Например, важно рассмотреть, можно ли идентифицировать определенную опасность по ее физическим характеристикам или ее можно распознать только техническими средствами, например, по индикаторам. Другими важными аспектами, влияющими на выбор параметра P, являются, например:

- работа под наблюдением или без него;
- выполнение работы опытным специалистом или непрофессионалом (дилетантом);
- скорость возникновения опасности (например, быстро или медленно);
- возможность избежать опасности (например, выброса);
- практический опыт в области безопасности процесса.

При возникновении опасной ситуации параметр P1 следует выбирать только тогда, когда есть реальный шанс уклониться от несчастного случая или значительно уменьшить его эффект. Параметр P2 выбирают, когда почти нет возможности избежать опасности.

На рисунке А.1 показана шкала для определения PL_r, связанного с обеспечением безопасности, который зависит от оценки риска. Схема должна рассматриваться для каждой функции безопасности. Метод оценки риска основан на ISO 14121 и должен использоваться в соответствии с ISO 12100.



1 — начальная точка оценки риска для элемента системы управления, связанного с обеспечением безопасности; *L* — низкий вклад в снижение рисков; *H* — высокий вклад в снижение рисков; PL_r — требуемый уровень эффективности защиты

Параметры риска:

S — тяжесть травмирования; *S1* — незначительные травмы (обычно обратимые); *S2* — тяжелые травмы (обычно необратимые); *F* — частота и/или время подверженности риску; *F1* — от редкой до очень частой и/или короткое время; *F2* — от частой до непрерывной и/или длительное время; *P* — вероятность избежать опасности или ограничение вреда; *P1* — возможно при определенных условиях; *P2* — вряд ли возможно

Рисунок А.1 — График рисков для определения необходимых PL_r для функции безопасности

Приложение В
(справочное)

Блочный метод и схема блоков, связанных с обеспечением безопасности

В.1 Блочный метод

Упрощенный подход требует блочно-ориентированное логическое представление SRP/CS. SRP/CS должен быть разделен на несколько блоков в соответствии со следующими правилами:

- блоки должны отражать логические части SRP/CS, относящиеся к выполнению функции безопасности;
- разные каналы выполнения функции безопасности должны быть вынесены в разные блоки; если один блок не может больше выполнять функцию безопасности, то это не должно влиять на выполнение функции безопасности через блоки других каналов;
- каждый канал может состоять из одного или нескольких блоков — три блока на канал в спроектированной архитектуре входящий, логический и исходящий не является обязательным набором, это просто пример логического разделения внутри канала;
- каждое аппаратное устройство, являющееся SRP/CS, должно принадлежать только одному блоку, таким образом обеспечивается расчет показателя $MTTF_d$ всего блока на основе показателей $MTTF_d$ отдельных аппаратных устройств, образующих блок (например, с учетом характера отказа, анализом последствий отказов или методом расчета элементов, см. приложение D.1);
- аппаратные устройства используются только для диагностики (например, тестирование оборудования) и не влияют на выполнение функции безопасности в разных каналах при опасном сбое аппаратных устройств и могут быть отделены от них при выполнении функции безопасности.

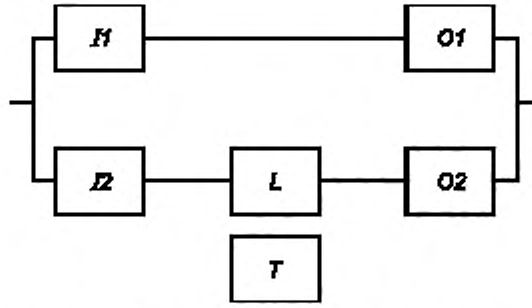
Примечание — Для целей настоящего стандарта «блоки» не соответствуют функциональным блокам или надежным блокам.

В.2 Схема блоков, связанных с обеспечением безопасности

Блоки, определенные блочным методом, можно использовать для графического представления логической структуры SRP/CS в схеме блоков, связанных с обеспечением безопасности. Для такого графического представления необходимо следующее руководство:

- сбой одного блока в последовательно сгруппированных блоках приводит к сбою всего канала (например, если одно аппаратное устройство в канале SRP/CS неисправно, весь канал не сможет больше выполнять функцию безопасности);
- только сбой всех каналов в параллельно сгруппированных блоках приводит к сбою функции безопасности (например, функция безопасности, выполняемая несколькими каналами, выполняется до тех пор, пока все каналы не станут неисправными);
- блоки, используемые только для тестирования, и те, которые не влияют на выполнение функции безопасности в разных каналах при сбоях, могут быть отделены от блоков в разных каналах.

Для примера см. рисунок В.1.



I1 и O1 формируют первый канал (последовательная группировка);
I2, L, O2 формируют второй канал, т. е. функция безопасности имеет два канала (параллельная группировка). T используется только для тестирования.

I1, I2 — устройства ввода, например, датчик, *L* — логика; *O1, O2* — выходное устройство, например, главный контактор; *T* — тестирующее устройство

Рисунок В.1 — Пример блок-схемы, связанной с безопасностью

Приложение С
(справочное)

Расчет и оценка среднего времени наработки на опасный отказ ($MTTF_d$) для отдельных компонентов

С.1 Общие положения

В приложении описывается несколько методов для расчета и оценки значений $MTTF_d$ отдельных компонентов: метод, описанный в С.2, базируется на подтвержденном практическом использовании для различных типов компонентов; метод, данный в С.3, применим для гидравлических компонентов; С.4 описывает методы расчета $MTTF_d$ для пневматических, механических и электромеханических компонентов с B_{10} (см. С.4.1); С.5 содержит перечень значений $MTTF_d$ для электронных компонентов.

С.2 Метод практического использования

Значения $MTTF_d$ или B_{10d} можно рассчитать в соответствии с таблицей С.1, если учитывать следующие критерии:

a) компоненты изготовляются в соответствии с хорошо проверенными принципами безопасности по ISO 13849-2 или по соответствующему стандарту (см. таблицу С.1) для проектирования компонентов (подтверждение данных по компонентам);

Примечание — Информация может быть найдена в перечне данных по производимым компонентам.

b) производитель компонентов определяет подходящее приложение и условия использования для пользователя;

c) проектирование SRP/CS удовлетворяет хорошо проверенным принципам безопасности по ISO 13849-2 для реализации и эксплуатации компонентов.

С.3 Гидравлические компоненты

Значение $MTTF_d$ для одного из гидравлических компонентов, например гидрораспределитель (клапан), может насчитывать до 150 лет, если выполняются следующие критерии:

a) гидравлические компоненты изготовляются в соответствии с хорошо проверенными принципами безопасности по ISO 13849-2, таблицы С.1 и С.2 для проектирования гидравлических компонентов (подтверждение данных по компонентам);

Примечание — Информация может быть найдена в перечне данных по производимым компонентам.

b) производитель гидравлических компонентов оговаривает применяемость и условия эксплуатации для пользователя. Производитель SRP/CS должен предоставить информацию, касающуюся соответствия компонентов базовым и хорошо проверенным принципам безопасности по ISO 13849-2, таблицы С.1 и С.2 для внедрения и эксплуатации гидравлических компонентов.

Однако если условия перечислений a) или b) не выполняются, то производитель предоставляет значения $MTTF_d$ для одного из гидравлических компонентов для проектирования.

Таблица С.1 — Международные нормы, касающиеся $MTTF_d$ или $B10_d$ для компонентов

Компоненты	Основные принципы безопасности по ISO 13849-2	Соответствующие стандарты	Стандартные значения: $MTTF_d$ (годы) B_{10d} (циклы)
Механические компоненты	Таблицы А.1 и А.2	—	$MTTF_d$ = 150
Гидравлические компоненты	Таблицы С.1 и С.2	[24], [42]	$MTTF_d$ = 150
Пневматические компоненты	Таблицы В.1 и В.2	[25], [43]	B_{10d} = 20 000 000
Реле и контакторы, реле с небольшой нагрузкой (механической нагрузкой)	Таблицы D.1 и D.2	[33], [36], [46]	B_{10d} = 20 000 000
Реле и контакторы, реле с максимальной нагрузкой	Таблицы D.1 и D.2	[33], [36], [46]	B_{10d} = 400 000
Бесконтактные выключатели с небольшой нагрузкой (механической нагрузкой)	Таблицы D.1 и D.2	[33], [45]	B_{10d} = 20 000 000
Бесконтактные выключатели с максимальной нагрузкой	Таблицы D.1 и D.2	[33], [45]	B_{10d} = 400 000
Контакторы с небольшой нагрузкой (механической нагрузкой)	Таблицы D.1 и D.2	[33]	B_{10d} = 20 000 000
Контакторы с нормальной нагрузкой	Таблицы D.1 и D.2	[33]	B_{10d} = 2 000 000
Путевой выключатель без нагрузки[a)]	Таблицы D.1 и D.2	[33], [45]	B_{10d} = 20 000 000
Путевой выключатель (с отдельным приводом, локировочный переключатель ограждения) без нагрузки[a)]	Таблицы D.1 и D.2	[33], [45]	B_{10d} = 2 000 000
Стоп-кран без нагрузки[a)]	Таблицы D.1 и D.2	[13], [33]	B_{10d} = 100 000
Стоп-кран с максимальными функциональными требованиями[a)]	Таблицы D.1 и D.2	[13], [33]	B_{10d} = 6050
Нажимная кнопка (например, выключатель блокировки) без нагрузки[a)]	Таблицы D.1 и D.2	[33]	B_{10d} = 100 000
Для определения и использования B_{10d} см. С.4. Примечание 1 — B_{10d} оценивается как удвоенное B_{10} (50 % опасной ошибки). Примечание 2 — Под «небольшой нагрузкой» подразумевается, например, 20 % от установленного значения (подробнее см. ISO 13849-2).			
[a)] Возможно, если исключено нарушение в процессе прямого управляющего воздействия.			

С.4 $MTTF_d$ для пневматических, механических и электромеханических компонентов

С.4.1 Общие положения

Для пневматических, механических и электромеханических компонентов (пневматические клапаны, реле, контакторы, выключатели, кулачков выключатели и др.) может быть сложно вычислить $MTTF_d$ компонентов, которое исчисляется в годах. В большинстве случаев производители указанных компонентов указывают усредненное количество циклов наработки до наступления опасного отказа, для числа компонентов до 10 % (B_{10d}). В этом приложении приводится метод для расчета $MTTF_d$ для компонентов с использованием B_{10} или T (время жизненного цикла), приводимых производителем для учета в зависимости от нарабатываемых циклов.

Оценка $MTTF_d$ одиночных пневматических, механических и электромеханических компонентов должна производиться с учетом С.4.2, если выполняются следующие критерии:

a) все компоненты производятся в соответствии с базовыми принципами безопасности по ISO 13849-2, таблицы В.1 или D.1 (соответствующее указание должно быть на табличке компонента).

Примечание — Информация должна быть приведена на табличке изделия его производителем.

b) все компоненты производятся в соответствии с категориями 1, 2, 3 или 4, установленными в ISO 13849-2, таблицы В.2 или D.2 для проектирования компонента (соответствующее указание должно быть на табличке компонента).

