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

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO 19014-2— 2024

МАШИНЫ ЗЕМЛЕРОЙНЫЕ

Функциональная безопасность

Часть 2

Проектирование и оценка оборудования и структуры систем управления, связанных с обеспечением безопасности

(ISO 19014-2:2022, IDT)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Российской ассоциацией производителей специализированной техники и оборудования (Ассоциацией «Росспецмаш») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 267 «Строительно-дорожные машины и оборудование»

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 августа 2024 г. № 176-П)

За принятие проголосовали:

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

4 Приказом Федерального агентства по техническому регулированию и метрологии от 30 сентября 2024 г. № 1326-ст межгосударственный стандарт ГОСТ ISO 19014-2—2024 введен в действие в качестве национального стандарта Российской Федерации с 1 января 2025 г.

5 Настоящий стандарт идентичен международному стандарту ISO 19014-2:2022 «Машины землеройные. Функциональная безопасность. Часть 2. Проектирование и оценка оборудования и структуры систем управления, связанных с обеспечением безопасности» («Earth-moving machinery — Functional safety — Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system», IDT).

Международный стандарт разработан Техническим комитетом по стандартизации ISO/TC 127 «Машины землеройные» Международной организации по стандартизации (ISO).

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

6 ВВЕДЕН ВПЕРВЫЕ

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

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

© ISO, 2022
© Оформление. ФГБУ «Институт стандартизации», 2024



В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 3
5 Общие требования 3
6 Разработка систем 4
7 Оценка эффективности защиты систем 5
8 Информация по эксплуатации и обслуживанию 16
Приложение А (справочное) Примеры систем и оценки 17
Приложение В (справочное) Примеры оценки с использованием баллов HSR 30
Приложение С (обязательное) Сопоставление с другими стандартами на функциональную безопасность 33
Приложение D (справочное) Оценка функции безопасности 34
Приложение Е (обязательное) Исключения и дополнения к ISO 13849-1 и ISO 13849-2 35
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам 38
Библиография 39

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

Функциональная безопасность

Часть 2

Проектирование и оценка оборудования и структуры систем управления, связанных с обеспечением безопасности

Earth-moving machinery. Functional safety. Part 2. Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

Дата введения — 2025—01—01

1 Область применения

Настоящий стандарт устанавливает общие принципы разработки и оценки достигнутого уровня эффективности защиты (MPL_a) систем управления, связанных с обеспечением безопасности (SCS) с использованием элементов, питаемых от всех источников энергии (например, электронных, электрических, гидравлических, механических), используемых в землеройных машинах (EMM) и их оборудовании по ISO 6165.

Принципы настоящего стандарта применяются к системам управления машинами (MCS), которые управляют движением машин или уменьшают опасность; такие системы оцениваются на предмет требуемого уровня эффективности защиты машины (MPL_r) в соответствии с ISO 19014-1 или ISO/TS 19014-5.

Из области применения настоящего стандарта исключены следующие системы:

- системы оповещения, не влияющие на движение машин (например, камеры и системы обнаружения препятствий);
- системы пожаротушения, за исключением случаев, когда срабатывание такой системы препятствует работе другой SCS или активирует ее.

Другие системы или элементы, отказ которых может быть известен оператору (например, стеклоочистители, фары и т. д.) или которые в основном используются для защиты имущества, а также звуковые предупреждения не входят в область применения настоящего стандарта.

Кроме того, в настоящем стандарте рассматриваются существенные опасности по ISO 12100, которые снижаются аппаратными элементами SCS.

Настоящий стандарт не распространяется на EMM, изготовленные до даты его публикации.

2 Нормативные ссылки

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

ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction (Безопасность машин. Основные понятия, общие принципы конструирования. Оценка и снижение рисков)

Издание официальное

ISO 13849-1:2015, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность машин. Элементы систем управления, связанные с обеспечением безопасности. Часть 1. Общие принципы проектирования)

ISO 13849-2:2012, Safety of machinery — Safety-related parts of control systems — Part 2: Validation (Безопасность машин. Элементы систем управления, связанные с обеспечением безопасности. Часть 2. Валидация)

ISO 19014-1, Earth-moving machinery — Functional safety — Part 1: Methodology to determine safetyrelated parts of the control system and performance requirements (Машины землеройные. Функциональная безопасность. Часть 1. Методология определения частей систем контроля, связанных с обеспечением безопасности, и требования к рабочим характеристикам)

