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

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO 15998 — 2013

Машины землеройные

СИСТЕМЫ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ КОМПОНЕНТОВ

Критерии эффективности и испытания на функциональную безопасность

(ISO 15998:2008, IDT)

Издание официальное

Москва
Стандартинформ
2014

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 Обществом с ограниченной ответственностью «ИЦ «ЦНИП СДМ» (ООО «ИЦ «ЦНИП СДМ») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 267 «Строительно-дорожные машины и оборудование»

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации по переписке (протокол от 27 декабря 2013 г. № 63-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004–97	Код страны по МК (ИСО 3166) 004–97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Кыргызстан	KG	Кыргызстандарт
Российская Федерация	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Настоящий стандарт идентичен международному стандарту ISO 15998 — 2008 Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety (Машины землеройные. Системы управления с использованием электронных компонентов. Критерии эффективности и испытания на функциональную безопасность).

Международный стандарт разработан Техническим комитетом по стандартизации ISO/TC 127 «Машины землеройные» Международной организации по стандартизации (ISO) и утвержден Европейским комитетом по стандартизации CEN в качестве европейского стандарта без внесения изменений.

Официальные экземпляры международного стандарта, на основе которого подготовлен настоящий межгосударственный стандарт, и международных стандартов, на которые даны ссылки, имеются в национальных органах по стандартизации.

Перевод с английского языка (en).

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

Степень соответствия — идентичная (IDT).

Разработанный стандарт может быть использован при ежегодной актуализации перечня стандартов, содержащих правила и методы исследований (испытаний), а так же стандартов, в результате применения которых на добровольной основе обеспечивается соблюдение требований технического регламента Таможенного союза «О безопасности машин и оборудования».

5 Приказом Федерального агентства по техническому регулированию и метрологии от 19 марта 2014 г. № 177-ст межгосударственный стандарт ГОСТ ISO 15998–2013 введен в действие в качестве национального стандарта Российской Федерации с 1 января 2015 г.

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

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

Машины землеройные

СИСТЕМЫ УПРАВЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ КОМПОНЕНТОВ

Критерии эффективности и испытания на функциональную безопасность

Earth-moving machinery. Machine-control systems (MCS) using electronic components. Performance criteria and tests for functional safety

Дата введения — 2015—01—01

1 Область применения

Настоящий стандарт устанавливает критерии эффективности и методы испытаний на функциональную безопасность систем управления машиной (MCS) с использованием электронных компонентов для землеройных машин и их оборудования, как определено в ISO 6165. Процедура ECE R79, ISO 13849-1 приложение 6, и IEC 62061 могут использоваться в качестве альтернативы, если проверка и испытания выполнены изготовителем с применением раздела 7 настоящего стандарта.

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.

ISO 6165 Earth-moving machinery — Basic types — Identification and terms and definitions (Машины землеройные. Классификация. Термины и определения)

ISO 13766 Earth-moving machinery — Electromagnetic compatibility (Машины землеройные. Электромагнитная совместимость)

IEC 60529 Degrees of protection provided by enclosures (IP Code) Степени защиты, обеспечиваемые корпусами (Код IP)

IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations (Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения)

3 Термины, определения и сокращения

Для целей настоящего стандарта применены термины, определения и сокращения, приведенные в IEC 61508-4, а также ниже перечисленные.

Издание официальное

3.1 Термины и определения

3.1.1

землеройная машина (earth-moving machinery): Самоходная или прицепная машина на гусеничном, колесном или шагающем ходу с рабочим или дополнительным оборудованием (рабочим органом) или с тем и другим, предназначенная главным образом для выполнения работ по выемке, рыхлению, погрузке, транспортированию, бурению, распределению, уплотнению земли, скального грунта и других материалов, а также прокладыванию в них траншей.

[ISO 6165:2006]

3.1.2 **система управления машиной;** MCS (machine-control system): Система, состоящая из компонентов, необходимых для выполнения функций системы, в том числе из датчиков, устройства обработки сигнала, монитора, органов управления и исполнительных механизмов или из нескольких из них.

Примечание — Рамки системы не ограничиваются электронным управлением, а определяются связанной с машиной функцией всей системы. Система, в общем, состоит из электронных, не электронных и соединительных устройств. Она может включать в себя механические, гидравлические, пневматические или оптические компоненты / системы.

3.1.3 **системная единица**(system unit): Часть системы управления машиной, которая содержит любое данное число компонентов и /или частей, объединенных в один или более модулей.

Пример — Блок управления коробкой передач с переключением скоростей под нагрузкой.

Примечание — Как правило, компоненты и/или части установлены в общем корпусе, а системная единица также может быть построена как механическое соединение с несколькими функциональными элементами.

3.1.4 **соединительное устройство** (connection devices): Устройство, используемое для электропитания, а также для передачи сигналов и данных.

3.1.5 **основная функция (система управления машиной)** (basic function (machine-control system): Задача управления.

3.1.6 **основная функция (системная единица)** (basic function (system unit): Получение сигналов и данных, их обработка и/или приведение в действие.

3.1.7 **системная функция** (system function): Любая функция, которая должна быть обработана системой управления машиной или системной единицей.

Примечание — В дополнение к основной функции, системные функции включают диагностику, самоконтроль, обработку сигнала и передачу данных к другим системам.

3.1.8 **концепция безопасности** (safety concept): Концепция, содержащая в себе описание методов, разработанных в системе, направленных на эффективность системы и безопасные действия в случае сбоя.

3.1.9 **связанные с безопасностью системы управления машиной** (safety-related machine-control systems): Системы управления машиной, которые управляют связанными с безопасностью функциями машины.

3.1.10 **безопасное состояние** (safe state): Состояние, в котором управляемое оборудование, процессы или системы автоматически или вручную остановлены или переключены, после нарушения нормальной работы системы управления машиной, в режим предотвращения неожиданных движений или потенциально опасного наращивания накопленной энергии (например, электричество высокого напряжения, гидравлические давления или сжатия пружин).

3.1.11 **проверенный компонент** (well-tried component): Компонент, относящейся к безопасному применению, который с успехом широко использовался ранее в подобных областях, и который был изготовлен и проверен с использованием норм, доказывающих его пригодность и надежность, связанных с безопасностью применения.

Примечание 1 — В некоторых проверенных компонентах определенные отказы также могут быть исключены, потому что коэффициент этих отказов, как известно, является очень низким.

Примечание 2 — Решение о признании отдельного компонента проверенным зависит от области применения.

3.1.12 **замещающая функция** (substitute function): Функция с предоставлением возможности непрерывности процесса в случае сбоя или отказа системы.

3.1.13 **функция аварийного движения** (emergency motion function): Функция, которая может быть применена в случае сбоя или отказа системы, чтобы предоставить возможность оператору осуществить аварийные движения.

Пример — Съезд машины с дороги общего пользования.

3.1.14 **программируемая электронная система;** PES (programmable electronic system): Система управления, защиты или контроля на основе одного или нескольких программируемых электронных устройств, включающая все элементы системы, такие как источники питания, датчики и другие устройства ввода, информационные шины и другие каналы связи, исполнительные механизмы и другие выходные устройства.

3.2 Сокращения

PES – программируемая электронная система;
MCS — система управления машиной;
FMEA –виды отказов и анализ следствий;
FTA — анализ дерева отказов;
ETA — анализ дерева событий;
SIL – достоверный уровень безопасности (см. IEC 61508-4:1998, 3.5.6);
IP Code — код степени защиты;
EMC — электромагнитная совместимость (см. ISO 13766:2006, 3.1);
OSI – взаимодействие открытых систем;
ASIC — прикладная интегральная схема;
RF — радиочастота.

4 Общие требования безопасности

4.1 Применение

Следующие критерии эффективности имеют силу для всех связанных с безопасностью систем управления машины, использующих электронные компоненты. Эти критерии эффективности применимы к любому типу MCS.

4.2 Описание системы управления машиной

Описание системы и краткий обзор должны содержать:

- список всех системных единиц с функциями, связанными с безопасностью;
- схема расположения соединительных устройств и системных единиц, поясняющая связанные с безопасностью функции системы управления машины.

Пример структуры и содержания системы находится в приложении С.

Для каждой системной единицы должны быть определены основные функции и взаимосвязи с другими единицами системы. Это может быть сделано в схематичной форме или с помощью блок-схемы.

Соединения должны быть изображены соответствующим способом; для электрической системы пригодна схема соединений.

Изображение должно однозначно определять каждое соединительное устройство (например, провода) относительно единиц системы (например, маркировкой выводов).

Системные единицы должны быть промаркированы идентификаторами (например, номер, символ, знак), так, чтобы можно было проверить сопоставление изображения системы и реальной MCS, установленной на машине.

Используя идентификатор, изготовитель доказывает, что системные единицы согласуются с документацией в отношении основной функции, концепции безопасности и взаимодействия. Структура идентификатора (например, буквенно-цифровая) может быть определена изготовителем, но должна быть однозначной.

Описание системы должно также включать требования к условиям окружающей среды во время эксплуатации машины:

- климатические условия (температура, влажность);
- механические условия (вибрация, удар);
- коррозийные условия (солевой туман, загазованность);
- электрические условия (не под напряжением, под напряжением линий электропередач);
- электромагнитные условия;
- скачки напряжения питания.

4.3 Описание основных функций

Основная функция системы управления машиной должна быть указана в кратком описании, которое может быть подкреплено графическими средствами, такими как функциональная схема или блок-схема. Описание должно содержать:

- перечень типов и значений входных сигналов MCS;
- перечень типов и значений управляемых выходных сигналов MCS;
- управление по замкнутому/разомкнутому контуру, используемые данные/воспринимающие элементы;
- допустимый рабочий и регулируемый диапазоны.

4.4 Анализ и оценка рисков

Анализ и оценка рисков для MCS должны быть выполнены с использованием описания систем в соответствии с 4.2 применительно к оценке рисков. Это может быть сделано в соответствии с методологией оценки рисков ISO 14121-1 и IEC 61508-5:1998, приложение D. Пример приведен в приложении А настоящего стандарта.