Примечание — Информация должна быть приведена на табличке изделия его производителем.

c) производитель компонентов определяет применение и условия их эксплуатации пользователем. Производитель SRP/CS должен предоставлять информацию, относящуюся к осуществлению хорошо проверенных принципов безопасности по ISO 13849-2, таблицы B.1 или D.1 для использования и поставок этих компонентов. Потребитель должен иметь информацию относительно категорий 1, 2, 3 и 4 согласно ISO 13849-2, таблицы B.2 и D.2 для использования компонентов в работе.

C.4.2 Расчет $MTTF_d$ для компонентов B_{10d}

Среднее количество циклов наработки до наступления опасного отказа для числа компонентов до 10 % (B_{10d})[1] должно быть определено производителем компонента в соответствии с положениями стандартов на продукцию и на методы испытаний (например, [28], [36]). Виды опасных нарушений компонентов должны быть разграничены, например, заклинивание в конечном положении или изменение времени отключения. Если не все компоненты в ходе испытаний получили опасные повреждения (неисправности, например, у пяти компонентов из семи испытуемых), то окончательный анализ для неповрежденных компонентов должен быть выполнен.

Расчет $MTTF_d$ с использованием среднегодовых чисел B_{10d} и $n_{ср}$ для компонентов производится по формулам C.1 и C.2:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \times n_{ср}} \tag{C.1}$$

где

$$n_{ср} = \frac{d_{ср} \times h_{ср} \times 3600\ сек\ /\ час}{t_{цикла}}\ (\text{число циклов в году}) \tag{C.2}$$

для компонентов с учетом допущений принимается:

$h_{ср}$ — средняя наработка (час/день);

$d_{ср}$ — средняя наработка (день/год);

$t_{цикла}$ — среднее время между началами двух последующих циклов для компонента (например, переключение клапана) (секунда/цикл).

Время наработки компонента ограничивается T_{10d} как среднее время до наступления опасного отказа для числа компонентов до 10 % и рассчитывается по формуле C.3:

$$T_{10d} = \frac{B_{10d}}{n_{ср}} \tag{C.3}$$

Примечание — Трактовка этой формулы в C.4.3.

B_{10d}, количество циклов наработки до наступления опасного отказа для числа компонентов до 10 %, должно быть преобразовано в T_{10d}, среднее время до наступления опасного отказа для числа компонентов до 10 % (формула C.4):

$$T_{10d} = \frac{B_{10d}}{n_{ср}} \tag{C.4}$$

Достоверность методов настоящего стандарта обоснована тем, что нарушения в компонентах распределяются экспоненциально во времени: $F(t) = 1 - \exp(-\lambda dt)$. Для пневматических и электромеханических компонентов наиболее подходит распределение Вейбулла. Однако если рабочее время компонентов ограничено средним временем T_{10d} до наступления опасного отказа для числа компонентов до 10 %, тогда значение постоянной опасного отказа (λ_d) больше этого периода рабочего времени и должно определяться по формуле C.5:

$$\lambda_d \approx \frac{0{,}1}{T_{10d}} = \frac{0{,}1 \times n_{ср}}{B_{10d}} \tag{C.5}$$

Уравнение C.5 показывает окончательно, что при значении постоянной опасного отказа до 10 % опасно поврежденных компонентов дают сбой через T_{10d} (лет), что соответствует B_{10d} (циклов). Окончательно по формуле C.6:

$$F(T_{10d}) = 1 - \exp(-\lambda_d T_{10d}) = 10\%\ \text{ при }\ \lambda_d = \frac{\ln(0{,}9)}{T_{10d}} = \frac{0{,}10536}{T_{10d}} \approx \frac{0{,}1}{T_{10d}} \tag{C.6}$$

С $MTTF_d = \frac{1}{\lambda_d}$ для экспоненциальной зависимости это представляется, как в формуле C.7:

$$MTTF_d = \frac{T_{10d}}{0{,}1} = \frac{B_{10d}}{0{,}1 \times n_{ср}} \tag{C.7}$$

[1] Если опасное воздействие не выделено и B_{10} неизвестно, то используют 50 % от B_{10}, принимая $B_{10d} = 2B_{10}$.

С.4.3 Пример

Для пневматического клапана производитель определил среднее значение B_{10d} в 60 млн циклов. Клапан применяется при двухсменной работе 220 рабочих дней в году. Среднее время между запуском в работу в двух циклах составляет 5 секунд. В результате получают следующие значения:

d_{op} — 220 дней в год;

h_{op} — 16 часов работы в день;

$t_{цикла}$ — 5 с, время цикла;

B_{10d} — 60 млн циклов наработки до опасного отказа для клапана.

Расчет с этими данными производится по формулам С.8, С.9, С.10:

$$n_{op} = \frac{220\,дней/год \times 16\,час/день \times 3600\,с/час}{5\,с/цикл} = 2{,}53 \times 10^6\,цикл/год \qquad (С.8)$$

$$T_{10d} = \frac{60 \times 10^6\,цикл}{2{,}53 \times 10^6\,цикл/год} = 23{,}7\,лет \qquad (С.9)$$

$$MTTF_d = \frac{23{,}7\,лет}{0{,}1} = 23{,}7\,лет \qquad (С.10)$$

В соответствии с таблицей 5 для $MTTF_d$ компонента дается оценка уровня — «высокий». Эти предположения имеют значение только в ограниченное время 23,7 года работы клапана.

С.5 Значения $MTTF_d$ для электрических компонентов

С.5.1 Общие положения

В таблицах С.2 — С.7 приведены некоторые типичные усредненные значения $MTTF_d$ для электрических компонентов. Эти значения взяты из [47] для серийных изделий. Различные доступные сведения относительно $MTTF_d$ для различных компонентов сведены в базы. Если конструктор SRP/CS имеет иные данные от производителя, он может использовать эти значения, вводя их в вышеприведенные примеры.

Значения, приведенные в таблицах С.2 — С.7, применимы для температуры 40 °С при номинальных токовой нагрузке и напряжении.

В таблицах значения $MTTF_d$ взяты из [47] для групп компонентов со всевозможными видами нарушений, а не только опасными. Это зависит в большей степени от применимости. Уточненный метод определения «типа» $MTTF_d$ для компонентов представляется как FMEA. Некоторые компоненты, например, транзисторы, используемые в ключевом режиме, могут давать короткие замыкания или размыкания как отказы. Только одно из этих двух состояний может быть опасным, поэтому текст колонки «Примечание» указывает на необходимость 50 % оценки опасных нарушений, т. к. в таблице приведено удвоенное $MTTF_d$ значение для компонентов по сравнению с приведенным $MTTF_d$. Там, где необходимо устранить неопределенность, наиболее тяжелый режим $MTTF_d$ для компонентов указан в колонке «$MTTF_d$ для тяжелого режима», где граница безопасности оценена в 10.

С.5.2 Полупроводники

См. таблицы С.2 и С.3.

Таблица С.2 — Транзисторы (в режиме переключений)

Транзистор	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Биполярный	TO18, TO92, SOT23	34 247	68 493	6 849	50 % опасных отказов
Биполярный, маломощный	TO5, TO39	5 708	11 416	1 142	50 % опасных отказов
Биполярный, мощный	TO3, TO220, D-Pack	1 941	3 881	388	50 % опасных отказов
ФЕТ	Junction MOS	22 831	45 662	4 566	50 % опасных отказов
МОС, силовой	TO3, TO220, D-Pack	1 142	2 283	228	50 % опасных отказов

Таблица С.3 — Диоды, силовые полупроводники и интегральные цепочки

Диод	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Общего назначения	—	114 155	228 311	22 831	50 % опасных отказов
Подавитель помех	—	15 981	31 963	3 196	50 % опасных отказов
Диод Зенера P_{tot} < 1W	—	114 155	228 311	22 831	50 % опасных отказов
Выпрямительные диоды	—	57 078	114 155	11 416	50 % опасных отказов
Диодные мосты	—	11 415	22 831	2 283	50 % опасных отказов
Тиристоры	—	2 283	4 566	457	50 % опасных отказов
Триаки, диаки	—	1 484	2 968	297	50 % опасных отказов
Интегральные цепочки (программируемые и непрограммируемые)	Используйте данные производителей				50 % опасных отказов

С.6 Пассивные компоненты

См. таблицы С.4 — С.7.

Таблица С.4 — Конденсаторы

Конденсатор	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Стандартные, не силовые	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57 078	114 155	11 416	50 % опасных отказов
Керамический	—	22 831	45 662	4 566	50 % опасных отказов
Алюминиевый электролитический	Жидкий электролит	22 831	45 662	4 566	50 % опасных отказов
Алюминиевый электролитический	Твердый электролит	37 671	75 342	7 534	50 % опасных отказов
Танталовый электролитический	Жидкий электролит	11 415	22 831	2 283	50 % опасных отказов
Танталовый электролитический	Твердый электролит	114 155	228 311	22 831	50 % опасных отказов

Таблица С.5 — Резисторы

Резистор	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Карбон пленка	—	114 155	228 311	22 831	50 % опасных отказов
Металлопленка	—	570 776	1 141 552	114 155	50 % опасных отказов
Металлооксидные и проволочные	—	22 831	45 662	4 566	50 % опасных отказов
	—	3 767	7 534	753	50 % опасных отказов

Таблица С.6 — Индуктивности

Индуктивности	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Для МС-применения	—	37 671	75 342	7 534	50 % опасных отказов
Низкочастотные индуктивности и трансформаторы	—	22 831	45 662	4 566	50 % опасных отказов
Питающие трансформаторы и трансформаторы для отключения и силового питания	—	11 415	22 831	2 283	50 % опасных отказов

Таблица С.7 — Оптосвязи

Оптосвязи	Обозначение	MTTF для компонентов, лет	$MTTF_d$ для компонентов, лет		Примечания
			обычный	тяжелый	
Биполярный выход	SFH 610	7 648	15 296	1 530	50 % опасных отказов
ФЕТ-выход	LH 1056	2 854	5 708	571	50 % опасных отказов

Приложение D
(справочное)

Упрощенный метод оценки среднего времени наработки на опасный отказ ($MTTF_d$) для каждого канала

D.1 Метод расчета элементов

«Метод расчета элементов» служит для оценки $MTTF_d$ отдельно для каждого канала. В этом расчете используются значения $MTTF_d$ каждого отдельного компонента, являющегося частью этого канала[1].

Общая формула (D.1):

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} = \sum_{j=1}^{N} \frac{n_j}{MTTF_{dj}} \qquad (D.1)$$

где $MTTF_d$ — для всего канала;

$MTTF_{di}$, $MTTF_{dj}$ — $MTTF_d$ каждого компонента, который вносит свой вклад в обеспечение функции безопасности.

Первая сумма представляет собой отдельное суммирование каждого компонента; вторая сумма равна первой и является упрощенной формой, в которой сгруппированы все n_j одинаковые компоненты с одинаковым значением $MTTF_{dj}$. Пример, приведенный в таблице D.1, дает значение $MTTF_d$ всего канала, равное 21,4 года, что является «средним» значением согласно таблице 5.