ISO 19014-3, Earth-moving machinery — Functional safety — Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system (Машины землеройные. Функциональная безопасность. Часть 3. Экологические показатели и требования к испытаниям электрических и электронных элементов, используемых в элементах системы управления, связанных с безопасностью)

ISO 19014-4:2020, Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (Машины землеройные. Функциональная безопасность. Часть 4. Разработка и оценка программного обеспечения и передачи данных для элементов системы управления, связанных с безопасностью)

ISO/TS 19014-5, Earth-moving machinery — Functional safety — Part 5: Table of Machine Performance Levels (Машины землеройные. Функциональная безопасность. Часть 5. Таблицы уровней эффективности защиты)

3 Термины и определения

В настоящем стандарте применены термины по ISO 12100, ISO 13849-1, ISO 19014-1, а также следующие термины с соответствующими определениями.

ISO и IEC поддерживают терминологические базы данных для использования в стандартизации по следующим ссылкам:

- онлайн-платформа ISO: gost.e-ecolog.ru ;
- Электропедия IEC: gost.e-ecolog.ru .

3.1 **электронная система управления, связанная с обеспечением безопасности;** ESCS (electronic safety control system): Система управления, связанная с обеспечением безопасности, состоящая из электронных элементов от устройства ввода до устройства вывода.

3.2 **функция** (function): Заданное поведение одной или нескольких MCS.

Примечание 1 — Блок управления (например, электронный блок управления) может выполнять более одной функции. Когда в блоке управления содержится несколько функций безопасности, каждая функция безопасности и связанная с ней цепь анализируются отдельно.

3.3 **неэлектронная система управления, связанная с обеспечением безопасности;** N/ESCS (non-electronic safety control system): Система управления, связанная с обеспечением безопасности, состоящая из неэлектронных элементов от устройства ввода до устройства вывода.

3.4 **безопасное состояние** (safe state): Состояние, при котором после отказа системы управления, связанной с обеспечением безопасности, управляемое оборудование, процесс или система автоматически или вручную останавливается или переключается в режим, предотвращающий непреднамеренное поведение или потенциально опасный выброс накопленной энергии.

Примечание 1 — Безопасное состояние может также включать сохранение функции (3.2) системы управления, связанной с обеспечением безопасности (например, рулевого управления) при наличии одиночного отказа в зависимости от уменьшаемой опасности.

3.5 **проверенный элемент** (well-tried component): Элемент для применения, связанного с безопасностью, который широко использовался в прошлом с успешными результатами в таких же или подобных применениях, который был изготовлен и проверен с использованием принципов, демонстрирующих его пригодность и надежность для применений, связанных с обеспечением безопасности.

4 Обозначения и сокращения

В настоящем стандарте применены следующие обозначения и сокращения.

a, b, c, d, e — уровни эффективности защиты машины;

B, 1, 2, 3, 4 — обозначение категорий;

ASIC — интегральная схема для конкретного применения (application specific integrated circuit);

CCF — отказ по общей причине (common cause failure);

DC — диагностический охват (diagnostic coverage);

DCavg — средний диагностический охват (average diagnostic coverage);

ECU — электронный блок управления (electronic control unit);

EMM — землеройная машина (earth-moving machinery);

ESCS — электронная система управления, связанная с обеспечением безопасности (electronic safety control system);

FMEA — анализ видов и последствий отказов (failure modes and effects analysis);

FMEDA — анализ видов отказов, последствий и диагностический анализ (failure modes, effects and diagnostics analysis);

FPGA — программируемая пользователем вентильная матрица (field programmable gate array);

HFT — аппаратная отказоустойчивость (hardware fault tolerance);

HSR — надежность гидравлической системы (hydraulic system robustness);

MCS — система управления машиной (machine control system);

MPL — уровень эффективности защиты машины (machine performance level);

MPLa — достигнутый уровень эффективности защиты машины (machine performance level achieved);

MPLr — требуемый уровень эффективности защиты машины (machine performance level required);

MTTF — среднее время наработки на отказ (mean time to failure);

MTTFd — среднее время наработки на опасный отказ (mean time to dangerous failure);

N/ESCS — неэлектронная система управления, связанная с обеспечением безопасности (non-electronic safety control system);

OTE — запрос от испытательного оборудования (output of test equipment);

SCS — система управления, связанная с обеспечением безопасности (safety control system);

SRP/CS — элемент системы управления, связанный с обеспечением безопасности (safety-related part of the control system);

TE — испытательное оборудование (test equipment).