4.5 Критерии эффективности для концепции безопасности

Основные принципы и функции системы, указанные изготовителем для концепции безопасности машины, должны быть учтены при разработке и производстве системы управления машиной. Концепция безопасности включает в себя все меры, предусматривающие безопасные действия при ненормальном режиме работы (для руководства см. IEC 61508-2:2000, подпункт 7.2.3.1). Они должны быть внесены в список общепонятным способом. Примеры мер безопасности:

- дублирование;
- процедуры обнаружения неисправностей;
- безопасное состояние, которое может инициироваться, например, функцией аварийного движения (см. 5.4).

Должно быть предоставлено документированное исследование выполнения концепции безопасности. Это может быть сделано с помощью анализа (например, FMEA, FTA, ETA) или эквивалентных методов, пригодных для концепции безопасности MCS.

Изготовитель должен документировать способ, которым на стадии разработки была проведена проверка правильности логики системы.

Переход от стандартного режима работы в безопасное состояние должен принимать во внимание необходимость устойчивости машины и минимизации риска травматизма людей.

Должен быть возможен вывод (активный или пассивный) машины или ее рабочего/комплектующего оборудования из опасной области или положения в случае сбоя MCS.

4.6 Окружающая среда и условия эксплуатации

4.6.1 Общие требования

Технические характеристики MCS должны быть основаны на условиях окружающей среды, в которой используются машины.

4.6.2 Температура окружающей среды и влажность

Система управления машиной должна безопасно функционировать, в соответствии с условиями, указанными в 7.2.2.

Ограничения, не имеющие никакого влияния на безопасное функционирование MCS, являются допустимыми.

Для особых условий эксплуатации машины и условий установки электронных частей изготовителем могут быть указаны другие условия окружающей среды.

4.6.3 Степень защиты (IP Code)

Основываясь на условиях установки, части MCS, выполняющие функциональную безопасность, должны удовлетворять, по крайней мере, следующей степени защиты, в соответствии с IEC 60529:

- IP 66 — для всех электрических частей, которые устанавливаются вне машины или подвергаются непосредственному воздействию окружающей среды.

Для особых условий эксплуатации машины и условий установки электронных частей изготовителем могут быть указаны другие условия окружающей среды.

4.6.4 Электромагнитная совместимость (EMC)

Система управления машиной должна удовлетворять требованиям стандарта ISO 13766.

4.6.5 Механическая вибрация и удары

Системные единицы, компоненты и части MCS должны быть спроектированы и установлены таким образом, что их функция безопасности поддерживалась при вибрации и ударных нагрузках в течение стандартной работы машины.

См. 7.2.3 и 7.2.4 для условий испытаний.

Для особых условий эксплуатации машины и условий установки электронных частей изготовителем могут быть указаны другие условия окружающей среды.

4.7 Функция аварийного останова

Должна быть предусмотрена функция аварийного останова, если этого требует концепция безопасности. В случае отказа, который может привести к опасным движениям или состоянию машины, аварийный останов должен перевести MCS или системную единицу, или машину в оговоренное безопасное состояние.

5 Дополнительные требования, связанные с безопасностью системы управления машиной

5.1 Общие требования

Требования, касающиеся систем управления машиной, связанных с функцией безопасности, должны иметь минимальный достоверный уровень надежности (SIL — 1) или аналогичный (см. A.3.2 приложение A).

Системы управления машиной, связанные с функцией безопасности, должны удовлетворять нижеследующим дополнительным требованиям в соответствии с оценкой риска.

5.2 Предотвращение отказов и управление отказами

5.2.1 Как руководство для мероприятий и алгоритмов предотвращения и управления ошибками применяют IEC 61508-2:2000, приложения A и B, или другие соизмеримые методы.

5.2.2 Отказы системы, связанной с безопасностью, по существу, различают согласно времени их происхождения:

a) отказы, вызванные ошибками, возникшими до или во время установки системы, например, ошибки программного обеспечения, включающие ошибки в исходных данных и в программе, аппаратные ошибки, включающие производственные ошибки и неправильный выбор компонентов;

b) Отказы, вызванные человеческим фактором и ошибками, происходящими в течение срока службы /работы машины и, в целом, после установки системы (например, случайные отказы оборудования, сбои, вызванные неправильным использованием).

Ошибки, типа упомянутых в перечислении a) могут быть обнаружены, исправлены и предотвращены мероприятиями, проведенными на различных этапах срока службы (см. IEC 61508-2:2000, приложение B). Меры для предотвращения ошибок — главным образом, расчетный и аналитический методы.

Ошибками, типа упомянутых в перечислении b) можно управлять только во время нормального режима работы (см. IEC 61508-2:2000, приложение A). Мероприятия по управлению этими ошибками должны входить в концепцию безопасности.

Некоторые мероприятия и методы, данные в IEC 61508-2, особенно важны (см. приложения A и B), поэтому они должны быть использованы независимо от уровня достоверной надежности. Другие также должны быть использованы независимо от этого уровня. Объем работ, требуемый для осуществления этих мероприятий, должен быть выбран такой, чтобы была достигнута эффективность, тре-

буемая IEC 61508-2:2000, таблицы с B.1 по B.5 (низкая/средняя /высокая). Все другие мероприятия, в принципе, заменимы. Они могут быть заменены по отдельности или в сочетании с другими мерами.

5.3 Требования к программируемым электронным системам (PES)

Программное обеспечение должно быть разработано и утверждено в соответствии с надлежащими мероприятиями (см., например, IEC 61508-3:1998, приложение A или ISO 13849-1:2006).

Концепции, разработка методов и инструментальных средств для программируемых электронных систем (PES), используемых в системах управления машиной, должны быть задокументированы.

5.4 Сбои или отказы электронных компонентов, используемых в системе управления машиной

В зависимости от оценки риска, в случае сбоя или отказа электронных компонентов, используемых системами управления машины, должно быть достигнуто безопасное состояние. Чтобы достигнуть безопасного состояния может быть использовано снижение производительности системы или замещение функции(й) как часть концепции безопасности.

Безопасное состояние может быть достигнуто за счет автоматического переключения на замещающую функцию (см. рисунок 1). Если этот переход осуществляется автоматически, с помощью MCS, то должен быть какой-нибудь признак для оператора, типа сигнала, индикации или снижения производительности (например, замедление движения).

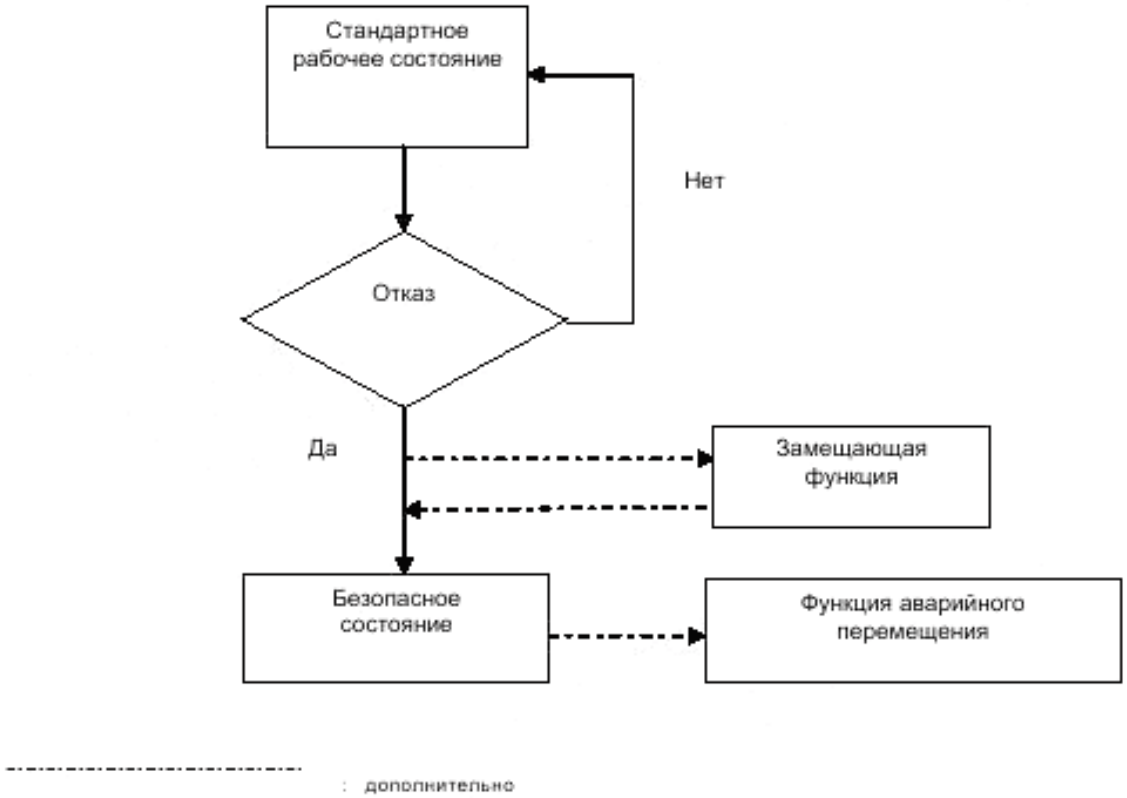


Рисунок 1 – Пример ввода в безопасное состояние

5.5 Процедура перезапуска

В случае ошибки, которая исчезает (подтверждается MCS), не должен быть разрешен автоматический перезапуск, если оценка риска доказывает, что может поддерживаться безопасный режим работы.