Таблица D.1 — Пример перечня элементов монтажной платы

j	Компонент	Количество единиц, n_j	$MTTF_{dj}$ Наихудший вариант, лет	1/ $MTTF_{dj}$ Наихудший вариант, 1/лет	n_j / $MTTF_{dj}$ Наихудший вариант, 1/лет
1	Транзисторы, биполярный, маломощный (см. таблицу B.2)	2	1 142	0,000 876	0,001 752
2	Резистор, пленочный, угольный (см. таблицу B.5)	5	22 831	0,000 044	0,000 219
3	Конденсатор, эталонный, несиловой (см. таблицу B.4)	4	11 416	0,000 088	0,000 350
4	Реле (с низкой нагрузкой, см. B.2) (B_{10d} = 20 000 000 циклов, n_{op} = 633 600)	4	315,66	0,003 168	0,012 672
5	Контактор (с номинальной нагрузкой, см. B.2) (B_{10d} = 2 000 000 циклов, n_{op} = 633 600)	1	31,57	0,031 676	0,031 676
$\Sigma(n_j/MTTF_{d\,j})$					0,046 669
$MTTF_d = 1/\Sigma(n_j/MTTF_{d\,j})$ [лет]					21,43

Примечание 1 — Этот метод основан на предположении, что отказ любого компонента внутри канала ведет к отказу всего канала. Расчет $MTTF_d$, приведенный в таблице D.1, основан на этом же.

Примечание 2 — В этом примере основное воздействие идет от замыкателя (контактора). Выбранные значения для $MTTF_d$ и B_{10d} для этого примера основаны на Приложении B. Например, если предположить, что d_{op} = 220 *дней/год*, h_{op} = 8 *ч/день*, $t_{цикл}$ = 10 *с/цикл* получим n_{op} = 633600 *цикл/год*. В общем случае применение значений для $MTTF_d$ и B_{10d}, заданных разработчиками, приведет к гораздо лучшему результату, а именно — более высокому значению $MTTF_d$ для канала.

D.2 $MTTF_d$ для разных каналов, симметризация $MTTF_d$ для каждого канала

Структурные построения 6.2 подразумевают, что для каналов SRP/CS значения $MTTF_d$ для каждого канала одинаковы. Значение для каждого канала должно быть в соответствии с рисунком 5.

Если значения $MTTF_d$ для каналов различаются, то существуют два варианта:

[1] Метод расчета элементов является приближенным и всегда дает значение с определенным запасом. Если требуются более точные значения, тогда конструктор должен учитывать состояния отказа, что может оказаться весьма трудной задачей.

- в худшем случае должно быть рассмотрено пониженное значение;
- уравнение (D.2) можно использовать для примерного вычисления значения, которым можно заменить среднее время до сбоя для каждого канала:

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right] \quad (D.2)$$

где $MTTF_{dC1}$ и $MTTF_{dC2}$ — значения для двух разных резервированных каналов.

Пример — На одном канале $MTTF_{dC1}$ = 3 года, а на другом $MTTF_{dC2}$ = 100 лет, в таком случае $MTTF_d$ = 66 лет для каждого канала. Это значит, что резервная система с $MTTF_d$, равным 100 годам на одном канале и 3 годам — на другом, эквивалентна системе, в которой на каждом канале среднее время до сбоя равно 66 годам.

При помощи вышеприведенной формулы система с двумя резервированными каналами и разным $MTTF_d$ на каждом канале может быть заменена на систему с одинаковым $MTTF_d$ на каждом канале. Данное действие необходимо для правильного использования рисунка 5.

Примечание — Данный метод подразумевает независимые параллельные каналы.

Приложение Е
(справочное)

Оценка меры диагностического охвата (DC) для функций и каналов

Е.1 Примеры диагностического охвата (DC)

См. таблицу Е.1.

Таблица Е.1 — Примеры диагностического охвата (DC)

Метод определения	DC
Входное устройство	
Испытания в режиме циклической нагрузки путем динамического изменения входного сигнала	90 %
Проверка правдоподобности, к примеру, применение нормально разомкнутых и нормально замкнутых механически соединенных контактов	99 %
Перекрестный контроль входов без применения динамических проверок	От 0 до 99%, зависит от того, насколько часто происходит изменение сигнала приложением
Перекрестный контроль входных сигналов с применением динамических проверок при отсутствии обнаружения короткого замыкания (для многих устройств ввода-вывода)	90 %
Перекрестный контроль входных сигналов и определение промежуточных результатов при помощи логической схемы и логически-временной программы наблюдения, а также с обнаружением статических сбоев и коротких замыканий (для многих устройств ввода-вывода)	99 %
Косвенное наблюдение (наблюдение при помощи переключателя давления, изучение электротехнических данных исполнительного устройства)	От 90 до 99 %, зависит от приложения
Прямое наблюдение (изучение электротехнических данных контрольных клапанов (вентилей), изучение электромеханических устройств с помощью механически соединенных контактов)	99 %
Обнаружение сбоев во время процесса	От 0 до 99 %, зависит от приложения; применение только одного этого метода недостаточно для требуемого уровня производительности
Исследование некоторых показателей датчика (время ответа, диапазон аналоговых сигналов, например, электрическое сопротивление, емкостное сопротивление)	60 %
Косвенное наблюдение (наблюдение при помощи переключателя давления, изучение электротехнических данных исполнительного устройства)	От 90 до 99 %, зависит от приложения
Прямое наблюдение (изучение электротехнических данных контрольных клапанов (вентилей), изучение электромеханических устройств с помощью механически соединенных контактов)	99 %
Обычный временной контроль логической схемы (например, таймер в качестве следящего устройства, где триггерные точки показаны в программе логической схемы)	60 %
Временной и логический контроль при помощи следящего устройства, в котором тестовое оборудование проверяет правдоподобие поведения логической схемы	90 %
Автоматические самопроверки на скрытые сбои в разных частях логической схемы (программы и банки данных, порты входа/выхода, интерфейсы)	90 % (зависит от метода проверки)

Продолжение таблицы Е.1

Метод определения	DC
Проверка реакционной способности устройства наблюдения (устройства слежения) при помощи устройства ввода на главном канале (либо при запуске, либо когда требуется применение функции безопасности, либо по требованию внешнего сигнала)	90 %
Динамический принцип (все компоненты логической схемы должны изменить состояние ВКЛ-ВЫКЛ-ВКЛ, когда требуется применение функции безопасности), например, блокирующая схема, приводимая в действие при помощи реле	99 %
Неизменяемая память: подпись одинарным словом (8 бит)	90 %
Неизменяемая память: подпись двойным словом (16 бит)	99 %
Изменяемая память: проверка оперативной памяти с применением резервных данных (флагов, маркеров, постоянных, счетчиков) и перекрестное сравнение этих данных	60 %
Изменяемая память: проверка на возможность чтения и записи в использованных участках памяти	60 %
Изменяемая память: контроль оперативной памяти при помощи модифицированного кода Хэмминга или при помощи самопроверки оперативной памяти (например «galpat» или «Abraham»)	99 %
Программная самопроверка процессора	От 60 до 90 %
Кодированная обработка данных в процессоре	От 90 до 99 %
Обнаружение сбоев во время процесса	От 0 до 99 %, зависит от приложения; применение только одного этого метода недостаточно для требуемого уровня производительности
Выходное устройство	
Контроль выходов одним каналом без динамической проверки	От 0 до 99 %, зависит от того, насколько часто происходит изменение сигнала приложением
Перекрестный контроль выходов без применения динамических проверок	От 0 до 99 %, зависит от того, насколько часто происходит изменение сигнала приложением
Перекрестный контроль выходных сигналов с применением динамических проверок при отсутствии обнаружения короткого замыкания (для многих устройств ввода-вывода)	90 %
Перекрестный контроль выходных сигналов и определение промежуточных результатов при помощи логической схемы и логически-временной программы наблюдения, а также с обнаружением статических сбоев и коротких замыканий (для многих устройств ввода-вывода)	99 %
Резервированное отключение без наблюдения за исполнительным устройством	0 %
Резервированное отключение с наблюдением за одним из исполнительных устройств при помощи логической схемы или тестового оборудования	90 %
Резервированное отключение с наблюдением за исполнительными устройствами при помощи логической схемы или тестового оборудования	99 %
Косвенное наблюдение (наблюдение при помощи переключателя давления, изучение электротехнических данных исполнительного устройства)	От 90 до 99 %, зависит от приложения

Окончание таблицы Е.1

Метод определения	DC
Обнаружение сбоев во время процесса	От 0 до 99 %, зависит от приложения; применение только одного этого метода недостаточно для требуемого уровня производительности
Прямое наблюдение (изучение электротехнических данных контрольных клапанов (вентилей), изучение электромеханических устройств с помощью механически соединенных контактов)	99 %
Примечание 1 — Для дополнительных методов определения см. IEC 61508-2, таблицы А.2 — А.15. Примечание 2 — Если среднее или высокое значение DC достигнуто в логической схеме, то должен применяться хотя бы один метод изменяемой памяти, неизменяемой памяти и процессора со значением DC как минимум 60 %. Также могут применяться методы, не описанные в данной таблице.	

Е.2 Определение среднего диагностического охвата DC (DC_{avg})

Во многих системах может быть использовано несколько методов обнаружения сбоев. Эти методы могут проверять разные части SRP/CS и могут иметь разное DC. Для определения PL по рисунку 5 можно использовать только одно среднее значение DC для всего SRP/CS.

DC может быть определен как отношение между частотой обнаруженных сбоев и частотой сбоев в общем. Из этого определения следует, что средний диагностический охват (DC_{avg}) определяется по формуле (Е.1):

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \qquad (E.1)$$

В данном случае все компоненты SRP/CS без исключения должны быть рассмотрены и суммированы. Для каждого блока учитывается $MTTF_d$ и DC. DC в этой формуле означает отношение частоты обнаруженных сбоев этой части (несмотря на примененные методы обнаружения сбоев) и частоты всех сбоев этой части. Таким образом, DC относится к проверенной части, а не к проверяющему устройству. В компонентах без системы обнаружения сбоев (которые не проверяются) DC = 0 и они влияют только на знаменатель DC_{avg}.

Приложение F
(справочное)

Оценка отказа по общей причине (CCF)

F.1 Требования для CCF

Подробное описание мер предотвращения отказов по общей причине CCF для датчиков и исполнительных устройств и частично для логических схем приведено в [8], приложение D. Не все меры, приведенные там, применимы в машиностроении. Самые важные меры приведены в данном приложении.

Примечание — В настоящем стандарте считается, что в резервных системах β — фактор согласно [6] должен быть меньше или равен 2 %.

F.2 Оценка эффекта CCF

Количественный процесс должен пройти во всей системе. Каждая часть, связанная с обеспечением безопасности системы управления, должна быть рассмотрена.

В таблице F.1 перечисляются методы уменьшения отказов по общим причинам и содержатся соответствующие значения, основанные на инженерной экспертизе.

Для каждого перечисленного метода может быть достигнута только высшая оценка или ничего. Если метод выполнен только частично, то оценка этого метода равна нулю.

В таблице F.2 представлена количественная оценка по CCF.