5 Общие требования

5.1 Применение

Серия стандартов ISO 19014 должна использоваться вместе с серией стандартов ISO 13849 применительно к EMM и заменяет собой стандарты ISO 15998. Если в настоящем стандарте приведены специальные требования, они имеют приоритет над требованиями серии ISO 13849; однако, если в настоящем стандарте не приведены специальные требования, должна применяться серия ISO 13849 с использованием PL вместо MPL (например, MPL = b аналогичен PL = b). Краткое изложение применимых разделов серии ISO 13849 или настоящем стандарте см. в таблицах E.1 и E.2 в приложении E.

Принципы, установленные в настоящем стандарте должны применяться к MCS, которые считаются SCS в соответствии с ISO 19014-1 или ISO/TS 19014-5. Другим системам управления машиной, которые вмешиваются в функцию безопасности системы управления, связанной с обеспечением безопасности, или отключают ее, должен быть присвоен тот же уровень эффективности защиты машины, что и системе, в которую они вмешиваются или действие которой приостанавливают.

Машины должны соответствовать требованиям безопасности и/или мерам защиты/снижения риска, изложенным в настоящем разделе. Кроме того, машина должна быть спроектирована в соответствии с принципами ISO 12100:2010 с учетом соответствующих, но не существенных опасностей, которые не рассматриваются в настоящем стандарте. Программное обеспечение, связанное с обеспечением безопасности, в любых элементах SCS должно соответствовать требованиям ISO 19014-4:2020.

5.2 Существующая SCS

Если существующая SCS была разработана в соответствии с ранее действовавшим стандартом и путем использования и проверки применения продемонстрировала снижение вероятности возникновения опасности до разумно возможного низкого уровня, не требуется обновлять документацию. При модификации ранее использовавшейся SCS необходимо провести анализ воздействия [см. ISO 19014-4:2020, подраздел 3.28)] модификаций, а также разработать и внедрить план действий для обеспечения выполнения требований безопасности.

6 Разработка систем

6.1 Обзор

Многие функции безопасности на мобильных машинах не имеют органов запуска/остановки, которые обычно используются в функциях безопасности стационарных машин, и не всегда добавляются к машине исключительно для уменьшения опасности. Например, рулевое управление, рабочие тормоза, движение и функционирование рабочего оборудования могут иметь модулированные или переменные органы управления в пределах определенного диапазона. Хотя эти типы систем могут соответствовать архитектуре ISO 13849, проектировщики должны учитывать, как характеристики функций безопасности могут отличаться на мобильной машине (например, требуется ли системе управление с обратной связью, а не с разомкнутой, для устранения неправильных движений органов управления, должна ли система устранять опасности, связанные с самопроизвольным срабатыванием также, как и отказы при использовании и т. д.).

Функция безопасности, которая полагается на систему управления для обеспечения необходимого снижения опасности для машины, может быть реализована с помощью SCS в рамках настоящего стандарта. SCS может содержать один или несколько SRP/CS, а несколько SCS могут совместно использовать один или несколько SRP/CS (например, логический блок, элементы управления питанием). Также возможно, что один SRP/CS реализует как функции безопасности, так и функции, не связанные с безопасностью.

Примечание — Индикаторы предупреждения о немедленных действиях см. в ISO 19014-1:2018 (приложение B).

Некоторым системам на мобильных машинах необходимо оставаться в работоспособном состоянии во время отказов. ISO 13849-1:2015 допускает это, но необходимы дополнительные меры для гарантии безопасности и отсутствия конфликтов параллельно действующих систем в соответствии с требованиями заявленной архитектуры.

Приложение C устанавливает минимальные требования, которые должны быть выполнены для использования систем, подсистем и SRP/CS, разработанных и оцененных методами, отличными от установленных в серии ISO 19014.

6.2 Общие требования

После определения функций безопасности SCS требования к функциям безопасности должны быть задокументированы. В течение жизненного цикла требования безопасности детализируются и уточняются на иерархических уровнях. Все требования безопасности должны быть описаны таким образом, чтобы они были однозначными, осуществимыми для реализации и согласовывались с другими требованиями.