6 Документация

Изготовитель должен сохранять, согласно своим правилам регистрации и хранения, записи методик производителя, все документы, имеющие отношение к общим требованиям безопасности системы управления машиной в соответствии с разделом 4. Документация должна включать, по крайней мере, нижеследующее:

- описание системы управления машиной в соответствии с 4.2
- описание основных функций в соответствии с 4.3;
- анализ и оценку рисков в соответствии с 4.4;
- требования к концепции безопасности в соответствии с 4.5 (включая блок-схему с функциональным описанием каждого блока, принципиальную схему внешних соединений, описание внешних сигналов);
- совокупность тестовых данных и результаты испытаний, надлежащим образом проверяющие все возможные неисправности.

Документация, показывающая каким образом была сделана проверка правильности логики системы на стадии разработки (см. пункт 4.5), должна включать:

- блок-схему с функциональным описанием каждого блока, и;
- принципиальную схему внешних соединений и описание внешних сигналов.

Подтверждение правильности концепции безопасности систем управления машиной в соответствии с разделом 5 основывается на детальной документации тех частей системы, которые связанны с безопасностью. Это может быть в форме:

- принципиальных схем для внутренних электронных схем с описанием отдельных блоков и компонентов;
- функционального описания принципиальной схемы;
- перечня частей, включая идентификацию и наименование отдельных позиций, номинальных значений и допустимых отклонений;
- описания соответствующих нагрузок, наименования модели и изготовителя компонентов, листов технических данных специальных и ответственных компонентов; и
- видов отказов и анализа последствий отказа.

7 Испытания MCS, связанные с безопасностью

7.1 Общие требования

Для MCS рекомендуются испытания, указанные в 7.2, предназначенные для удовлетворения общим требованиям в соответствии с разделом 4, тем не менее альтернативные методы подтверждения также разрешены. Испытания могут быть выполнены на уровне системных единиц MCS поочередно (например, сборочных узлов). Проверка должна показать, что MCS работает как предназначено указанными режимами эксплуатации машины (техническими требованиями на проектирование).

7.2 Испытания систем управления машиной

7.2.1 Содержание испытания

Проводятся следующие испытания:

a) проверка основных функций (см. функции и описание системы в соответствии с 4.2 и описание основных функций в соответствии с 4.3);

b) испытание ввода в безопасное состояние (см. 5.4);

c) функциональные испытания на температуру и влажность в соответствии с 4.6.2 и 7.2.2;

d) испытания на электромагнитную совместимость в соответствии с 4.6.4;

e) испытание на удар и вибрацию в соответствии с 4.6.5, 7.2.3 и 7.2.4.

7.2.2 Климатические испытания на функционирование при температуре и влажности окружающей среды

Все функциональные возможности компонентов системы управления машиной, связанные с безопасностью, должны быть проверены на соответствие эксплуатационным требованиям 4.6.2 в соответствии с техническими условиями изготовителя или правилами IEC 60068-2-14, при следующих условиях окружающей среды:

- температура окружающей среды — от минус 25 °С;

- температура окружающей среды — до плюс 70 °С;
- относительная влажность — от 30 %;
- относительная влажность — до 95 %.

Приращение температуры должно составлять 1°С за 3 мин. Требуется два цикла температурных испытаний.

Максимальное номинальное напряжение должно быть выбрано во время нагревания до максимальной температуры окружающей среды, а минимальное номинальное напряжение должно быть выбрано при самой низкой температуре окружающей среды.

Испытательная нагрузка при максимальной температуре окружающей среды должна составлять 3/4, а также должен быть максимальный уровень нагрузки для каждого одночасового цикла. В ходе этих испытаний должны быть проверены все функции системы.

7.2.3 Вибрационные испытания

7.2.3.1. Компоненты MCS должны быть испытаны в той же самой позиции и с тем же способом крепления, который применяют на машине.

7.2.3.2. Испытания должны быть проведены в соответствии с IEC 60068-2-6 по синусоидальной кривой или в соответствии с техническими условиями изготовителя, таким образом, чтобы выполнялись особые условия 4.6.2, 4.6.3 и 4.6.5.

Соотношение между амплитудой и ускорением приведены в таблице 1.

Таблица 1

Частота	Моторный отсек	Все остальные места
$f < fT$	амплитуда ± 21 мм	амплитуда ± 15 мм
$f \geq fT$	ускорение 70 м/с2 (7g)	ускорение = 50 м/с2 (5g)
	амплитуда < ± 21 мм	амплитуда < ± 15 мм

Частотный диапазон f: от 5 до 200 Гц;
частота перехода (fT): от 8 Гц до 9 Гц;
количество циклов частоты: 20 ;
частота развертки: 1 октава/мин.

Допускают прерывание частотных циклов. Испытания должны быть проведены по взаимно перпендикулярным осям, причем одна из осей должна совпадать с продольной осью машины.

7.2.3.3 Испытательный образец должен быть запитан номинальным напряжением и в ходе процедуры испытаний должен быть проверен на функционирование. Не должно быть никакой потери функции безопасности.

7.2.3.4 Не должно наблюдаться никаких трещин или деформаций и после испытания, вся MCS в целом должна быть работоспособна.

7.2.4 Испытание на удары

Ударные испытания должны быть выполнены либо в соответствии с техническими условиями изготовителя или с правилами IEC 60068-2-27.

Испытуемый образец должен быть установлен на испытательном оборудовании с тем же креплением, как и на машине. Усилие затяжки должно быть в соответствии с указаниями изготовителя машины. Минимальная ударная нагрузка должна быть в соответствии с техническими условиями изготовителя (например, ускорение 150 м/с^2 (15 g) с 11 мс длительностью импульса, или, предпочтительно, 300 м/с2 (30 g) с 18 мс длительностью импульса).

7.2.5 Дополнительные функциональные тесты для безопасности системы управления машиной

Все системы управления машиной, связанные с безопасностью, должны быть испытаны в соответствии с разделом 5 со следующим дополнением.

Должны быть проведены основные функциональные испытания, например, в соответствии с IEC 61508-7:2000, B.5.1 и расширенные функциональные испытания, например, в соответствии с IEC 61508-7:2000, B.6.8.

Примечание — Для проверки допускаются альтернативные мероприятия приведенные в настоящем стандарте, кроме указанных в IEC 61508.

Приложение А
(справочное)

Руководство по оценке риска

А.1 Общие требования

Оценка риска имеет отношение к каждой опасной ситуации при применении машины. Рекомендуется, чтобы группа экспертов проанализировала все опасности с двух точек зрения:

a) опасность для оператора машины;

b) опасность для окружающих людей.

Метод, описанный в настоящем приложении, поддерживает выбор достоверного уровня безопасности для соответствующей функции безопасности (см. графы риска, показанные на рисунках А.1 и А.2). Для получения подробной информации по оценке рисков, см. ISO 14121-1, IEC 61508-5 или иные аналогичные методологии оценки риска.

В А.2 описан метод граф риска; это качественный метод, который позволяет определить достоверный уровень безопасности MCS по известным факторам риска. Это качественный подход использует множество параметров, которые совместно описывают характер опасной ситуации, когда система дает сбой или не отвечает. Один параметр выбирают из четырех групп (см. таблицу А.1), затем выбранные параметры объединяют для определения достоверного уровня безопасности размещенной системы.

А.2 Использование граф риска

Определение параметров риска осуществляют без анализа конкретных особенностей безопасности, интегрированной в MSC. Объяснение граф риска, показанных на рисунках А.1 и А.2, приведено ниже:

- использование параметров риска *C*, *F* и *P*, как это определено в таблице А.1, приводит к ряду выводов. Каждый из этих выводов отображают на одной из трех шкал (W_1, W_2 и W_3). Каждая точка на этих шкалах — признак необходимой достоверной безопасности, которая должна быть решена с помощью рассмотрения MCS;

- отображение на W_1, W_2 или W_3, как определено в таблице А.1, позволяет использовать другие мероприятия снижения риска. Разделение признаков по шкалам на W_1, W_2 и W_3 должно учитывать три разных уровня снижения риска другими мероприятиями. То есть, шкала W_3 обеспечивает минимальное снижение риска, внесенное с помощью других мероприятий (то есть имеет место самая высокая вероятность нежелательного возникновения), шкала W_2 обеспечивает среднее снижение, и шкала W_1 обеспечивает максимальное снижение. Для конкретных промежуточных выводов в графах риска (после того, как использовали параметры риска *C*, *F* и *P*) и для конкретных шкал *W* (то есть W_1, W_2 или W_3) окончательный вывод графы риска дает уровень достоверной безопасности MCS (то есть 1, 2, 3 или 4) и является мерой необходимого снижения риска для этой системы. Это снижение риска, вместе со снижениями риска, достигнутыми другими мерами (например, с помощью другой технологии, связанной с безопасностью системы, и другими внешними средствами для снижения риска), которые расчитываются по алгоритму *W*, дает необходимое снижение риска для определенной ситуации.