Таблица F.1 — Количественная оценка мер предотвращения CCF

	Меры предотвращения CCF	Оценка
1	Разделение/Отделение	
	Физическое разделение между сигнальными каналами: - разделение в проводке/трубопроводе; - достаточный зазор и расстояние между проводниками на печатных платах	15
2	Разнообразие	
	Используются разные технологии или физические принципы: - первый канал электронный с возможностью программирования, а второй канал оптико-проводной; - способ запуска; - давление и температура. Измерение расстояния и давления, цифровое и аналоговое. Компоненты от разных производителей	20
3	Проектирование/Приложение/Опыт	
3.1	Защита от скачков напряжения, перепадов давления и скачков тока и т. д.	15
3.2	Используемые успешно испытанные компоненты	5
4	Оценка/анализ	
	Учтены ли все результаты анализа режима сбоев, чтобы избежать сбоев по общей причине	5
5	Компетентность/обучение	
	Были ли проектировщики/операторы обучены, чтобы понимать причины и последствия сбоев по общим причинам?	5
6	Экология	
6.1	Предотвращение загрязнения и электромагнитная совместимость согласно соответствующим стандартам. Струйные системы: фильтрация рабочей среды под давлением, предотвращение попадания грязи, спуск сжатого воздуха в соответствии с требованиями разработчиков, что касается чистоты рабочей среды под давлением. Электрические системы: проверена ли система на электромагнитную совместимость согласно соответствующим стандартам? Для комбинированных систем струйных и электрических — оба аспекта должны быть приняты во внимание	25

Окончание таблицы F.1

	Меры предотвращения CCF	Оценка
6.2	Другие влияния Соответствует ли система всем требованиям к иммунитету на все возможные экологические влияния, такие как температура, ударная нагрузка, вибрация, влажность? (согласно соответствующим стандартам)	10
	Сумма	максимально достижимая 100

Таблица F.2 — Количественная оценка CCF

Общая оценка	Меры предотвращения CCFa)
65 и более	Соответствует требованиям
Менее 65	Процесс не удался — выберите дополнительные меры
a) Когда технические меры не являются актуальными, баллы в этой колонке могут учитываться в комплексном расчете.	

Приложение G
(справочное)

Систематический сбой

G.1 Общая информация

Подробный список мер предотвращения систематических сбоев, которые должны быть приняты согласно общим и хорошо проверенным принципам безопасности, приведен в ISO 13849-2.

G.2 Методы контроля систематических сбоев

Должны быть применены следующие меры:

- использование обесточивания (см. ISO 13849-2).

Система управления должна быть разработана так, что при потере энергии машина может достигнуть и поддерживать безопасное состояние;

- методы контроля эффектов электрического пробоя, перепадов напряжения, перенапряжения и пониженного напряжения.

Реакция SRP/CS на электрический пробой, перепады напряжения, перенапряжение и пониженное напряжение должна быть определена заранее так, чтобы машина могла достигнуть и поддерживать безопасное состояние (см. также [29] и А.8 [9]);

- методы контроля и предотвращения эффектов физического характера (температура, влажность, вода, вибрация, пыль, ржавеющие вещества, электромагнитное воздействие).

Реакция SRP/CS на эффекты физического характера должна быть определена заранее так, чтобы машина могла достигнуть и поддерживать безопасное состояние (см. также [31] и 29]);

- контроль управляющей программы должен быть осуществлен в SRP/CS с применением программного обеспечения, позволяющего обнаружить неисправности в управляющей программе.

Неисправности появляются, если отдельные элементы программы (модули приложений, подпрограммы или команды) обрабатываются в неправильной последовательности, или в неправильный промежуток времени, или при неправильных настройках часов процессора (см. А.9 [9]);

- методы контроля эффектов ошибок, возникающих во время любого процесса передачи данных (см. 7.4.8 [6]).

В дополнение один или более из следующих методов должен быть применен, принимая во внимание сложность SRP/CS и PL:

- обнаружение сбоев при помощи автоматических проверок;
- проверки при использовании резервированного оборудования;
- разнообразное оборудование;
- работа в положительном режиме;
- механические контакты;
- процесс прямого размыкания контактов;
- ориентированный режим отказа;
- превышение параметров на необходимую величину коэффициента, с помощью чего производитель может показать, что ухудшение номинальных значений параметров увеличит надежность — в тех случаях, когда такое превышение возможно, должен применяться коэффициент запаса со значением не менее 1,5.

См. также ISO 13849-2, D.3.

G.3 Меры по исключению систематических сбоев

Должны осуществляться следующие меры:

- применение подходящих материалов и надлежащей обработки.

Выбор материала, методов получения и обработки, например, в зависимости от напряжения, прочности, упругости, трения, износа, подверженности коррозии, температуры, электропроводности, диэлектрической прочности;

- правильное задание размеров и формы.

Например, в зависимости от напряжения, подверженности деформации, усталостной нагрузки, температуры, шероховатости поверхности, допусков, обработки;

- правильный подбор, сочетание, размещение, сборка и установка элементов, включая прокладку кабеля, проводной монтаж и другие соединения.

Применять необходимые стандарты и указания по применению от производителя, например, страницы каталога, инструкции по установке, спецификации, а также применение надлежащей инженерно-технической практики;

- совместимость.

Использовать элементы, имеющие совместимые рабочие характеристики;

- выдержка заданных условий окружающей среды.

Разрабатывать SRP/CS так, чтобы они могли работать во всех ожидаемых условиях окружающей среды и любых предвиденных неблагоприятных условиях, например, температуры, влажности, вибрации и электромагнитного излучения (см. ISO 13849-2, G.2);

- использование элементов, разработанных в соответствии с установленным стандартом и имеющих четко определенные режимы сбоя.

Сократить риск появления необнаруженных неисправностей с помощью применения элементов с особыми характеристиками (см. В.3.3 [9]).

Кроме того, в зависимости от сложности SRP/CS и его PL должна применяться одна или более из приведенных мер;

- оценка аппаратно-приводных средств технического обеспечения (например, осмотром или сквозным контролем).

Выявить несоответствия между спецификацией и фактическим исполнением с помощью оценки и анализа (см. В.3.7 и В.3.8 [9]);

- автоматизированное проектирование инструментальных средств систем, поддерживающих моделирование или анализ.

Представляют систематизированную методику расчета и включают в себя автоматизированные элементы конструкции, которые уже доступны и протестированы (см. В.3.5 [9]);

- моделирование.

Представляет систематизированный и всесторонний контроль конструкции SRP/CS на основе функциональных возможностей и правильного задания параметров их компонентов (см. В.3.6 [9]).

G.4 Меры по исключению систематических сбоев в процессе интеграции SRP/CS

Следующие меры должны быть приняты в процессе интеграции SRP/CS:

- функциональное тестирование;
- проектное управление;
- документирование.

Кроме того, в зависимости от сложности SRP/CS и их PL должно быть проведено тестирование методом черного ящика.

Приложение Н
(справочное)

Пример комбинации нескольких элементов системы управления, связанных с обеспечением безопасности

Рисунок Н.1 является принципиальной схемой в части обеспечения безопасности одной из функций управления исполнительным механизмом станка. Это не функциональная/рабочая схема, этот рисунок показан только для наглядного представления принципа объединения категорий и технических средств для выполнения одной функции.

Контроль обеспечивается посредством электронной логической схемы управления и гидрораспределителя. Снижение риска происходит за счет AOPD, которое обнаруживает возможность появления опасной ситуации и предотвращает внезапный пуск гидроцилиндра, когда происходит прерывание светового луча.

К элементам безопасности, выполняющим функцию безопасности, относятся: AOPD, электронная логическая схема управления, гидрораспределитель и средства связи.

Такие объединенные элементы безопасности обеспечивают функцию останова, которая является функцией безопасности. Когда происходит прерывание светового луча в AOPD, устройство вывода подает сигнал на электронную логическую схему управления, которая передает сигнал на гидрораспределитель, чтобы остановить поток жидкости на выходе SRP/CS. На станке происходит останов опасного перемещения исполнительного механизма.

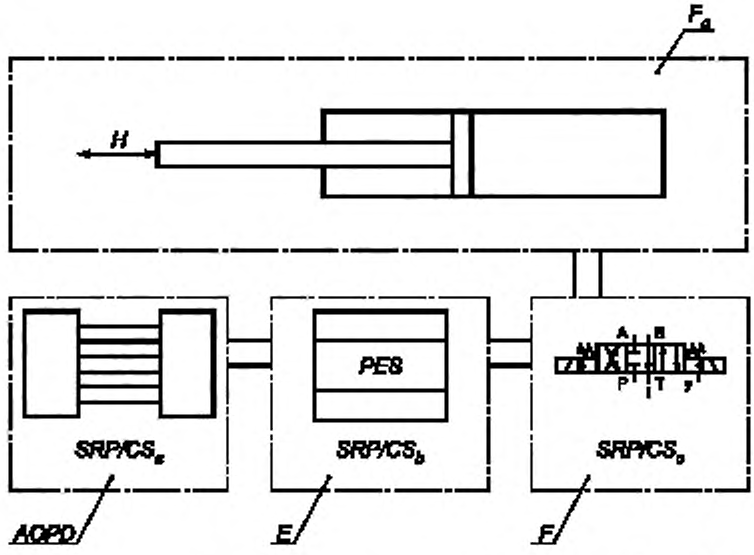
Комбинация элементов безопасности обеспечивает функцию безопасности, которая представляет собой сочетание разных категорий и технических средств на основании требований, изложенных в разделе 6. С помощью принципов, приведенных в настоящем стандарте, элементы безопасности, показанные на рисунке Н.2, можно описать следующим образом:

- категория 2, PL = *c* для электрочувствительного предохранительного оборудования (световой барьер). Для уменьшения вероятности возникновения неисправности в этом оборудовании применяются хорошо проверенные принципы безопасности;
- категория 3, PL = *d* для электронной логической схемы управления. Для увеличения уровня эффективности защиты электронной логической схемы управления в этом SRP/CS реализуется структура с резервированием, которая обеспечивает выполнение нескольких мер по определению неисправностей, с помощью чего определяется большая часть одиночных неисправностей;
- категория 1, PL = *c* для гидрораспределителя. Статус успешно испытанных присваивается преимущественно элементам специального назначением. В данном примере распределитель считается успешно испытанным компонентом. Для сокращения вероятности возникновения неисправностей устройство составлено из успешно испытанных компонентов с применением хорошо проверенных принципов безопасности, все условия эксплуатации учитываются (см. 6.2.4).

Примечание 1 — Положение, размер и компоновка средств связи должны быть учтены.

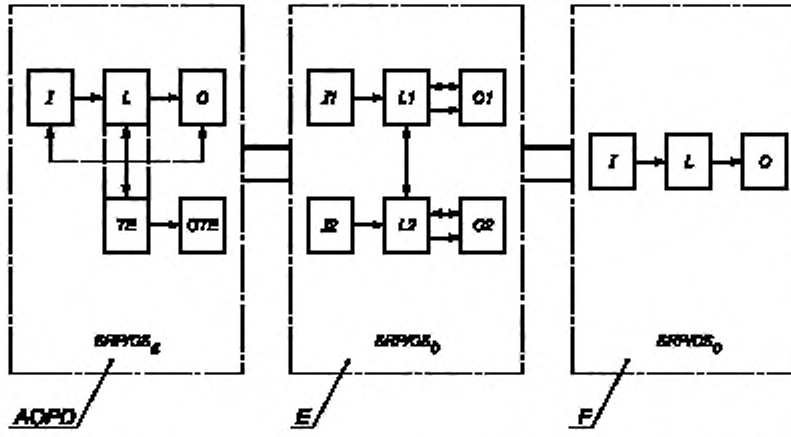
Такое сочетание со значениями PL_{low} = *c* и N_{low} = 2 приводит к общему значению уровня PL = *c* (см. 6.3).