При проектировании необходимо учитывать следующее:

- конфликтующие входные или выходные сигналы;
- потерю энергии сигнала и срабатывания любой из систем (например, раздельная подача масла для каждого канала, резервные источники питания для ECU);
- конфликтующие безопасные состояния, требуемые несколькими типами отказов, которые решает система;
- системы, требующие функционирования во время отказа;
- независимость процесса оценки от процесса проектирования;

- когда SCS предназначены для синхронного использования (например, автоматизация задач), система управления должна быть спроектирована таким образом, чтобы уменьшать опасности из-за отсутствия синхронизации.

Примечание — Примером такой синхронизации ЕММ является стрела, рукоять и ковш экскаватора, которые управляются одновременно.

6.3 Конструкция оборудования

Аппаратная структура SCS может обеспечивать меры (например, избыточность, разнообразие и мониторинг) для предотвращения, обнаружения или допущения ошибок. Практические меры могут включать избыточность, разнообразие и мониторинг.

Процесс разработки аппаратного обеспечения должен соответствовать стандарту ISO 13849-1:2015, как указано в приложении Е. Разработчик должен начать с уровня системы, где определены функции безопасности и связанные с ними требования.

Система может быть разбита на подсистемы для облегчения разработки.

Там, где это применимо, каждая фаза цикла разработки должна быть проверена.

На рисунке 1 изображен процесс разработки оборудования в виде V-модели. Для разработки может быть использован любой процесс проектирования, соответствующий требованиям ISO 19014.

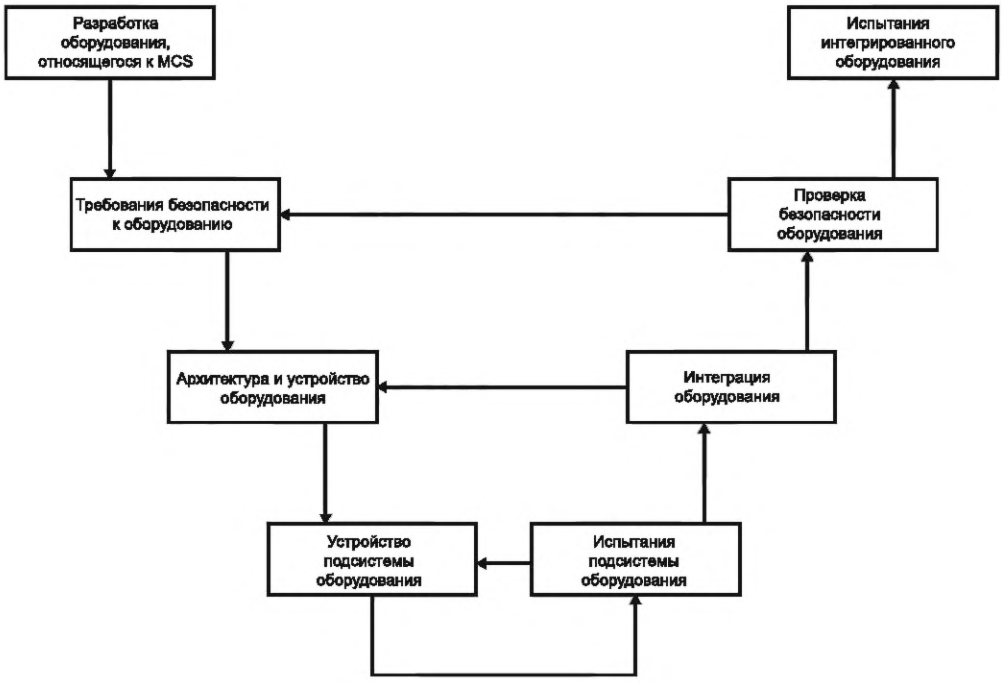


Рисунок 1 — V-модель разработки оборудования

7 Оценка эффективности защиты систем

7.1 Достигнутый уровень эффективности защиты машины (MPL_a)

Достигнутая эффективность элементов, относящихся к обеспечению безопасности для выполнения функции безопасности выражается через определение MPL_a.

Должна быть продемонстрирована и задокументирована способность выполнять функцию безопасности в ожидаемых условиях окружающей среды, как указано в ISO 19014-3.