Таблица А.1 — Пример данных имеющих отношение к графе риска (см. рисунки А.1 и А.2)

Параметры риска		Классификация	Комментарии
Результат (C)	C1	Незначительные травмы	Для объяснения C1, C2, C3 и C4 должны быть приняты во внимания последствия несчастного случая и нормального исцеления
	C2	Серьезные увечья одного или более лиц; смерть одного человека	
	C3	Смерть нескольких человек	
	C4	Большое количество погибших	

Окончание таблицы А.1

Параметры риска		Классификация	Комментарии
Частота и время воздействия в опасной зоне (F)	F1	Воздействие от редкого до частого.	
	F2	Воздействие от частого до постоянного.	
Возможность избежания опасного события (P)	P1	Возможность при некоторых условиях	Этот параметр принимает во внимание: - управление процессом [контролируемый (то есть управляемый квалифицированными или людьми низкой квалификации) или неконтролируемый]; - темп развития опасного случая (например, внезапно, быстро или медленно); - легкость распознавания опасности (например, замеченная немедленно, обнаруженная техническими мерами или обнаруженная без технических мер); - предотвращение опасного случая (например, возможность эвакуации, не возможность эвакуации, или возможность эвакуации при определенных условиях); и - фактический опыт безопасности (такой опыт может существовать с идентичными MCS или подобными MCS или может не существовать)
	P2	Почти невозможно	
Вероятность нежелательного события (W)	W1	Очень небольшая вероятность, что нежелательные события случатся и вероятно только несколько нежелательных событий	Цель фактора W состоит в том, чтобы оценить частоту нежелательного возникновения, имеющего место без дополнения любых MCS, включая любые внешние средства для снижения риска. Если отсутствует опыт построения MCS или подобных систем, а также, если этот опыт минимален, оценка фактора W может быть сделана расчетным путем. В таком случае должно быть произведено прогнозирование худшего случая
	W2	Небольшая вероятность, что нежелательные события случатся и вероятно немного нежелательных событий	
	W3	Сравнительно высокая вероятность, что нежелательные события случатся и вероятны частые нежелательные события	

А.3 Пример анализа риска электронного управления переключением передач

А.3.1 Идентификация опасностей и распределения параметров риска

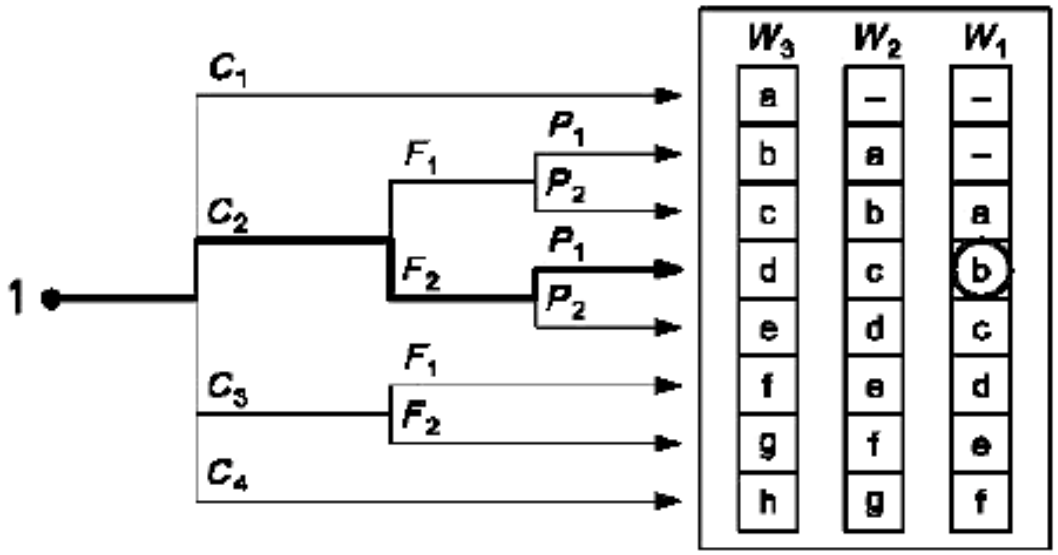
Это может быть внесение в соответствующий перечень всех рассмотренных опасностей. Таблице А.2 показывает пример идентификации опасностей и распределения параметров риска при использовании электронного управления переключением передач.

Таблица А.2 — Пример идентификации опасности и распределения параметра риска

Опасность для оператора	C	F	P	W
Неожиданное понижение передачи в случае сбоя, например, с четвертой на первую передачу	C2 Оператор мог быть серьезно ранен при внезапно уменьшеной скорости	F2 Оператор постоянно не защищен от воздействия	P1 Оператор может использовать ремень безопасности	W1 Опыт показывает, что вероятность таких случаев может быть оценена как W1
Неожиданный запуск (при неподвижном состоянии) в случае сбоя	C2 В худшем случае оборудование переместится в опасную область (столкновение или рывок)	F2 Оператор постоянно не защищен	P1 Оператор может использовать тормоз	W1 Опыт показывает, что вероятность таких случаев может быть оценена как W1
Опасность для других людей				
Неожиданное понижение передачи в случае сбоя, например, с четвертой на первую передачу, на стройплощадке	Отсутствие ожидаемых опасностей			
Неожиданное понижение передачи в случае сбоя, например, с четвертой на первую передачу, при передвижении по дорогам общего пользования	C2 Возможность столкновения при внезапной остановке машины	F1 Ограничение передвижения по дорогам общего пользования	P1 Возможность использовать тормоза или уклонение от других транспортныхсредств	W1 Опыт показывает, что вероятность таких инцидентов может быть оценена как W1
Неожиданный запуск (при неподвижном состоянии) в случае сбоя на стройплощадке	C2 Возможность серьезной травмы других людей	F1 В общем, машины используют для перемещения так, чтобы другие люди не находились вне пределов рабочей зоны	P1 Люди могут отклониться (при низкой скорости)	W1 Опыт показывает, что вероятность таких инцидентов может быть оценена как W1
Неожиданный запуск (при неподвижном состоянии) в случае сбоя при передвижении по дорогам общего пользования	C2 Возможность серьезной травмы других людей	F1 Ограничение передвижения по дорогам общего пользования	P1 Люди могут отклониться (низкая скорость)	W1 Опыт показывает, что вероятность таких инцидентов может быть оценена как W1
Примечание — Эта таблица представляет собой только пример. Оцениваемые параметры риска должны быть адаптированы для каждой отдельной MCS. Опасности описаны не в полной мере, и необходимо рассмотреть дополнительные опасности и ситуации.				

А.3.2 Анализ риска

Использование оцениваемых параметров риска в качестве входных данных для граф риска, показанных на рисунках А.1 и А.2, дает достоверный уровень безопасности (SIL) — 1 в примере, показанном на рисунке А.1, где анализируется опасность для оператора; а в примере, показанном на рисунке А.2, где анализируется опасность для других людей, ни один достоверный уровень безопасности (SIL) не достигается.



Требуемое минимальное снижение риска	Степень эффективности (PL) в соответствии с ISO 13849-1	SIL
—	—	Нет нормативов безопасности
a	a	Нет специальных нормативов безопасности
b, c	b, c	1
d	d	2
e, f	e	3
g		4
h		Недостаточно MCS

1 — отправная точка для оценки риска; *C* — параметр последствий риска; *F* — параметры частоты и время подверженности риску; *P* — параметры возможности избегания риска; *W* — вероятность возникновения нежелательных случаев; от a до h — оценки необходимого снижения риска для MCS

Последствия:

частота и длительность:

возможность избегания опасного события:

вероятность избегания нежелательного события:

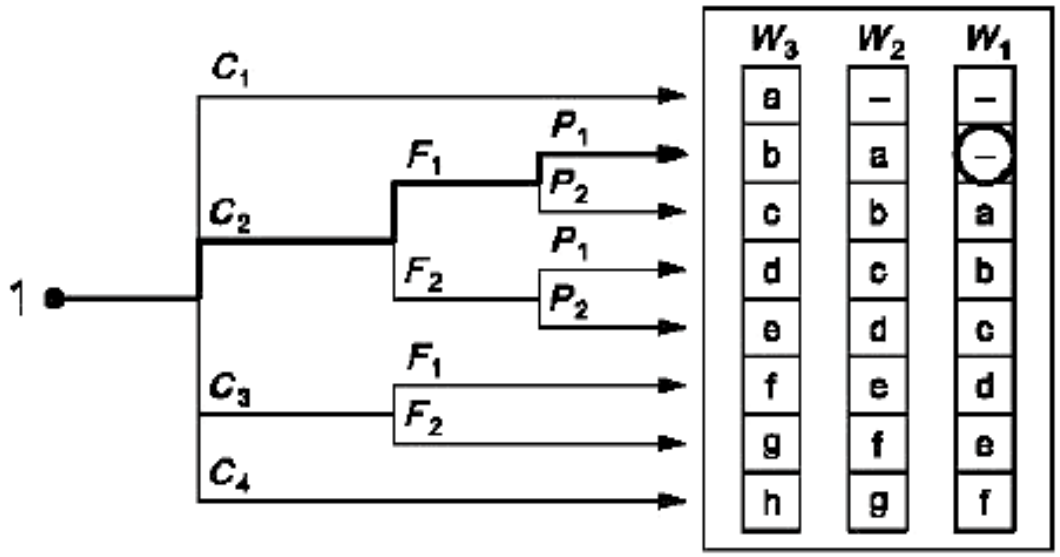
C_2 (серьезные долговременные травмы одного или нескольких лиц, смерть человека);

F_2 (частота долговременного нахождения в опасной зоне);

P_1 (возможно при некоторых условиях);

W_1 (очень небольшая вероятность нежелательных событий и вероятность нескольких нежелательных событий)

Рисунок А.1 — Графа риска — Риск для оператора



Необходимое минимальное снижение риска	SIL
—	Нет нормативов безопасности
a	Нет специальных нормативов безопасности
b, c	1
d	2
e, f	3
g	4
h	Недостаточно MCS

1 — отправная точка для оценки риска; *C* — параметр последствий риска; *F* — параметры частоты и время подверженности риску; *P* — параметры возможности избегания риска; *W* — вероятность возникновения нежелательных случаев; от a до h — оценки необходимого снижения риска для MCS

Последствия: C_2 (серьезные долговременные травмы одного или нескольких лиц, смерть человека);

частота и длительность: F_2 (частота долговременного нахождения в опасной зоне);

возможность избегания опасного события: P_1 (возможно при некоторых условиях);

вероятность избегания нежелательного события: W_1 (очень небольшая вероятность нежелательных событий и вероятность нескольких нежелательных событий)

Рисунок А.2 — Графа риска — Риск для других людей

А.3.3 Заключение

Оба исследования риска приводят к заключению, что переключение передач в трансмиссии должно быть спроектировано в соответствии с достоверным уровнем безопасности SIL –1.