Примечание 2 — В случае возникновения одной неисправности в элементах категории 1 или категории 2 на рисунке Н.2 возможна потеря функции безопасности.



AOPD — активное оптоэлектронное защитное устройство (например, световой барьер); *SRP/CS*$_a$: категория 2 [тип 2], *PL* = *c*; *E* — электронная логическая схема управления, *SRP/CS*$_b$: категория 3, *PL* = *d*; *F* — гидрораспределитель, *SRP/CS*$_b$: категория 1, *PL* = *c*; F_a — гидроцилиндр; *H* — опасное перемещение

Рисунок Н.1 — Пример. Структурная схема, поясняющая комбинации SRP/CS



AOPD — активное оптоэлектронное защитное устройство (например, световой барьер); *E* — электронная логическая схема управления, *F* — гидрораспределитель; *I*, *I1*, *I2* — входные устройства, например, датчик; *L*, *L1*, *L2* — логические блоки; *O*, *O1*, *O2*, *OTE* — выходные устройства, например, главный контактор; *TE* — испытательное оборудование

Рисунок Н.2 — Структурное построение для рисунка Н.1

Приложение I
(справочное)

Примеры

I.1 Общие сведения

Данное приложение содержит примеры использования методов, изложенных в предыдущих приложениях, для идентификации функции безопасности и определения PL. Также приведена количественная оценка двух широко применяемых схем управления. Для поэтапной процедуры см. рисунок 3.

Два примера различных схем управления, A и B, рассмотрены на рисунке I.1 и I.3. Оба примера представляют выполнение одной и той же функции блокировки защитной дверцы. Первый пример построен в виде одного канала электромеханического элемента с высоким значением $MTTF_d$, а второй состоит из двух каналов — одного электромеханического и другого программируемого электронного, — включая испытания, но состоит из элементов с более низким значением $MTTF_d$.

I.2 Функция безопасности и требуемый уровень эффективности защиты (PL_r)

Для обоих примеров функция безопасности блокировки защитного устройства может быть выбрана следующим образом.

Опасное перемещение будет остановлено, если защитная дверца будет открытой (обеспечивается отключением электродвигателя).

Параметры риска согласно методу, основанному на графе риска (см. рисунок А.1):

- последствия, S = S2, серьезный ущерб;
- частота и/или время воздействия опасности, F = F1, от редкого до более частого возникновения опасности и/или непродолжительное время воздействия опасности;
- вероятность избегания опасности, P = P1, возможно при некоторых условиях.

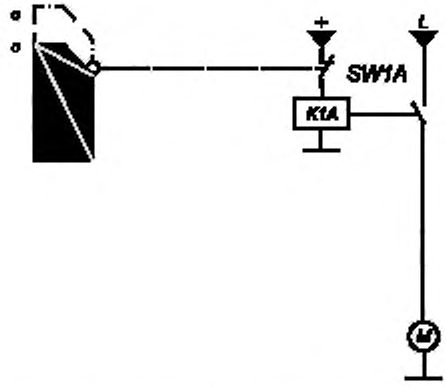
Такой выбор решений приводит к определению $PL_r = c$.

Определение предпочтительной категории: уровень эффективности защиты достигается наиболее надежными одноканальными системами (категория 1) или резервными структурами (категория 2 или 3) (см. рисунок 5 и раздел 6).

I.3 Пример A, одноканальная система

I.3.1 Идентификация элементов безопасности

На рисунке I.1 представлены все элементы, вносящие вклад в обеспечение функции безопасности. Функциональные элементы, не вносящие вклад в обеспечение функции безопасности блокировки (такие как пуск и остановы), не изображены.



o — разомкнуто; *c* — замкнуто; *M* — двигатель; *K1A* — контактор;
SW1A — выключатель (нормально замкнутый)

Рисунок I.1 — Схема управления A для выполнения функции безопасности

В данном примере дверной выключатель связан с контактором, который отключает соединение, передающее мощность двигателю, а также нормально замыкает контакты (но без подтверждения исключения неисправностей):

- один канал электромеханического компонененты;
- выключатель SW1A имеет средний уровень значения $MTTF_d$;
- контактор K1A имеет низкий уровень значения $MTTF_d$.

Выбранный контактор в данном примере является успешно испытанным компонентом в соответствии с ISO 13849-2.

Таким образом, элементы безопасности и их распределение по каналам можно представить в виде структурной схемы безопасности, как на рисунке I.2.

K1A — контактор; *SW1A* — выключатель

Рисунок I.2 — Структурная схема, представляющая элементы безопасности для примера А

I.3.2 Количественная оценка $MTTF_d$ для каждого канала, DC_{avg}, CCF, категории, PL

Принято проводить оценку $MTTF_d$ для каждого канала, DC_{avg} и отказа по общей причине в соответствии с приложениями C, D, E и F, или оценка предоставляется производителем. Оценка категорий производится в соответствии с 6.2. Оценки:

- $MTTF_d$

Контактор K1A и выключатель SW1A вносят вклад в значение $MTTF_d$ для одного канала. Принято, что значения $MTTF_{dK1A}$ = 50 лет и $MTTF_{dSW1A}$ = 20 лет предоставляются производителем. Согласно методу расчета элементов из D.1 значение $MTTF_d$ для одного канала рассчитывается по формуле (I.1):

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{dSW1A}} + \frac{1}{MTTF_{dK1A}} = \frac{1}{20\ лет} + \frac{1}{50\ лет} = \frac{0{,}07}{лет} \qquad (I.1)$$

откуда получается $MTTF_d$ = 14,3 года или «среднее значение» для канала согласно 4.5.2, таблице 5.

Примечание — Если информация для K1A недоступна, то принимается наихудший вариант согласно C.2 или C.4.

- DC

Поскольку тестирование для структурной схемы А не проводится, то принимается DC = 0 согласно 4.5.3, таблице 6;

- категория

Несмотря на то что для данной схемы предпочтительной категорией является категория 1, результатом расчета $MTTF_d$ канала является «среднее значение». Это говорит о том, что такой схемой достигается только категория B.

Входные данные для рисунка 5: $MTTF_d$ для каждого канала «среднее» (14,3 года), DC_{avg} = 0 и категория B.

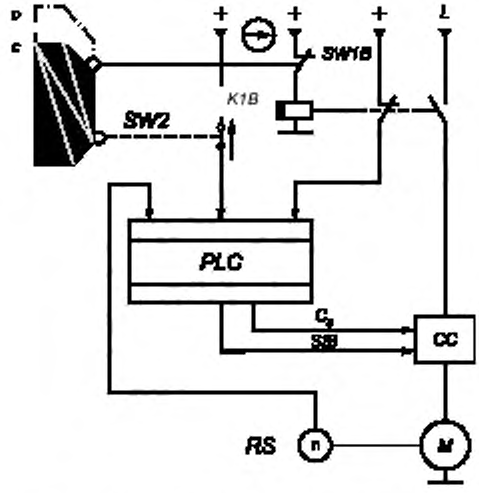
Это может трактоваться как PL= *b*.

Данный результат не совпадает с PL_r согласно I.2. Таким образом, получается, что схема должна быть перестроена и вновь проведена ее оценка, до тех пор пока не будет достигнут уровень эффективности защиты в соответствии с требованиями по сокращению риска для примера, приведенного в I.2.

I.4 Пример B, резервная система

I.4.1 Идентификация элементов безопасности

На рисунке I.3 представлены все элементы, обеспечивающие функции безопасности. Функциональные элементы, не вносящие вклад в обеспечение функции безопасности блокировки (такие как пуск и останов или отключение K1B с выдержкой времени), не изображены.



PLC — программируемый логический контроллер; *CC* — преобразователь тока;
M — двигатель; *RS* — датчик вращения; *o* — разомкнуто; *c* — замкнуто;
C_S — функция безопасного останова (стандартная); *SIB* — импульс безопасной блокировки;
K1B — контактор, *SW1B* — выключатель (нормально замкнутый);
SW2 — выключатель (нормально разомкнутый)

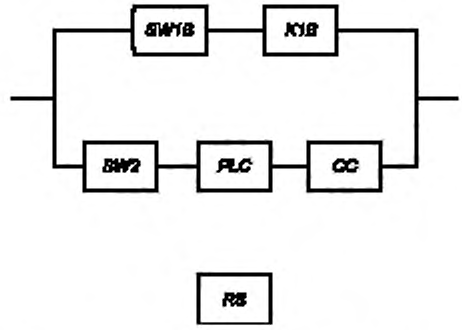
Рисунок I.3 — Схема управления B для выполнения функции безопасности

Во втором примере используются два канала, обеспечивающие резервирование. В первом канале, наподобие примера A, используется дверной выключатель с прямым открытым действием, который работает в позитивном режиме приведения в действие. Дверной выключатель связан с контактором, который отключает соединение, передающее мощность двигателю. Во втором канале используются дополнительные (программируемые) электронные элементы. Второй дверной выключатель связан с программируемым логическим контроллером, который управляет преобразователем тока и отключает соединение, передающее мощность двигателю:

- резервированные каналы, один электромеханический и другой программируемый электронный;
- выключатель SW1B с принудительным механическим замыканием и размыканием контактов, SW2 имеет средний уровень значения $MTTF_d$;
- контактор K1B имеет средний уровень значения $MTTF_d$, в данном примере выбранный контактор не является успешно испытанным компонентом;
- электронные компоненты имеют средний уровень значения $MTTF_d$.

Таким образом, элементы безопасности и их распределение по каналам можно представить в виде структурной схемы элементов безопасности, как показано на рисунке I.4.

Примечание — Во избежание излишних различий необходимо отметить, что требования к программному обеспечению согласно 4.6 для канала PLC не применяются.



SW1B и *K1B* составляют первый канал, *SW2*, *PLC* и *CC* составляют второй канал; *RS* используется только для тестирования преобразователя тока.

SW1B — блокировочное устройство; *K1B* — контактор; *SW2* — выключатель;
PLC — программируемый логический контроллер, *CC* — преобразователь тока;
RS — датчик вращения

Рисунок I.4 — Структурная схема,
представляющая элементы безопасности для примера B

I.4.2 Количественная оценка $MTTF_d$ для каждого канала, DC_{avg}, CCF, категории, PL

Принято проводить оценку $MTTF_d$ для каждого канала, DC_{avg} и CCF в соответствии с приложениями C, D, E и F, или оценка предоставляется производителем. Оценка категорий производится в соответствии с 6.2.

Выключатель SW1B имеет прямое открытое действие и работает в негативном режиме приведения в действие. Поэтому исключение неисправностей проводится при неразомкнутом контакте и не приведенном в действие выключателе из-за механической неисправности (например, поломка плунжера, износ рабочего кулачка, разрегулировка).