Процедура оценки MPL_a следующая:

a) определяют рабочую среду элемента и уровень нагрузки;

b) идентифицируют элементы;

c) идентифицируют и документируют исключения отказов (подраздел 7.2) или с помощью соответствующего анализа системы (например, FMEA, анализа дерева отказов и т. д.);

d) рассчитывают $MTTF_d$ (см. ISO 13849-1:2015, приложение D) и следует убедиться, что $MTTF_d$ соответствует требуемому уровню (см. ISO 13849-1:2015);

e) определяют, может ли оборудование обеспечить требуемый уровень DC (ISO 13849-1:2015, приложение E). Для систем, использующих взаимодействие программного обеспечения для определения диагностического охвата, этот анализ может только определить, доступно ли оборудование для поддержки DC, но не проверить, выполнены ли требования к DC для системы;

f) при необходимости рассматривают CCF (см. ISO 13849-1:2015, приложение F);

g) учитывают систематические отказы (ISO 13849-1:2015, приложение G);

h) учитывать возможное взаимодействие с другими функциями безопасности;

i) для проектирования FPGA и ASIC — см. IEC 61508-2:2010, приложения E или F.

Дополнительную информацию об оценке функции безопасности см. в приложении D.

7.2 Оценка безопасности оборудования

7.2.1 Общие положения

В ISO 13849-2:2012 (приложения от A до D), перечислены отказы, исключения отказов и неисправности для различных типов элементов; эти перечни не являются исчерпывающими. При необходимости должны быть рассмотрены и перечислены дополнительные отказы, исключения отказов и неисправности; в таких случаях также должен быть разработан метод оценки.

Для определения отказов и исключений отказов необходимо выполнить анализ видов и последствий отказа (FMEA), анализ дерева отказов или аналогичный анализ системы.

7.2.2 Рассмотрение отказов

В общем случае можно рассматривать следующие критерии отказов:

- если из-за отказа другие элементы выходят из строя, то первый отказ вместе со всеми последующими отказами должен рассматриваться как один отказ;
- два или более отказа, имеющие общую причину, должны рассматриваться как один отказ (известный как CCF);
- одновременное возникновение двух или более отказов, имеющих разные причины, считается крайне маловероятным и, следовательно, не рассматривается.

7.2.3 Исключение отказов

Исключения отказов используются при разработке аппаратного обеспечения как средство приостановки механизмов отказа, ведущих к известным опасностям, в соответствии с признанными передовыми отраслевыми практиками. Исключение отказа — это компромисс между техническими требованиями безопасности и теоретической возможностью возникновения отказа.

Исключение отказа может основываться на следующих критериях:

- техническая невероятность возникновения некоторых отказов;
- общепринятый технический опыт, не зависящий от рассматриваемого применения;
- технические требования, относящиеся к применению и конкретной опасности.

Если отказы исключены, в технической документации должно быть приведено подробное обоснование.

Исключения отказов могут применяться через следующую иерархию.

1) Отказ по базе отказов — после выявления всех отказов, некоторые отказы могут быть исключены на основании вышеуказанных критериев; те отказы, которые не исключены, могут быть обработаны диагностическими средствами в системе управления.

2) Уровень элементов — если все известные отказы SCS могут быть исключены из-за ошибок на уровне элементов, то элемент может быть полностью исключен из отказов.

3) Уровень системы — если все отказы во всех элементах устранены путем исключения отказов, анализ гидравлических систем может быть выполнен с использованием процесса HSR, описанного

в 7.4. Механические системы могут быть исключены из отказов на уровне системы, если элементы спроектированы с учетом соответствующего коэффициента безопасности, а требования по техническому обслуживанию для поддержания правильной функциональности системы включены в руководство по обслуживанию и ремонту в соответствии с разделом 8.

7.2.4 Среднее время наработки на опасный отказ ($MTTF_d$)

Процесс определения $MTTF_d$ описан в ISO 13849-1:2015 (пункт 4.5.2). В то время как ISO 13849-1 рекомендует принципиальное предположение о частоте опасных отказов 50 % (например, $B_{10d} = 2B_{10}$), можно использовать более низкую частоту отказов, если это подтверждается анализом (например, эмпирическими данными, FMEA).

7.3 Диагностический охват (DC)

7.3.1 DC ESCS

См. ISO 13849-1:2015 (пункт 4.5.3).

7.3.2 DC N/ESCS

DC неэлектронных систем определяется одним или несколькими из следующих факторов.