Приложение В
(справочное)

Схематичный пример содержания технических условий для систем

№	Наименование
1	Функциональные требования
1.1	Внешние интерфейсы
1.2	Интерфейс «человек-машина»
1.3	Рабочий режим
1.4	Системные функции
2	Требования техники безопасности
2.1	Зарегистрированные руководства и правила безопасности
2.2	Ошибки и отказы, которые следует учитывать
2.3	Ответные действия на ошибки и отказы (включая временной режим)
2.4	Процедура перезапуска
2.5	Предельные уровни безопасности и функциональной надежности
2.6	Специальные меры для обеспечения требуемой отказоустойчивости
2.7	Организационные меры для защиты от внешних воздействий
3	Условия окружающей среды, которые должны быть учтены
3.1	Виды условий окружающей среды
3.2	Допустимые предельные значения
3.3	Реакция системы на отдельные условия окружающей среды
4	Требования к проектированию
4.1	Специальные технические условия на проектирование и изготовление
4.2	Используемые компоненты
4.3	Ответственый персонал
4.4	Используемые средства производства и материалы
4.5	Используемые соединительные устройства
5	Отдельные рабочие режимы и техническое обслуживание
5.1	Необходимые устройства и интерфейсы для тестирования и обслуживания
5.2	Общие технические условия для установки
5.3	Общие организационные условия для эксплуатации и технического обслуживания
5.4	Требования к приемочным испытаниям и контроль за серийной продукцией

Приложение С
(справочное)

Перечень проверенных компонентов

С.1 Общие требования

Проверенные принципиальные подходы к безопасности, например:

- предотвращение некоторых неисправностей, таких как короткое замыкание, например, разделением схем;
- снижение вероятности дефектов, например, уточнением допусков или переоценкой компонентов;
- выбор метода устранения неисправности, например, путем обеспечения размыкания цепи, когда жизненно важно обесточивание в случае повреждения;
- раннее обнаружение дефектов; и
- ограничение последствий неисправностей, например, путем заземления оборудования.

Недавно разработанные компоненты и принципы безопасности могут быть рассмотрены как эквивалентные проверенным компонентам, если они удовлетворяют вышеупомянутым условиям.

Проверенные компоненты, применяемые в некоторых случаях, для других случаев могут не соответствовать.

Таблицы С.1 и С.2 являются примерами и должны быть проверены проектировщиком на применимость.

С .2 Механические части и компоненты

Таблица С.1

Проверенные компоненты	Условия для статуса «проверенные»	Стандарт или технические характеристики
Винт	Должны быть рассмотрены все факторы, влияющие на соединительный винт и его применение	Механические соединяющие элементы, типа винтов, гаек, шайб, заклепок, шплинтов, болтов и т.д. должны быть стандартизированы
Пружина	См. использование проверенной пружины описанное в ISO 13849-2:2003, таблица А.2	Технические характеристики для пружинных сталей и других специальных применений даны в ISO 4960
Эксцентрик	Следует рассмотреть все факторы, влияющие на установку эксцентрика (например, часть блокировочного устройства)	См. ISO 14119 (блокировочные устройства)
Шплинт	Следует рассмотреть все факторы, влияющие на применение	—
Тяга управления	Следует рассмотреть все факторы, влияющие на применение	—
Подъемная стрела	Следует рассмотреть все факторы, влияющие на применение	—

С.3 Гидравлические части / компоненты

- гидравлические цилиндры;
- трубопроводы, рукава;
- основные регулирующие клапана.

С.4 Электронные компоненты

Таблица С.2

Испытанные компоненты	Условия для статуса «испытан»	Стандарт или спецификация
Выключатель с принудительным приведением в действие (включение непосредственным воздействием), например: - кнопка; - переключатель; - управляемый эксцентриком многопозиционный переключатель, например, для выбора режима	—	IEC 60947-5-1:2003, приложение K
Устройство аварийного останова	—	ISO 13850
Плавкий предохранитель	—	IEC 60269-1
Автоматический выключатель	—	IEC 60947-2
Дифференциальный автоматический выключатель/RCD (при обнаружении тока утечки)	—	IEC 60947-2:2006, Приложение B
Сетевой выключатель	Только если a) рассмотрены другие различные факторы, такие как вибрация, и в) неисправности предотвращают соответствующими методами, например, уменьшением допусков (см. ISO 13849-2:2003, таблица D.2); и c) токовая нагрузка, ограничена тепловым защитным устройством, и d) цепи защищены устройством защиты от перегрузок	ISO 13849-2
Устройство (или оборудование) управления и защитного отключения (CPS)	—	IEC 60947-6-2
Дополнительный выключатель (например, релейный выключатель)	Только если: a) рассмотрены другие различные факторы, такие как вибрация; в) явно усиливается действие; c) неисправности предотвращаются соответствующими методами, например, уменьшением допусков (см. ISO 13849-2:2003, таблица D.2); d) ток в контактах ограничен плавким предохранителем или автоматическим выключателем, чтобы предотвратить свариваемость контактов; e) контакты управляются механически напрямую, когда они используются для текущего контроля.	EH 50205 IEC 60204-1:1997, 5.3.2 и 9.3.3 IEC 60947-5-1
Трансформатор	—	IEC 61558-1

Окончание таблицы С.2

Испытанные компоненты	Условия для статуса «испытан»	Стандарт или спецификация
Кабель	Оболочки внешней кабельной разводки должны быть защищены от механических повреждений (включая, например, повреждения от вибрации или изгиба)	IEC 60204-1:1997, раздел 13
Штепсельные разъемы и контактные гнезда	—	В соответствии с стандартом на электрооборудование. Для блокировочных устройств, см. также ISO 14119
Температурное реле	—	С точки зрения электрики см. IEC 60947-5-1:2003, приложение К
Реле давления	—	С точки зрения электрики см. IEC 60947-5-1:2003, приложение К. С точки зрения давления см. ISO 13849-2:2003, приложения В и С
Электромагнитный клапан	—	Европейские или Международные стандарты отсутствуют

Приложение D
(справочное)

Рекомендации для магистральных систем передачи, связанные с безопасностью сообщений

D.1 Область применения

Настоящие приложение дает рекомендации для передачи связанных с безопасностью сообщений, используемых в MCS. Связь может иметь место между различными системными единицами MCS и/или между интеллектуальными датчиками/ действующими субъектами и системными единицами MCS.

Примечание 1 — На данный момент рассматривают только те закрытые (инкапсулированные) магистральные системы, в которых изготовитель определил число и тип участников (то есть единиц, связанных магистралью). Расширение этой системы для дальнейшей передачи данных здесь не рассматривают. Внутренние данные и адресные шины исключены из области применения.

Примечание 2 — Используемой магистральной системой может быть система по протоколу SAE J 1939 и со стандартными компонентами для передачи (см. модели в D.3).

D.2 Термины и определения

Для настоящего приложения применяются нижеследующие термины с соответствующими определениями:

D.2.1 **магистральная система** (bus system): Система для передачи связанных с безопасностью сообщений, состоящая, в дополнение к системным единицам (источникам и приемникам информации), из каналов передачи/средств передачи (например, электрических линий, оптоволоконных линий, RF — передачи) и устройств сопряжения между источником сообщения/приемником и электроникой магистрали (протокол ASICs, приемопередатчики и т.д.)

См. Рисунок D.1.

Примечание — Для дистанционного управления, см. ISO 15817.

D.2.2 **инкапсулированная магистральная система** (encapsulated bus system): Инкапсулированная система, состоящая из фиксированного числа или установленного максимального числа магистральных участников, связанных друг с другом через средства передачи с четко определенными и установленными рабочими/эксплуатационными характеристиками.

D.2.3 **источник сообщений** (message source), **отправитель сообщений** (message sender): **Отправитель сообщений** связанных с безопасностью.

D.2.4 **приемник сообщений** (message sink), **получатель сообщений** (message receiver): Приемник сообщений связанных с безопасностью.

D.2.5 **сообщение** (message): Сообщение, содержащее пользовательские данные, адреса и данные для обеспечения достоверности передачи и т.д.

D.2.6 **максимальный размер расширения** (maximum extension size): Максимальное допустимое число отправителей и получателей, которые заняты обменом сообщений, определяемых системой.

D.2.7 **длительность безопасного процесса** (process safety time): Промежуток времени между отказом, произошедшим в MCS, и возникновением опасного события, если функция безопасности не выполнена.

D.2.8 **время реагирования электроники** (electrical reaction time): Промежуток времени от «электронного» обнаружения события, связанного с безопасностью, до начала «электронного» реагирования.

Примечание — Время реагирования электроники состоит из нескольких единичных отрезков, например, времени передачи шиной.

D.2.9 Ошибка передачи

D.2.9.1 **повторение** (repetition): Ошибка из-за ошибки магистрального участника, в связи с чем, предыдущие, старые сообщения повторяются в некорректный момент времени, в результате чего происходят опасные для получателя искажения (например, сигнал "закрыта дверца люка", когда она уже открыта).

D.2.9.2 **срыв** (loss): Непреднамеренное удаление сообщения (например, запроса безопасного останова) из-за ошибки магистрального участника.

D.2.9.3 **вставка** (insertion): Непреднамеренное введение (например, отмена безопасного останова) из-за ошибки магистрального участника.

D.2.9.4 **некорректная последовательность** (incorrect sequence): Непреднамеренное изменение очередности сообщений из-за ошибки магистрального участника.

Примеры — Правильная последовательность: перед приведением в безопасный останов выбирается уменьшенная скорость.

Некорректная последовательность: немедленный безопасный останов, а затем выбор пониженной скорости.

Последствия: машина продолжает движение вместо того, чтобы оставаться в режиме безопасного останова.

Примечание — Магистральные системы могут содержать элементы хранящегося блока данных для срочной передачи (FIFO и т.д.), которые могут изменить правильную последовательность.

D.2.9.5 фальсификация сообщения (message falsification): Непреднамеренное искажение сообщений из-за ошибки магистрального участника или из-за ошибок в канале передачи.

D.2.9.6 замедление (retardation): Непреднамеренное замедление или задержка функции безопасности из-за перегрузки канала передачи при стандартном обмене данными или в случае перегрузки магистрального участника, отправившего некорректные сообщения.