Примечание — Такие допущения действительны для выключателей вспомогательных цепей согласно IEC 60957-5-1, приложение K, при условии надежного механического крепления и приведения выключателей в действие согласно спецификации производителя (см. ISO 13849-2).

Оценка:

- $MTTF_d$

Контактор K1B является единственным элементом, вносящим вклад в значение $MTTF_d$ первого канала. Принято, что значение $MTTF_{dK1B}$ = 30 лет предоставляется производителем. Согласно методу расчета элементов из D.1 значение $MTTF_d$ для первого канала рассчитывается по формуле (I.2):

$$\frac{1}{MTTF_{dC1}} = \frac{1}{MTTF_{dK1B}} \tag{I.2}$$

откуда получается $MTTF_d$ = 30 лет.

Во втором канале в значение $MTTF_{dC2}$ вносят вклад элементы SW2, PLC, CC. Принято, что для этих трех компонентов, также как и для компонента RS, значение $MTTF_d$ = 20 лет предоставляется производителем. Согласно методу расчета элементов из D.1 значение $MTTF_{dC2}$ для второго канала рассчитывается по формуле (I.3):

$$\frac{1}{MTTF_{dC2}} = \frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}} = \frac{1}{20\ лет} + \frac{1}{20\ лет} + \frac{1}{20\ лет} = \frac{0{,}15}{лет} \tag{I.3}$$

откуда получается $MTTF_d$ = 6,7 года.

Поскольку два канала имеют разные значения $MTTF_d$, то для расчета значения, которым можно заменить $MTTF_d$ симметричной двуканальной системы на $MTTF_d$ одноканальной, применяется формула из пункта D.2. По этой формуле получаем $MTTF_d$ = 20 лет или «среднее значение» для канала согласно 4.5.2, таблица 5;

- DC

В схеме управления B четыре элемента безопасности тестируются с помощью PLC: SW2 и K1B проверяются с помощью PLC, PLC является самотестирующимся элементом и CC контролируется через RS с помощью PLC. Соответствующее значение DC каждого протестированного элемента:

1) DC_{SW2} = 60 %, «низкое значение» вследствие контроля входных сигналов без испытания в динамическом режиме, см. таблицу E.1 (третья строка раздела таблицы «входное устройство»);

2) DC_{K1B} = 99 %, «высокое значение» благодаря наличию нормально замкнутых и разомкнутых механически связанных контактов, см. таблицу Е.1 (вторая строка раздела таблицы «входное устройство»);

3) DC_{PLC} = 30 %, «несущественное значение» вследствие низкой эффективности самотестирования (принимается, что производитель рассчитал это значение методом анализа видов и последствий отказов), и

4) DC_{CC} = 90 %, «среднее значение» благодаря наличию резервированного канала выключения и контролю привода с помощью логической схемы управления, см. таблицу Е.1 (шестая строка раздела таблицы «выходное устройство») — если PLC отслеживает отказы CC, тогда можно остановить перемещение с помощью импульса безопасной блокировки (дополнительный канал выключения).

Для оценки PL по рисунку 5 необходимо среднее значение DC (DC_{avg}) в качестве входного, рассчитанного по формуле (I.4).

$$DC_{avg} = \frac{\frac{DC_{SW2}}{MTTF_{dSW2}} + \frac{DC_{K1B}}{MTTF_{dK1B}} + \frac{DC_{PLC}}{MTTF_{dPLC}} + \frac{DC_{CC}}{MTTF_{dCC}}}{\frac{1}{MTTF_{dSW2}} + \frac{1}{MTTF_{dK1B}} + \frac{1}{MTTF_{dPLC}} + \frac{1}{MTTF_{dCC}}} = \frac{\frac{0,6}{20\,л} + \frac{0,99}{30\,л} + \frac{0,3}{20\,л} + \frac{0,9}{20\,л}}{\frac{1}{20\,л} + \frac{1}{30\,л} + \frac{1}{20\,л} + \frac{1}{20\,л}} = \frac{0,123}{0,183} = 67,1\ \% \quad (I.4)$$

Таким образом, значение DC_{avg} является «низким» согласно 4.5.3 и таблице 6;

- CCF

Принято, что оценка мер, направленных на предотвращение отказа по общей причине CCF согласно F.2 была проведена для схемы управления В. Баллы назначаются как показано в таблице I.1.

Таблица I.1 — Оценка мер, направленных на предотвращение отказа по общей причине CCF, для примера В

Наименование		Балл оценки схемы управления	Максимально возможный балл
1	Разделение/отделение		
	Физическое разделение между каналами сигналов	15	15
2	Многообразие		
	Применение различных технологий/конструкций или физических принципов	20	20
3	Разработка/применение/эксплуатация		
3.1	Защита от перенапряжения, избыточного давления, перегрузки по току и т. д.	0	15
3.2	Использование успешно испытанных компонентов	5	5
4	Оценка/анализ		
	Учтены ли результаты анализа видов и последствий отказов, проведенного с целью исключения отказа по общей причине в расчете?	5	5
5	Компетентность/обученность		
	Обучены ли разработчики пониманию причин и последствий отказов по общей причине?	0	5
6	Окружающая среда		
6.1	Предотвращение загрязнения и электромагнитной совместимости (ЭМС) перед CCF в соответствии с необходимыми стандартами	25	25
6.2	Другие воздействия Учтены ли требования невосприимчивости ко всем существенным изменениям окружающей среды, таким как температура, ударная нагрузка, вибрации, влажность (например, как указано в соответствующих стандартах)?	10	10
	Итого	80	Максимум 100

Принятые меры по предотвращению CCF считаются достаточными при минимальном количестве баллов 65. В примере В количество баллов 80 является достаточным для выполнения требований для CCF.

Одиночная неисправность какого-либо элемента не ведет к потере функции безопасности. Там, где практически возможно, одиночная неисправность должна обнаруживаться до или во время следующего запроса на выполнение функции безопасности. DC_{avg} должен находиться в интервале от 60 до 90 %. Меры по предотвращению CCF должны быть достаточными. Данные характеристики являются типовыми для категории 3.

Входные данные для рисунка 5: $MTTF_d$ для канала «среднее значение» (20 лет), DC_{avg} «малое значение» и категория 3.

Это может трактоваться, как PL = *c*.

Данный результат совпадает с требуемым уровнем эффективности защиты с из I.2. Таким образом, схема управления В соответствует требованиям по сокращению риска для примера, приведенного в I.2.

Приложение J
(справочное)

Программное обеспечение

J.1 Описание примера

В данном приложении представлены примеры реализации SRESW соответствующего SRP/CS для PL_r = *d*. SRP/CS связаны с оборудованием машины, что обеспечивает:

- сбор информации, переданной различными датчиками;
- обработку данных, необходимую для работы элементов системы управления с учетом требований по безопасности; и
- управление исполнительными механизмами.

Схематическое представление работы SRESW на уровне функциональных блоков показано на рисунке J.1.

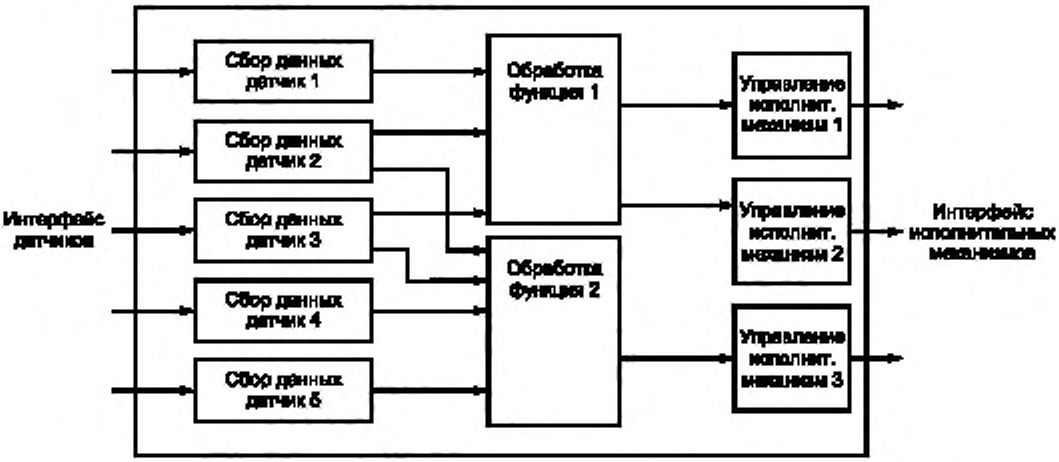


Рисунок J.1 — Пример схематического представления работы программного обеспечения на уровне функциональных блоков

J.2 Применение V-модели жизненного цикла безопасности программного обеспечения

В таблице J.1 представлен типовой синтез выполняемых работ и документации по применению V-модели жизненного цикла безопасности программного обеспечения для контроля машины.

Таблица J.1 — Выполняемые работы и документация жизненного цикла безопасности программного обеспечения

Опытно-конструкторские работы	Работы по верификации	Соответствующая документация
Машина: Идентификация функций, включающих элементы системы управления, связанные с безопасностью	Идентификация функций безопасности	«Спецификация безопасности для контроля машин»
Структура: Построение структуры управления, включающей датчики и исполнительные механизмы	Комментарии к параметрам безопасности выбранных элементов	«Построение структуры управления»
Спецификация программного обеспечения: Перевод функций машины в функции программного обеспечения	Перечитывание описаний (см. J.3)	«Описание программного обеспечения»
Структура ПО: Группирование функций в функциональные блоки	Описание критических блоков, которые являются объектами более масштабного анализа и проверки	«Моделирование функциональных блоков»
Кодирование: Кодирование в соответствии с правилами программирования (см. J.4)	Перечитывание кода. Проверка функций и их соответствия правилам	«Кодирование комментариев в программе»; «Кодирование страниц, подлежащих перечитыванию»
Проверка: Выполнение тестовых сценариев: эксплуатационный аспект функций; аспект поведения в случае отказа	Проверка тестового покрытия; Проверка результатов тестирования	«Матрица соответствия», которая дает перекрестные ссылки на пункты спецификации и необходимые тестирования «Протоколы испытаний», включающие в себя тестовые сценарии и комментарии к полученным результатам

J.3 Проверка соответствия программного обеспечения его спецификации

Как часть жизненного цикла безопасности программного обеспечения работа по верификации на уровне спецификации программного обеспечения заключается в чтении описаний с целью подтверждения, что все особые позиции описаны корректно. При проверке каждой функции необходимо учитывать:

- ограничение случаев ошибочной интерпретации спецификации системы;
- избежание расхождений в спецификации, что приводит к непредсказуемому поведению SRP/CS;
- точное описание условий включения и отключения функций;
- гарантию того, что все возможные исходы учтены и проработаны;
- проверку согласованности;
- различные варианты параметризации;
- поведение вследствие отказа.

J.4 Примеры правил программирования

Для случая отказа по общей причине должна быть предусмотрена возможность аутентификации программы по таким данным, как автор, дата загрузки, версия и последний вид доступа к программе. Следующие правила программирования могут быть выделены:

а) правила программирования на уровне структуры программы.