1) Выбор наиболее подходящего аналогичного типа оценки диагностического охвата в соответствии с ISO 13849-1:2015 (приложение E). Например, подвижный клапан, сравнивающий давление масла и выполняющий действие на основе этого давления, сравним с непрерывным мониторингом; следовательно, можно поставить оценку 99 %.

2) Расчет процента DC с помощью FMEDA.

3) Исключение отказов может применяться ко всем или некоторым отказам. Если это делается для некоторых отказов, но не для всех, то необходимо будет рассчитать соответствующий DC.

4) Прямая механическая связь элементов может рассматриваться как 99 % DC.

7.4 Меры по снижению отказов гидравлических систем на системном уровне, основанные на надежности гидравлической системы (HSR)

7.4.1 Общие положения

Оценка MPL_a гидравлических систем рулевого управления и торможения требует оценки отказов элементов в основном канале управления. Из-за характеристик гидравлических элементов и их применения в EMM эти отказы не могут быть устранены с помощью методов обнаружения отказов, используемых в электронных системах. Балл оценки HSR определяется с использованием критериев, приведенных в таблице 1. Основой этой оценки является надежность конструкции гидравлической системы в условиях безопасности EMM. Критерии в таблице 1 основываются на основных принципах безопасности, критериях исключения отказов и проверенных принципах безопасности (например, изложенных в ISO 13849-2:2012, а также на признанных передовых методах проектирования, разработки и производства гидравлических SCS).

Примечание — Эти критерии могут также применяться к гидравлическим системам, не используемым для рулевого управления и торможения, но, учитывая, что эти системы обычно относятся к категории 1, использование таблицы 2 для расчета DC не требуется для анализа системы категории 1.

7.4.2 Расчет оценки HSR

Оценка HSR определяется в процентах по следующей формуле

$$r = \frac{t}{100 - q} \cdot 100,$$

где r — HSR;

q — сумма критериев, которые не снижают вероятность опасного отказа для предполагаемой функции безопасности, которую функция безопасности смягчает;

t — представляет собой сумму остальных применимых критериев, которым удовлетворяет система.

Критерий, которому система не удовлетворяет, не должен включаться в q. (Например, вторичный источник энергии не будет применимым критерием для системы с пружинным приводом и гидравлическим расцеплением, где безопасное состояние системы находится во включенном состоянии).

Каждый SRP/CS в оцениваемой гидравлической системе должен соответствовать требованиям по заданным критериям для получения балла. Частичные оценки не допускаются (например, если име-

ется три клапана и только два из них соответствуют заданным критериям, то оценка по критериям будет равна нулю).

Гидравлические системы должны соответствовать требованиям ISO 13849-2:2012 (пункты С.1 и С.2). Исключение отказов может применяться на уровне элементов, если все применимые отказы могут быть исключены в соответствии с ISO 13849-2:2012 (приложение С).

Таблица 1 — Критерии оценки надежности гидравлической системы

Ссылка	Критерий	Баллы
A	Завышение размеров (например, достаточный зазор клапана, прямолинейность и цилиндричность)	10
B	Меры противодействия прилипанию или прокручиванию клапанов	10
C	Меры противодействия нежелательному гидравлическому воздействию (например, подача высокого давления на оба порта гидромотора)	10
D	Вторичный источник энергии (например, пружинный аккумулятор) или отказоустойчивая конструкция при потере первичного источника энергии	20
E	Медленно или ступенчато прогрессирующий отказ (например, снижение эффективности усилителя рулевого управления перед опасным отказом)	10
F	Предотвращение разрыва шланга (например, от проникновения мусора/истирания)	10
G	В системе поддерживается требуемая чистота гидравлической жидкости	10
H	Меры противодействия кавитации, вызванной аэрацией или вязкостью гидравлической жидкости	10
I	Меры противодействия проблемам с передачей давления, вызванным аэрацией или вязкостью гидравлической жидкости (например, вентиляционный контур)	10
	Всего баллов	

Таблица 2 определяет DC, с которым коррелирует данная оценка HSR, и MPL_a можно определить, используя это значение DC, категорию архитектуры системы, $MTTF_d$ и CCF, адаптированные из ISO 13849-1:2015 (таблица 6.)

См. таблицу 3 для объяснения категории 2M.