D.2.9.7 объединение связанных и несвязанных с безопасностью сообщений (coupling of safety-related and non-safety-related messages): Непреднамеренное распознавание несвязанного с безопасностью сообщения как возможно связанного с безопасностью сообщения.

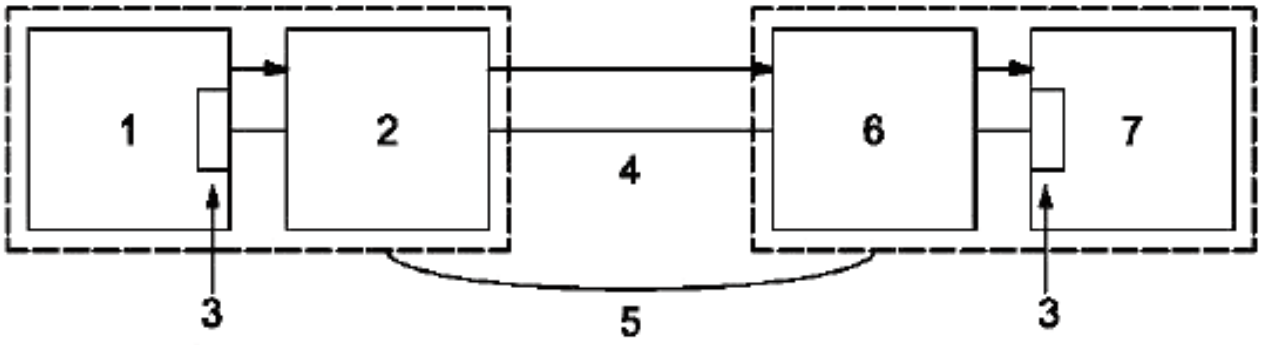
D.3 Модели и описания

D.3.1 Общие требования

Для целей настоящего приложения нижеследующие модели описывают некоторые функции магистральной системы или конфигурацию магистральной системы.

D.3.2 Модель магистральной системы

Рисунок D.1 показывает модель для магистральной системы.

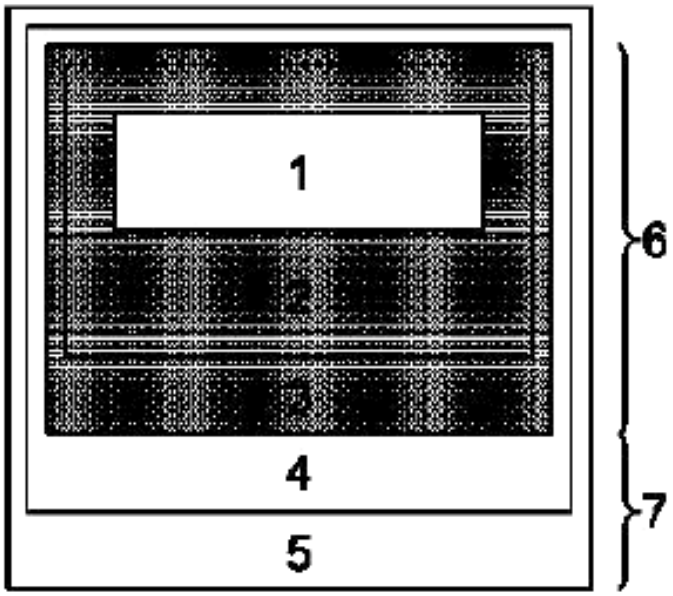


1 — источник сообщения; *2* — магистральный отправитель; *3* — помехи; *4* — канал передачи; *5* — магистраль; *6* — магистральный получатель; *7* — приемник сообщений

Рисунок D.1 — Базисная модель магистральной системы

D.3.3 Модель для передачи сообщений, связанных с безопасностью (в соответствии с OSI)

Рисунок D.2. показывает модель для передачи сообщений, связанных с безопасностью.



1 — данные прикладной программы схемы безопасности; 2 — процедуры безопасности, например, идентификация; 3 — кодирование достоверности, например, CRC; 4 — протокол передачи; 5 — код передачи (блок данных для срочной передачи); 6 — уровни безопасности; 7 — передающие уровни

Рисунок D.2 — OSI модель для передачи связанных с безопасностью сообщений

Уровни безопасности содержат процедуры безопасности и кодирования достоверности. Передающие уровни содержат протокол передачи и код передачи.

В безопасных уровнях связанные с безопасностью пользовательские данные должны быть добавлены к безопасным процедурам с кодированием достоверности (например, CRC) и быть переданы уровнями передачи.

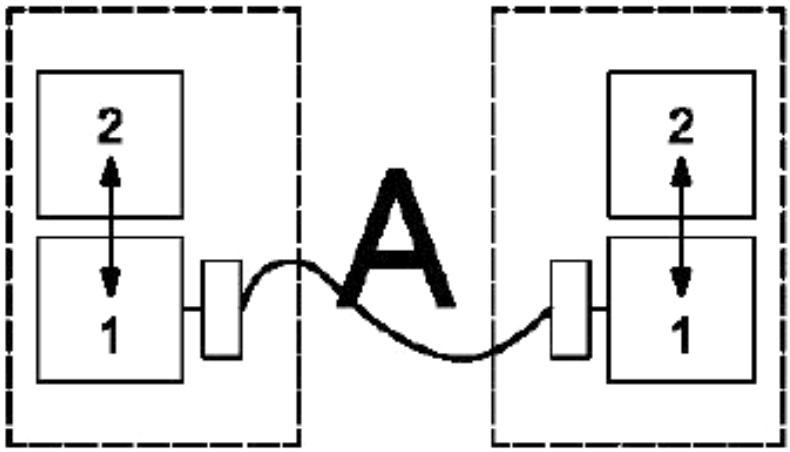
D.3.4 Конфигурация магистральных систем

D.3.4.1 Общие требования

Возможны различные конфигурации магистральных систем. Нижеследующие модели от A до D описывают типичные конфигурацию системы. Они частично отличаются по их отказоустойчивости. Также описаны основные преимущества и недостатки.

D.3.4.2 Модель A: одноканальная система

Система, изображенная на рисунке D.3, служит в качестве рекомендованного образца для других моделей. Подключение к магистральной шине имеет только один канал (канал 1).Сообщения из канала 2, который не подключен к шине, сохраняются и передаются в канал 1, который подключен к шине.

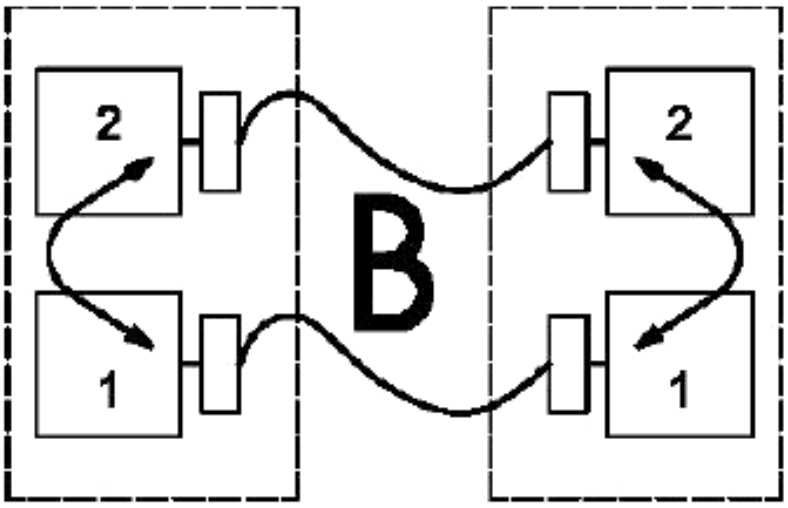


1 — канал 1; *2* — канал 2

Рисунок D.3 — Конфигурация модели А

D.3.4.3 Модель В

Рисунок D.4 показывает систему с резервированием. В этом случае все уровни безопасности и передающие уровни продублированы.

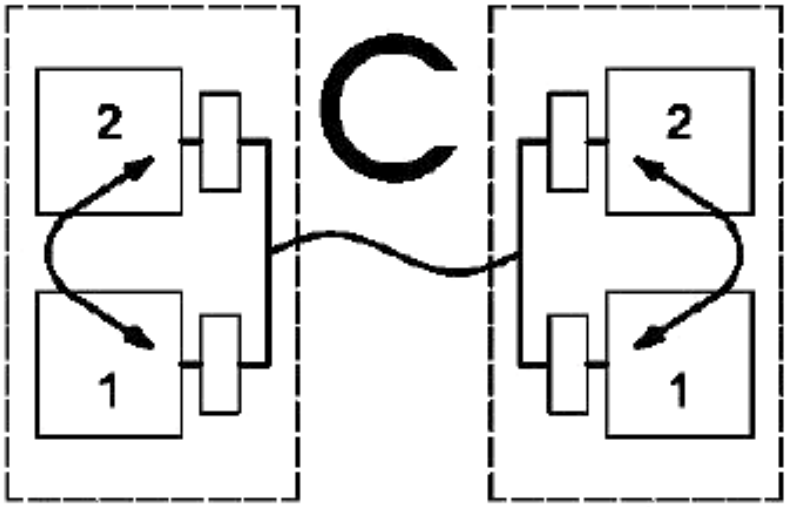


1 — канал 1; *2* — канал 2

Рисунок D.4 — Конфигурация модели В

D.3.4.4 Модель C

Рисунок D.5 показывает модель, сопоставимую с моделью B, но средство передачи имеет только один канал.