Программирование должно быть выполнено так, чтобы общая структура была последовательной и понятной и позволяла легко определить местонахождение различной обработки данных, что подразумевает:

1) применение шаблонов типовой программы или функциональных блоков;

2) деление программы на части для того, чтобы определить основные элементы, соответствующие «входам», «обработке данных» и «выходам»;

3) комментарии к каждой части программы в ее начале, чтобы облегчить обновление комментария в случае внесения изменений;

4) описание возможностей, которыми обладает функциональный блок, при его вызове;

5) ячейки памяти должны заполняться одним-единственным типом данных, и должны применяться единые метки;

6) порядок работы не должен зависеть от переменных величин, таких как адрес перехода, полученный во время выполнения программы, и условные разрешенные переходы;

b) правила программирования, касающиеся применения переменных величин:

- срабатывание и останов любого выходного устройства должны происходить только один раз (централизованные условия);
- программа должна быть построена так, чтобы уравнения для обновления переменной величины были централизованы;
- каждая глобальная переменная, вход или выход, должна иметь достаточно явное мнемоническое имя, а также должна быть описана комментарием в начале программы;

c) правила программирования на уровне функционального блока:

- предпочтительно использовать функциональные блоки, которые были утверждены поставщиком элементов системы управления, связанных с обеспечением безопасности, при этом проверяя, чтобы принятые условия эксплуатации этих утвержденных блоков соответствовали условиям программы;
- размер кодового блока должен быть ограничен следующими величинами:

I) параметрами — максимум восемь цифр и два целочисленных входа, один выход;

II) функциональным кодом — максимум 10 локальных переменных, максимум 20 булевых уравнений;

- функциональные блоки не должны изменять глобальные переменные;
- цифровое значение должно контролироваться относительно заданных критериев с целью обеспечения области достоверности;
- функциональный блок должен быть проверен на несовместимость переменных;
- код неисправности блока должен обеспечивать выделение одной неисправности среди остальных;
- коды неисправностей и состояние блока после определения неисправности должны быть описаны комментариями;
- возврат блока в исходное состояние или восстановление нормального состояния должны быть описаны комментариями.

Приложение К
(справочное)

Числовое представление рисунка 5

См. таблицу К.1.

Таблица К.1 — Числовое представление рисунка 5

$MTTF_d$ каждого канала, лет	Средняя вероятность опасного отказа в час (1/ч) и соответствующий уровень эффективности защиты (PL)						
	Кат. B PL DC_{avg} = 0 (никакое)	Кат. 1 PL DC_{avg} = 0 (никаков)	Кат. 2 PL DC_{avg} = низкое	Кат. 2 PL DC_{avg} = среднее	Кат. 3 PL DC_{avg} = низкое	Кат. 3 PL DC_{avg} = среднее	Кат. 4 PL DC_{avg} = высокое
3	$3{,}80\times10^{-5}$ a		$2{,}58\times10^{-5}$ a	$1{,}99\times10^{-5}$ a	$1{,}26\times10^{-5}$ a	$6{,}09\times10^{-6}$ b	
3,3	$3{,}46\times10^{-5}$ a		$2{,}33\times10^{-5}$ a	$1{,}79\times10^{-5}$ a	$1{,}13\times10^{-5}$ a	$5{,}41\times10^{-6}$ b	
3,6	$3{,}17\times10^{-5}$ a		$2{,}13\times10^{-5}$ a	$1{,}62\times10^{-5}$ a	$1{,}03\times10^{-5}$ a	$4{,}86\times10^{-6}$ b	
3,9	$2{,}93\times10^{-5}$ a		$1{,}95\times10^{-5}$ a	$1{,}48\times10^{-5}$ a	$9{,}37\times10^{-6}$ b	$4{,}40\times10^{-6}$ b	
4,3	$2{,}65\times10^{-5}$ a		$1{,}76\times10^{-5}$ a	$1{,}33\times10^{-5}$ a	$8{,}39\times10^{-6}$ b	$3{,}89\times10^{-6}$ b	
4,7	$2{,}43\times10^{-5}$ a		$1{,}60\times10^{-5}$ a	$1{,}20\times10^{-5}$ a	$7{,}58\times10^{-6}$ b	$3{,}48\times10^{-6}$ b	
5,1	$2{,}24\times10^{-5}$ a		$1{,}47\times10^{-5}$ a	$1{,}10\times10^{-5}$ a	$6{,}91\times10^{-6}$ b	$3{,}15\times10^{-6}$ b	
5,6	$2{,}04\times10^{-5}$ a		$1{,}33\times10^{-5}$ a	$9{,}87\times10^{-6}$ b	$6{,}21\times10^{-6}$ b	$2{,}80\times10^{-6}$ c	
6,2	$1{,}84\times10^{-5}$ a		$1{,}19\times10^{-5}$ a	$8{,}80\times10^{-6}$ b	$5{,}53\times10^{-6}$ b	$2{,}47\times10^{-6}$ c	
6,8	$1{,}68\times10^{-5}$ a		$1{,}08\times10^{-5}$ a	$7{,}93\times10^{-6}$ b	$4{,}98\times10^{-6}$ b	$2{,}20\times10^{-6}$ c	
7,5	$1{,}52\times10^{-5}$ a		$9{,}75\times10^{-6}$ b	$7{,}10\times10^{-6}$ b	$4{,}45\times10^{-6}$ b	$1{,}96\times10^{-6}$ c	
8,2	$1{,}39\times10^{-5}$ a		$8{,}87\times10^{-6}$ b	$6{,}43\times10^{-6}$ b	$4{,}02\times10^{-6}$ b	$1{,}74\times10^{-6}$ c	
9,1	$1{,}25\times10^{-5}$ a		$7{,}94\times10^{-6}$ b	$5{,}71\times10^{-6}$ b	$3{,}57\times10^{-6}$ b	$1{,}53\times10^{-6}$ c	
10	$1{,}14\times10^{-5}$ a		$7{,}18\times10^{-6}$ b	$5{,}14\times10^{-6}$ b	$3{,}21\times10^{-6}$ b	$1{,}36\times10^{-6}$ c	
11	$1{,}04\times10^{-5}$ a		$6{,}44\times10^{-6}$ b	$4{,}53\times10^{-6}$ b	$2{,}81\times10^{-6}$ c	$1{,}18\times10^{-6}$ c	
12	$9{,}51\times10^{-6}$ b		$5{,}84\times10^{-6}$ b	$4{,}04\times10^{-6}$ b	$2{,}49\times10^{-6}$ c	$1{,}04\times10^{-6}$ c	
13	$8{,}78\times10^{-6}$ b		$5{,}33\times10^{-6}$ b	$3{,}64\times10^{-6}$ b	$2{,}23\times10^{-6}$ c	$9{,}21\times10^{-7}$ d	
15	$7{,}61\times10^{-6}$ b		$4{,}53\times10^{-6}$ b	$3{,}01\times10^{-6}$ b	$1{,}82\times10^{-6}$ c	$7{,}44\times10^{-7}$ d	
16	$7{,}13\times10^{-6}$ b		$4{,}21\times10^{-6}$ b	$2{,}77\times10^{-6}$ c	$1{,}67\times10^{-6}$ c	$6{,}76\times10^{-7}$ d	
18	$6{,}34\times10^{-6}$ b		$3{,}68\times10^{-6}$ b	$2{,}37\times10^{-6}$ c	$1{,}41\times10^{-6}$ c	$5{,}67\times10^{-7}$ d	
20	$5{,}71\times10^{-6}$ b		$3{,}26\times10^{-6}$ b	$2{,}06\times10^{-6}$ c	$1{,}22\times10^{-6}$ c	$4{,}85\times10^{-7}$ d	
22	$5{,}19\times10^{-6}$ b		$2{,}93\times10^{-6}$ c	$1{,}82\times10^{-6}$ c	$1{,}07\times10^{-6}$ c	$4{,}21\times10^{-7}$ d	
24	$4{,}76\times10^{-6}$ b		$2{,}65\times10^{-6}$ c	$1{,}62\times10^{-6}$ c	$9{,}47\times10^{-7}$ d	$3{,}70\times10^{-7}$ d	
27	$4{,}23\times10^{-6}$ b		$2{,}32\times10^{-6}$ c	$1{,}39\times10^{-6}$ c	$8{,}04\times10^{-7}$ d	$3{,}10\times10^{-7}$ d	
30		$3{,}80\times10^{-6}$ b	$2{,}06\times10^{-6}$ c	$1{,}21\times10^{-6}$ c	$6{,}94\times10^{-7}$ d	$2{,}65\times10^{-7}$ d	$9{,}54\times10^{-8}$ e
33		$3{,}46\times10^{-6}$ b	$1{,}85\times10^{-6}$ c	$1{,}06\times10^{-6}$ c	$5{,}94\times10^{-7}$ d	$2{,}30\times10^{-7}$ d	$8{,}57\times10^{-8}$ e
36		$3{,}17\times10^{-6}$ b	$1{,}67\times10^{-6}$ c	$9{,}39\times10^{-7}$ d	$5{,}16\times10^{-7}$ d	$2{,}01\times10^{-7}$ d	$7{,}77\times10^{-8}$ e
39		$2{,}93\times10^{-6}$ c	$1{,}53\times10^{-6}$ c	$8{,}40\times10^{-7}$ d	$4{,}53\times10^{-7}$ d	$1{,}78\times10^{-7}$ d	$7{,}11\times10^{-8}$ e

Окончание таблицы К.1

$MTTF_d$ каждого канала, лет	Средняя вероятность опасного отказа в час (1/ч) и соответствующий уровень эффективности защиты (PL)						
	Кат. B PL DC_{avg} = 0 (никакое)	Кат. 1 PL DC_{avg} = 0 (никакое)	Кат. 2 PL DC_{avg} = низкое	Кат. 2 PL DC_{avg} = среднее	Кат. 3 PL DC_{avg} = низкое	Кат. 3 PL DC_{avg} = среднее	Кат. 4 PL DC_{avg} = высокое
43		$2{,}65\times10^{-6}$ c	$1{,}37\times10^{-6}$ c	$7{,}34\times10^{-7}$ d	$3{,}87\times10^{-7}$ d	$1{,}54\times10^{-7}$ d	$6{,}37\times10^{-8}$ e
47		$2{,}43\times10^{-6}$ c	$1{,}24\times10^{-6}$ c	$6{,}49\times10^{-7}$ d	$3{,}35\times10^{-7}$ d	$1{,}34\times10^{-7}$ d	$5{,}76\times10^{-8}$ e
51		$2{,}24\times10^{-6}$ c	$1{,}13\times10^{-6}$ c	$5{,}80\times10^{-7}$ d	$2{,}93\times10^{-7}$ d	$1{,}19\times10^{-7}$ d	$5{,}26\times10^{-8}$ e
56		$2{,}04\times10^{-6}$ c	$1{,}02\times10^{-6}$ c	$5{,}10\times10^{-7}$ d	$2{,}52\times10^{-7}$ d	$1{,}03\times10^{-7}$ d	$4{,}73\times10^{-8}$ e
62		$1{,}84\times10^{-6}$ c	$9{,}06\times10^{-7}$ d	$4{,}43\times10^{-7}$ d	$2{,}13\times10^{-7}$ d	$8{,}84\times10^{-8}$ e	$4{,}22\times10^{-8}$ e
68		$1{,}68\times10^{-6}$ c	$8{,}17\times10^{-7}$ d	$3{,}90\times10^{-7}$ d	$1{,}84\times10^{-7}$ d	$7{,}68\times10^{-8}$ e	$3{,}80\times10^{-8}$ e
75		$1{,}52\times10^{-6}$ c	$7{,}31\times10^{-7}$ d	$3{,}40\times10^{-7}$ d	$1{,}57\times10^{-7}$ d	$6{,}62\times10^{-8}$ e	$3{,}41\times10^{-8}$ e
82		$1{,}39\times10^{-6}$ c	$6{,}61\times10^{-7}$ d	$3{,}01\times10^{-7}$ d	$1{,}35\times10^{-7}$ d	$5{,}79\times10^{-8}$ e	$3{,}08\times10^{-8}$ e
91		$1{,}25\times10^{-6}$ c	$5{,}88\times10^{-7}$ d	$2{,}61\times10^{-7}$ d	$1{,}14\times10^{-7}$ d	$4{,}94\times10^{-8}$ e	$2{,}74\times10^{-8}$ e
100		$1{,}14\times10^{-6}$ c	$5{,}28\times10^{-7}$ d	$1{,}01\times10^{-7}$ d	$1{,}01\times10^{-7}$ d	$4{,}29\times10^{-8}$ e	$2{,}47\times10^{-8}$ e