Таблица 2 — Корреляция HSR и DC для определения MPL_a

Баллы HSR	Эквивалентный DC	MPL			
		$MTTF_d$ = средний		$MTTF_d$ = высокий	
		Категория B	Категория 2M	Категория 1	Категория 2M
От 50 % до 80 %	60 %	MPL_a = b	MPL_a = b	MPL_a = c	MPL_a = c
Свыше 80 %	90 %	MPL_a = b	MPL_a = c	MPL_a = c	MPL_a = d

См. приложение В для примеров оценок с использованием шкалы HSR.

7.5 Классификация категорий

7.5.1 Общее

Должна быть выбрана соответствующая архитектура, отвечающая требованиям к системе. Разнообразие возможных структур велико, но основные концепции обычно схожи. Таким образом, большинство существующих структур можно отнести к одной из категорий, описанных в ISO 13849-1:2015 (подраздел 6.2); однако для некоторых конструкций, используемых в системах рулевого управления и торможения, требуется адаптация из-за характеристик гидравлической системы, характерных для ЕММ. Для каждой категории дается типичное представление в виде блок-схемы, связанной с безопасностью. Эти типичные реализации называются назначенными архитектурами и перечислены в контексте каждой из следующих категорий.

Некоторые SCS очень сложны и не обязательно точно соответствуют одной из назначенных архитектур. Проекты, отвечающие свойствам соответствующей категории, в целом эквивалентны соответствующей категории назначенной архитектуры. На рисунках 2 и 3 показаны общие архитектуры, а не конкретные примеры. Отклонение от этих архитектур всегда возможно, но любое отклонение должно быть обосновано с помощью соответствующих аналитических инструментов, демонстрирующих соответствие системы требуемому уровню эффективности защиты. Для альтернативных архитектур HFT и любые другие требования должны оставаться эквивалентными соответствующей категории. Назначенные архитектуры должны рассматриваться как логические схемы, а не просто принципиальные схемы. Для категорий 3 и 4 это означает, что не все элементы обязательно физически дублированы, но существуют резервные средства, гарантирующие, что отказ не приведет к потере функции безопасности (например, ECU с параллельной обработкой, перекрестным контролем и внешними датчиками относится к категории 3 или 4).

В таблице 3 представлен обзор категорий SCS, требований и поведения системы в случае отказов. Рекомендуется использовать проверенные элементы. Проверенным элементом для применения, связанного с безопасностью, должны быть элементы, которые:

a) широко использовались в прошлом с успешными результатами в аналогичных применениях или

b) изготовлены и проверены с использованием принципов и технологий, демонстрирующих пригодность и надежность для применений, связанных с безопасностью. Используемые мероприятия по проектированию и проверке должны включать (где применимо):

- соответствие определению проверенного элемента в настоящем стандарте;
- стендовые испытания нагрузочной способности и функциональности;
- контрольные испытания на нагрузки с соответствующим запасом прочности;
- ускоренные испытания на долговечность;
- компьютерный анализ и физические корреляционные исследования;
- экологические испытания по ISO 19014-3;
- поддержку требуемого $MTTF_d$.

MCS, которые конфликтуют с функцией безопасности SCS или приостанавливают ее, должны иметь тот же уровень эффективности защиты машины, что и SCS, если только не будет доказано, что для нее требуется другой MPL_r в соответствии с ISO 19014-1 или ISO/TS 19014-5.

Таблица 3 — Сводка требований по категориям

Категория	Сводка требований	Поведение системы	$MTTF_d$	DC	CCF	HFT
B	SRP/CS и/или их защитное оборудование, а также их элементы должны быть спроектированы, изготовлены, выбраны, собраны и объединены в соответствии с применимыми стандартами, чтобы они могли противостоять ожидаемому воздействию. Должны использоваться основные принципы безопасности	Возникновение отказа может привести к потере функции безопасности	От низкого до среднего	Нет	Не применимо	0
1	Применяются требования категории B. Должны использоваться проверенные элементы и проверенные принципы безопасности	Возникновение отказа может привести к потере функции безопасности. Эффективность защиты машины выше, чем требуется для системы категории B	Высокий	Нет	Не применимо	0