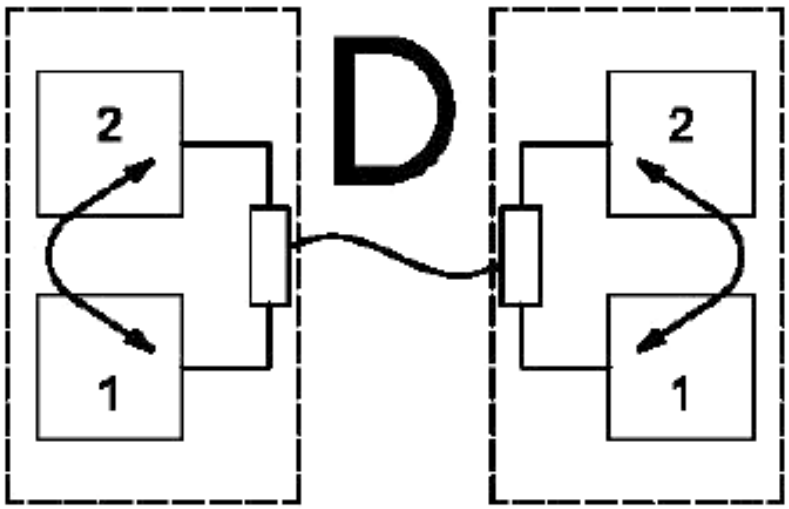


1 — канал 1; *2* — канал 2

Рисунок D.5 — Конфигурация модели C

D.3.4.5 Модель D

Рисунок D.6 показывает систему с двумя каналами для уровней безопасности, в то время как передающий уровень имеет один канал. Оба уровня безопасности имеют независимый доступ к передающему уровню. Пользовательские данные могут быть переданы одним или двумя блоками данных для срочной передачи.



1 — канал 1; 2 — канал 2

Рисунок D.6 — Конфигурация модели D

D.4 Описание способов контроля за ошибками передачи

D.4.1 Общие требования

Этот раздел перечисляет способы контроля за ошибками передачи.

D.4.2 Порядковый номер

Порядковый номер добавляют к каждому сообщению, которыми обмениваются отправитель и получатель. Этот порядковый номер может быть определен как дополнительное поле данных, содержащее номер, который меняется определенным способом от предыдущего сообщения к следующему.

D.4.3 Метка времени

Содержание сообщения, как правило, действительно в данный момент времени. Метку времени (например, дата и время) добавляют к сообщению, переданному отправителем. Метки времени разделяют на относительную метку времени, абсолютную метку времени и двойную метку времени.

D.4.4 Время истечения срока (время простоя)

В течение передачи сообщения получатель проверяет, превышает ли время задержки между двумя сообщениями определенное значение. В этом случае ошибка фиксируется.

D.4.5 Подтверждение приема/эхо-сигнал

Приемник сообщения посылает сообщение (эхо-сигнал) о содержании первоначально полученного сообщения обратно к источнику. Например, в подтверждение приема можно повторить полученные надлежащим образом данные, чтобы отправитель имел возможность проверять правильность приема.

Примечание — Некоторые магистральные системы используют термины "подтверждение приема", "эхо-сигнал" и "подтверждение получения" как синонимы.

D.4.6 Идентификация отправителя и получателя

Сообщения могут содержать идентификацию унифицированного отправителя и/или получателя, определяющую логический адрес связанного с безопасностью участника.

D.4.7 Дублирование с текущим перекрестным контролем

Отправитель и получатель имеют завершенную двухканальную структуру, см. модели B и C. Эти сообщения передаются самостоятельно дважды. В дополнение к этому передаваемые сообщения перекрестно проверяются по магистрали или по отдельной связи внутри сдвоенной единицы канала отправителя/получателя для надежности операции.

Если имеется разница, то она должна быть рассмотрена как ошибка во время передачи в единице обработки отправителя или в устройстве обработки данных получателя. Если используются резервные средства, это должно быть рассматриваться как случай общего отказа (например, может происходить ошибка обнаружения случая общего отказа из-за различий в избыточной структуре).

D.4.8 Различия обеспечения достоверности данных, связанных с безопасностью (SR) и не связанных с безопасностью (NSR)

Если, связанные с безопасностью (SR) и не связанные с безопасностью (NSR) данные передаются через ту же самую магистраль (шину), может использоваться различное обеспечение достоверности данных или принципы кодирования (различные CRC алгоритмы, различные образующие полиномы) для того, чтобы гарантировать, что NSR сообщения не могут влиять на любую функцию безопасности в получателе.

Примечание — Различие обеспечения достоверности данных также означает, что NSR сообщения не имеют обеспечения достоверности данных.

D.5 Рекомендации

D.5.1 Возможные способы управления ошибками передачи

D.5.1.1 Чтобы быть безопасно переданными, сообщения должны быть сформированы безопасным способом (см. 4.5). Средства передачи (например, магистральная линия, включающая интерфейс ASICs) непосредственно не расцениваются как достаточно безопасные. Механизм достоверности данных находится исключительно под ответственностью устройства обработки данных источника сообщения и приемника сообщения (см. рисунок D.7).

D.5.1.2 Должен быть использован механизм времени истечения срока.

D.5.1.3 Механизм обнаружения ошибок передачи и реагирования в случае отказа должен быть встроен в приемник и отвечать за запуск связанного с безопасностью реагирования в пределах длительности безопасного процесса.

D.5.1.4 В случае ошибок передачи, определенных в D.2.9, должно инициироваться соответствующее реагирование на ошибки (например, остановка запроса).

D.5.1.5 Длительность безопасного процесса в схеме безопасности, указанная изготовителем, и время, требуемое для начала связанного с безопасностью реагирования, не должно быть превышено даже в случае ошибки.

Примечание — В некоторых магистральных системах частота передачи и время безопасности процесса связаны с числом участников. Внимание: связанная с безопасностью частота передачи и время безопасности процесса могут ограничивать число участников.

D.5.1.6 Для передачи магистральной системой связанных с безопасностью сообщений должно быть выбрано, по крайней мере, одно мероприятие против каждой ошибки передачи (см. таблицу D.1). Реагирование должно быть основано на оценке степени риска.

D.5.1.7 Должно быть учтено влияние не связанных с безопасностью магистральных участников шины (любое электронное устройство, соединенное с магистралью) на связанных с безопасностью магистральных участников (например, посыланием многократных связанных с безопасностью сообщений).

D.5.2 Обеспечение достоверности данных

D.5.2.1Общие требования

Обеспечение достоверности данных — важная составляющая достижения требуемого SIL.

Все мероприятия для обеспечения достоверности данных должны быть выполнены контролирующими частями MCS, разработанными для удовлетворения требования 4.4. Коэффициент необнаруженных ошибок, Λ, должен быть вычислен от вероятности необнаружения ошибки, R(p), контролирующего связанного с безопасностью механизма обеспечения достоверности данных и скорости передачи связанных с безопасностью сообщений.

Следует использовать следующую формулу, чтобы вычислить коэффициент необнаруженных ошибок от вероятности необнаружения ошибки:

$\Lambda = 3\,600 \times R(p) \times V \times m \times 100$ (ошибки передачи/час),

где 3 600 –коэффициент, используемый для вычисления передачи в час;

v — требуемая частота (1/с) связанных с безопасностью сообщений, чтобы достигнуть необходимое время реагирования;

R (p) — вероятность необнаружения ошибки;

m — число сообщений, требуемых для выполнения функции безопасности.

Коэффициент 100 подтверждает, что передача составляет только 1 % (запас прочности) рекомендуемой достоверной безопасности. Это приводит к заключению, что передача является достаточно безопасной. В зависимости от оценки риска изготовитель может отступать от запаса прочности.

Для оценки R (p), основанной на информации изготовителя вероятность ошибки в символе должна быть принята как p = 0,01, пока не доказано другое.

Должно соответствовать:

Для SIL 3, $\Lambda < 10^{-7}$.

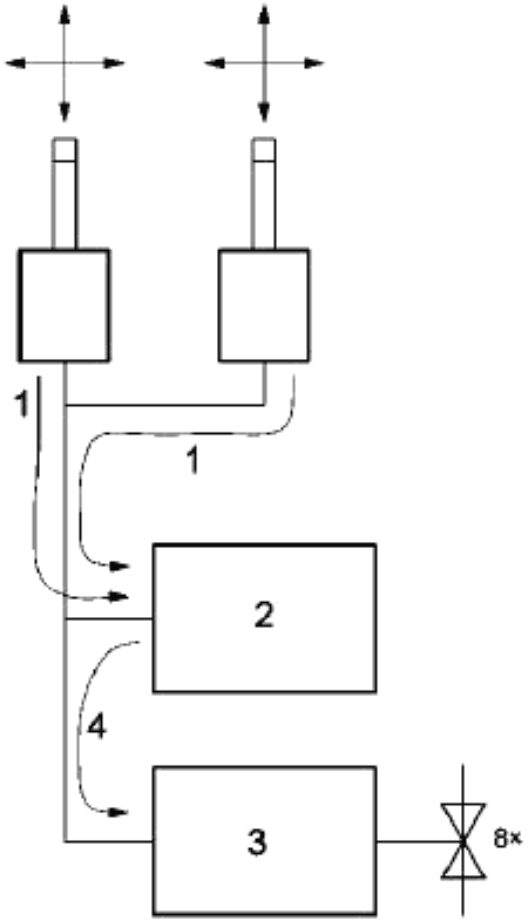
Для SIL 2, $\Lambda < 10^{-6}$.

Для SIL 1, $\Lambda < 10^{-5}$.

Примечание — Эти возможные коэффициенты необнаруженных ошибок приведены в IEC 61508 (вероятности опасных ошибок в час) и должны быть рассмотрены как примеры.

D.5.2.2 Пример вычисления коэффициента необнаруженных ошибок передачи связанных с безопасностью сообщений для магистральной системы (см. рисунок D.7).

Движение землеройных машин управляется двумя джойстиками. Для безопасной функции "безопасное движение" — требуется SIL 2. Информация относительно положений джойстиков передана магистральной системой к главному контроллеру (главное управление каналом связи), который оценивает сообщения и передает соответствующие команды управления на восемь гидравлических двигателей.