Приложение ДА
(обязательное)

Сведения о соответствии межгосударственных стандартов ссылочным международным стандартам

Таблица ДА.1

Обозначение и наименование ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO 12100 Безопасность машин. Основные принципы конструирования. Оценка риска и снижение риска	IDT	ГОСТ ISO 12100-2013 Безопасность машин. Основные принципы конструирования. Оценка риска и снижение риска
ISO 13849-2:2003 Безопасность машин. Детали систем управления, связанные с обеспечением безопасности. Часть 2. Валидация	—	*
ISO 14121 Безопасность машин. Принципы оценки рисков	—	*
IEC 60050-191:1990 Международный словарь по электротехнике — Раздел 191: Функциональная надежность и качество обслуживания	—	*
IEC 61508-1 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования		
IEC 61508-3:1998 + Поправка 1999 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению	—	*
IEC 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и аббревиатуры	—	*

* Соответствующий межгосударственный стандарт отсутствует. До их утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
- IDT — идентичный стандарт.

Библиография

Публикации на программируемые электронные системы

[1] IEC 61000-4-4 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 4: Electrical fast transient/burst immunity test (МЭК 61000-4-4 Электромагнитная совместимость (ЭМС). Часть 4: Методы испытаний и измерений. Раздел 4: Испытания на устойчивость к электрическим быстрым переходным процессам/пачкам)

[2] IEC 61496:1:2004 Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests (МЭК 61496:1:2004 Безопасность машин. Электрочувствительные защитные устройства. Часть 1. Общие требования и испытания)

[3] IEC 61496-2 Safety of machinery — Electro-sensitive protective equipment — Part 2: Particular requirements for equipment using active opto-electronic protective devices [МЭК 61496-2 Безопасность механизмов. Электрочувствительные средства защиты. Часть 2. Частные требования к средствам защиты, использующим активные оптоэлектронные защитные приборы (AOPD)]

[4] IEC 61496-3 Safety of machinery — Electro-sensitive protective equipment — Part 3: Particular requirements for active opto-electronic protective devices responsive to diffuse reflection (AOPDDR) [МЭК 61496-3 Безопасность механизмов. Электрочувствительные средства защиты. Часть 3. Частные требования к средствам защиты, использующим активные оптоэлектронные защитные приборы, чувствительные к рассеянному отражению (AOPDDR)]

[5] IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements (МЭК 61508-1:1998 Безопасность машин. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования)

[6] IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical /electronic/programmable electronic safety-related systems (МЭК 61508-2:2000 Безопасность машин. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к электрическим, электронным, программируемым электронным системам, связанным с безопасностью)

[7] IEC 61508-5:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels (МЭК 61508-5:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности)

[8] IEC 61508-6:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (МЭК 61508-6:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2 и МЭК 61508-3)

[9] IEC 61508-7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures (МЭК 61508-7:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Обзор методов и средств измерения)

[10] IEC 62061:2005 Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems (МЭК 62061:2005 Безопасность машин. Функциональная безопасность электрических, электронных и программируемых электронных систем контроля, связанных с безопасностью)

Другие публикации

[13] ISO 13850:2008 — Safety of machinery — Emergency stop — Principles for design (ИСО 13850:2008 Безопасность машин. Аварийный останов. Принципы проектирования)

[14] ISO 13851 — Safety of machinery — Two-hand control devices — Functional aspects and design principles (ИСО 13851 Безопасность машин. Двуручные устройства управления. Функциональные аспекты и принципы конструирования)

[15] ISO 13856-1 — Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors (ИСО 13856-1 Безопасность машин. Сенсорные защитные устройства. Часть 1. Общие принципы расчета и испытания сенсорных ковриков и полов)

[16] ISO 13856-2 — Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for the design and testing of pressure-sensitive edges and pressure-sensitive bars (ИСО 13856-2 Безопасность машин. Сенсорные защитные устройства. Часть 2. Общие принципы расчета и испытания сенсорных кромок и штанг)

[17] ISO 11428 — Safety of machinery — Visual danger signals — General requirements, design and testing (ИСО 11428 Безопасность оборудования. Визуальные сигналы опасности. Общие требования, конструирование и испытания)

[18] ISO 9001:2008 — Quality management systems — Requirement (ИСО 9001:2008 Системы менеджмента качества. Требования)

[19] ISO 9355-1 — Ergonomic requirements for the design of displays and control actuators — Part 1: Human interactions with displays and control actuators (ИСО 9355-1 Эргономические требования к конструкции дисплеев и органов управления. Часть 1. Взаимодействие человека с дисплеями и органами управления)

[20] ISO 9355-2 — Ergonomic requirements for the design of displays and control actuators — Part 2: Displays (ИСО 9355-2 Эргономические требования к проектированию дисплеев и механизмов управления. Часть 2. Дисплеи)

[21] ISO 9355-3 — Ergonomic requirements for the design of displays and control actuators — Part 3: Control actuators (ИСО 9355-3 Акустика. Определение уровней звуковой мощности источников шума по интенсивности звука. Часть 1. Измерения в отдельных точках)

[22] ISO 11429 — Ergonomics — System of auditory and visual danger and information signals (ИСО 11429 Эргономика. Система звуковых и визуальных сигналов опасности и информационные сигналы)

[23] ISO 7731 — Ergonomics — Danger signal for public and work areas — Auditory danger signals (ИСО 7731 Эргономика. Сигналы опасности для административных и рабочих помещений. Звуковые сигналы опасности)

[24] ISO 4413 — Hydraulic fluid power — General rules relating to systems (ИСО 4413 Гидравлика. Общие правила и требования безопасности систем и их компонентов)

[25] ISO 4414 — Pneumatic fluid power — General rules relating to systems (ИСО 4414-2010 Пневматика. Общие правила и требования безопасности систем и их компонентов)

[26] ISO 13855:2002 Safety of machinery — Positioning of protective equipment with respect to the approach speeds of parts of the human body (ИСО 13855:2002 Безопасность оборудования. Расположение защитных устройств с учетом скоростей приближения частей тела человека)

[27] ISO 14118 Safety of machinery — Prevention of unexpected start-up (ИСО 14118:2008 Безопасность машин. Предупреждение неожиданных пусков)

[28] ISO 19973 Actuators pneumatic. Assessment of the reliability of the components through testing (ISO 19973 Приводы пневматические. Оценка надежности элементов посредством испытаний)

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

[30] IEC 60447 Basic and safety principles for man-machine interface (MMI) — Actuating principles (МЭК 60447 Интерфейс человек — машина. Основные принципы безопасности, маркировка и идентификация. Принципы включения)

[31] IEC 60529 Degrees of protection provided by enclosures (IP code) [МЭК 60529:2001 Степени защиты, обеспечиваемые корпусами (Код IP)]

[32] IEC 60812 Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA) (МЭК 60812 Методы анализа надежности систем — Метод анализа видов и последствий отказов)

[33] IEC 60947 Low-voltage switchgear and control gear (МЭК 60947 Аппаратура коммутационная и механизмы управления низковольтные комплектные)

[34] IEC 61000-6-2 Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments (МЭК 61000-6-2 Электромагнитная совместимость. Часть 6-2. Общие стандарты. Невосприимчивость к промышленной окружающей среде)

[35] IEC 61800-3 Adjustable speed electrical power drive systems — Part 3: EMC requirements and specific test methods (МЭК 61800-3 Системы электроприводов с регулируемой скоростью. Часть 3. Стандартные требования к электромагнитной совместимости продукции и специальные методы испытаний)

[36] МЭК 61810 Electromechanical elementary relays (IEC 61810 Реле электромеханические с ненормируемым временем срабатывания)

[38] IEC 61310 (all parts) Safety of machinery — Indication, marking and actuation (МЭК 61310 (все части) Безопасность машин. Индикация, маркировка и приведение в действие)

[39] IEC 61131-3:2003 Programmable controllers — Part 3: Programming languages (МЭК 61131-3:2003 Микроконтроллеры программируемые. Часть 3. Языки программирования)

[41] EN 614-1 Safety of machinery — Ergonomic design principles — Part 1: Terminology and general principles (ЕН 614-1 Безопасность машин и механизмов. Эргономические принципы проектирования. Часть 1. Терминология и общие принципы)

[42] EN ISO 4413 Hydraulic fluid power — General rules and safety requirements for systems and their components (ЕН ИСО 4413 Гидравлика. Общие правила и требования безопасности систем и их компонентов)

[43] EN ISO 4414	Pneumatic fluid power — General rules and safety requirements for systems and their components (ЕН ИСО 4414 Пневматика. Общие правила и требования безопасности систем и их компонентов)
[44] EN 1005-3	Safety of machinery — Human physical performance — Part 3: Recommended force limits for machinery operation (ЕН 1005-3 Безопасность машин. Физические возможности человека. Часть 3. Рекомендуемые пределы усилий при работе на машинах)
[45] EN 1088:1995	Safety of machinery — Interlocking devices associated with guards — Principles for design and selection (ЕН 1088:1995 Безопасность машин. Блокировочные устройства, связанные с ограждениями. Основные принципы для проектирования и выбора)
[46] EN 50205	Safety switch (ЕН 50205 Реле безопасности)
[47] SN 29500 (all parts)	Failure rates of components (СН 29500 (все части) Интенсивность отказов компонентов)

УДК 621.9.02 – 434.5.006.354 МКС 13.110 ОКП 38 1000, IDT 91 0000 92 2000 96 9000

Ключевые слова: безопасность, машина, риск, защитные устройства, управляющее устройство, элементы систем управления, принципы конструирования

Редактор *В.Н. Колысов*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *И.В. Белюсенко*

Сдано в набор 09.11.2015. Подписано в печать 15.12.2015. Формат 60 × 84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 8,84. Уч.-изд. л. 7,87. Тираж 41 экз. Зак. 4177.

Набрано в ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
www. jurisizdat. ru y-book@mail.ru

Издано и отпечатано во
ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4
www.gostinfo.ru info@gostinfo.ru