1 — два сообщения; *2* — главный контролер; *3* — управление гидравликой; *4* — восемь сообщений.

Рисунок D.7 — Пример связанной с безопасностью магистральной системы

Для вычисления коэффициента необнаруженных ошибок выдвигают следующие предположения:

a) каждое сообщение, которое будет передано, состоит из одного простого блока данных для срочной передачи;

b) каждый джойстик передает одно сообщение при перемещении джойстика по оси X и оси Y;

c) главный контроллер получает сообщения, оценивает выходную информацию и передает восемь сообщений на гидравлические двигатели для движения землеройной машины;

d) чтобы обеспечить требуемое электрическое время реагирования, обновление выходной информации для гидравлических двигателей имеет место каждые 100 мс. Это означает, что частота V передачи связанных с безопасностью сообщений должна быть 10/с;

e) схемное решение для преобразования связанных с безопасностью сообщений в системе управления не является частью этого рассмотрения. Принимается, что конструктивное исполнение выполняет соответствующие связанные с безопасностью рекомендации;

f) для передачи используется стандартная магистральная система с наихудшей вероятностью необнаружения ошибки — R (p) = 7×10-9. Принимается, что ошибка стандартизированной достоверной кодировки сообщений, осуществленная в интегральных микросхемах протокола, также распознается другими перехватывающими магистральными участниками, и указывается посылкой блока данных ошибки.

Для коэффициента необнаруженных ошибок сделан нижеследующий приблизительный расчет:

$\Lambda = 3\,600 \times R(p) \times v \times m \times 100$ (ошибки передачи/час);

$\Lambda = 3\,600 \times 7{\times}10\text{-}9{\times}\ 10\ (8 + 2 + 2) \times 100$ (ошибки передачи/час);

$\Lambda = 0{,}3$ (ошибки передачи/час);

$\Lambda > \Lambda$ треб, поэтому эта магистральная система не соответствует рекомендациям.

Для улучшения коэффициента необнаруженных ошибок приняты следующие мероприятия:

- каждое связанное с безопасностью сообщение, которое будет передано, состоит из двух магистральных блоков данных;

- каждая пара двух магистральных блоков данных проверяется на непротиворечивость магистральными участниками получения. Если распознается противоречивость, будет иметь место реагирование на ошибку.

Это означает, что отказ передачи возможен только при идентичных ошибках передачи в обоих сообщениях. Вероятность фальсификации одного сообщения определяется наихудшей вероятностью необнаружения ошибки стандартной магистральной системы.

В случае двух блоков данных, вероятность необнаружения ошибки R (p)обш определяется квадратом наихудшей вероятности необнаружения ошибки

R (p)обш. = R (p)2.

Эти предположения приводят к следующему:

$\Lambda = 3\,600 \times R(p) \times v \times m \times 100$ (ошибки передачи/час);

$\Lambda = 3\,600 \times (7 \times 10\text{-}9)2 \times 10 \times 12 \times 100$ (ошибки передачи/час);

$\Lambda = 2{,}1 \times 10\text{-}9$ (ошибки передачи/час);

$\Lambda > \Lambda$ треб=10-6, поэтому эта магистральная система соответствует рекомендациям.

Таблица D.1 — Эффективность различных мер в случае возможных ошибок передачи

Ошибки передачи	Мероприятия в сообщение							
	Порядковый номер, см. D.4.2	Отметка времени, см. D.4.3	Время истечения срока, см. D.4.4	Подтверждение приема, см. D.4.5	Идентификация отправителя и получателя, см. D.4.6	Обеспечение достоверности данных, см. D.4.8	Дублирование с двойной проверкой, см. D.4.7	Различие системы обеспечения достоверности данных SR и сообщений non-SR, см. D.4.8
Повторение, см. D.2.9.1	X	X					X	
Срыв, см. D.2.9.2	X			X			X	
Вставка см. D.2.9.3	X			X [a]	X [b]		X	
Некорректная последовательность, см. D.2.9.4	X	X					X	
Фальсификация сообщений, см. D.2.9.5				X		X	Только для последовательной шины [d]	
Замедление, см. D.2.9.6		X	X [c]					
Объединение SR и non-SR D 2.9.7				X [a]	X			X

a) Зависит от применения.

b) Только для идентификации отправителя. Обнаруживает только вставку недействительного источника.

c) Необходимый во всех случаях.

d) Эта мера только сопоставима с высококачественным механизмом гарантии данных, если вычислением можно доказать, что коэффициент необнаруженных ошибок Λ достигает показателей в соответствии с D.5.2, а также если два сообщения посылают через независимые приемопередатчики.

Библиография

ISO 4960:2007	Cold-reduced carbon steel strip with a mass fraction of carbon over 0,25 % (Сталь углеродистая полосовая, обжатая в холодном состоянии, с содержанием углерода свыше 0,25 %)
ISO 13849-1:2006	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность машин. Детали систем управления, связанные с обеспечением безопасности. Часть 1. Общие принципы проектирования)
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 13850	Safety of machinery — Emergency stop — Principles for design (Безопасность машин. Аварийный останов. Принципы проектирования)
ISO 14119	Safety of machinery — Interlocking devices associated with guards — Principles for design and selection (Безопасность машин. Блокировочные устройства для ограждений. Принципы конструкции и выбора)
ISO 14121-1:2007	Safety of machinery — Risk assessment — Part 1: Principles (Безопасность машин. Оценка риска. Часть 1. Принципы)
ISO 15817:2005	Earth-moving machinery — Safety requirements for remote operator control (Машины землеройные. Требования безопасности к дистанционному управлению)
IEC 60068-2-6	Environmental testing — Part 2: Tests — Test Fc: Vibration (sinusoidal) (Основные методы испытания на воздействие внешних факторов. Часть 2. Испытания. Испытание FC и руководство. Вибрация (синусоидальная))
IEC 60068-2-14	Environmental testing — Part 2: Tests — Test N: Change of temperature (Испытания на воздействие внешних факторов. Часть 2. Испытания. Испытание N: Смена температуры)
IEC 60068-2-27	Environmental testing — Part 2: Tests — Test Ea and guidance: Shock (Испытания на воздействие внешних факторов. Часть 2. Испытания. Часть 2: Испытания. Испытание Ea и руководство: Удар)
IEC 60204-1:1997	Safety of machinery — Electrical equipment of machines — Part 1: General requirements (Электрооборудование промышленных машин. Безопасность. Часть 1. Общие требования)
IEC 60269-1:2006	Low-voltage fuses — Part 1: General requirements (Предохранители плавкие низковольтные. Часть 1: Общие требования)
IEC 60947-2:2006	Low-voltage switchgear and controlgear — Part 2: Circuit-breakers (Комплектное распределительное устройство. Часть 2. Автоматические выключатели)
IEC 60947-5-1:2003	Low-voltage switchgear and controlgear — Part 5-1: Control circuit devices and switching elements — Electromechanical control circuit devices (Аппаратура коммутационная и механизмы управления низковольтные комплектные. Часть 5-1. Устройства и коммутационные элементы цепей управления. Электромеханические устройства цепей управления)
IEC 60947-6-2:2007	Low-voltage switchgear and controlgear — Part 6-2: Multiple function equipment — Control and protective switching devices (or equipment) (CPS) (Аппаратура коммутационная и механизмы управления низковольтные комплектные. Часть 6-2. Многофункциональная аппаратура. Коммутационные устройства (или аппаратура) управления и защиты (CPS))
IEC 61508-1:1998	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 1. Общие требования)
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 (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 2. Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью)
IEC 61508-3:1998	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 3. Требования к программному обеспечению)

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 (Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 5. Примеры методов для определения уровней целостности защиты)
IEC 61508-6:2000	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines of the application of IEC 61508-2 and IEC 61508-3 (Системы электрические/электронные /программируемые электронные, связанные с функциональной безопасностью. Часть 6. Руководящие указания по применению стандартов IEC 61508-2 и IEC 61508-3)
IEC 61508-7:2000	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures (Функциональная безопасность электрических/электронных/программируемых электронных систем, обеспечивающих безопасность. Часть 7. Обзор методов и средств измерения)
IEC 61558-1	Safety of power transformers, power supplies, reactors and similar products — Part 1: General requirements and tests (Трансформаторы силовые, блоки питания и аналогичные изделия. Часть 1. Общие требования и испытания)
IEC 62061:2005	Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems (Безопасность машин и механизмов. Функциональная безопасность электрических, электронных и программируемых электронных систем контроля, связанных с безопасностью)
EN 50205	Relays with forcibly guided (linked) contacts (Реле с принудительно управляемым (механически связанным) контактами)
ECE R79	Uniform provisions concerning the approval of vehicles with regard to steering equipment, Annex 6, Special requirements to be applied to the safety aspects of complex electronic vehicle control systems (Единообразные предписания, касающиеся официального утверждения транспортных средств в отношении механизмов рулевого управления)
SAE J 1939	Recommended Practice for a Serial Control and Communications Vehicle Network (Рекомендации для обмена сообщениями между двумя сегментами сети)

Приложение ДА
(справочное)

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 6165 Машины землеройные. Классификация. Термины и определения	–	*
ISO 13766 Машины землеройные. Электромагнитная совместимость	–	*
IEC 60529 Степени защиты, обеспечиваемые корпусами (Код IP)	IDT	ГОСТ 14254–96 Степени защиты, обеспечиваемые оболочками (Код IP)
IEC 61508 — 4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения	–	*

* Соответствующий межгосударственный стандарт отсутствует. До его 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 обозначения степени соответствия стандарта:

- IDT — идентичный стандарт.

УДК 621.869.4-788:629.614.006.354 МКС 53.100 IDT

Ключевые слова: машины землеройные, управление с использованием электронных компонентов, концепция безопасности, программируемая электронная система PES

Подписано в печать 02.10.2014. Формат 60x84¼.
Усл. печ. л. 4,19. Тираж 32 экз. Зак. 4104

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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