Продолжение таблицы 3

Категория	Сводка требований	Поведение системы	$MTTF_d$	DC	CCF	HFT
2	Должны применяться требования категории B и использоваться проверенные принципы безопасности. Функция безопасности должна проверяться через соответствующие промежутки времени системой управления машиной	Возникновение отказа может привести к потере функции безопасности, но предпринимаются действия для снижения риска, связанного с отказом. Обнаружение отказа во входных и выходных устройствах осуществимо во время или до следующего обращения к функции безопасности	Низкий	От низкого до среднего	Требуется[a]	0
2M	Требования категории 1 применяются к гидравлическим SRP/CS. Требования категории 2 применяются к другим технологиям	Возникновение отказа может привести к потере функции безопасности. Отслеживается способность системы выполнять функцию или применимые отказы являются исключенными. Система будет реагировать при наличии неисключенного отказа	Высокий для гидравлических элементов, низкий для остальных технологий	От низкого до среднего (см. таблицу 2 для гидравлических элементов)	Требуется[a]	0
3	Должны применяться требования категории B и использоваться проверенные принципы безопасности. Элементы систем, связанных с обеспечением безопасности, должны быть сконструированы таким образом, чтобы единичный отказ любого из этих элементов не приводил к потере функции безопасности, и всякий раз, когда это практически осуществимо, единичный отказ обнаруживался	При возникновении одиночного отказа функция безопасности всегда выполняется, но накопление необнаруженных отказов может привести к потере функции безопасности. Некоторые отказы во входных, логических и выходных устройствах обнаруживаются во время или до следующего обращения к функции безопасности	От низкого до высокого	От низкого до среднего	Требуется	1
4	Должны применяться требования категории B и использоваться проверенные принципы безопасности. Элементы систем, связанных с обеспечением безопасности, должны быть сконструированы таким образом, чтобы единичный отказ любого из этих элементов не приводил к потере функции безопасности, и единичный отказ	При возникновении одиночного отказа функция безопасности всегда выполняется, но накопление необнаруженных отказов может привести к потере функции безопасности. Эффективность защиты машины выше, чем требуется для системы категории 3. Все отказы входных, логических и выходных устройств обнаруживаются во время или до сле-	Высокий	Высокий	Требуется	1

Окончание таблицы 3

Категория	Сводка требований	Поведение системы	$MTTF_d$	DC	CCF	HFT
4	обнаруживался во время или до следующего обращения к функции безопасности, но если это обнаружение невозможно, накопление необнаруженных отказов не должно приводить к потере функции безопасности	дующего обращения к функции безопасности, или накопление отказов не может привести к потере функции безопасности	Высокий	Высокий	Требуется	1
[a] Архитектура категории 2 может быть чувствительна к CCF.						

Для обозначенных архитектур, описанных далее в таблице 4, делаются следующие типичные предположения:

- срок службы, 20 лет;
- постоянная интенсивность отказов в течение срока службы;
- для категории 2 частота использований ≤ 1/100 частоты тестирования [см. также примечание в ISO 13849-1:2015 (приложение K)]; или тестирование происходит немедленно при использовании функции безопасности, и общее время для обнаружения отказа и приведения машины в безопасное состояние (обычно для остановки машины) меньше, чем время достижения опасности;
- для категории 2 $MTTF_d$ тестового канала превышает половину $MTTF_d$ базового или функционального канала.

Таблица 4 — Категории для различных технологий

Категория	Механика	Пневматика	Гидравлика	Электроника	Электрика
1	✓	✓	✓	N/A	✓
2	N/A	✓	✓	✓	N/A
3	P/A	P/A	P/A	✓	P/A
4	P/A	P/A	P/A	✓	P/A

N/A — не применяется;
P/A — применяется параллельно;
✓ — применяется.

Примечание 1 — Информацию по P/A см. 7.6, примеры — в приложении A.

Примечание 2 — Сложные электронные элементы (например, микропроцессор, специализированная интегральная схема) не могут использоваться в архитектуре категории 1.

7.5.2 Категория B/Категория 1

7.5.2.1 Пояснение к применению категории B/категории 1 для N/ESCS

Большинство гидравлических и пневматических клапанов и механических соединений имеют архитектуру категории B/категории 1. В случае гидравлического клапана функции входа, логики и выхода выполняются за счет конструкции пружины и золотника внутри клапана. Их можно рассматривать как входные, логические и выходные элементы в одном корпусе. Эти системы аналогичны своим электрическим аналогам в том смысле, что они могут выполнять ту же функцию, используя другую технологию передачи сигнала. На рисунке 2 показан пример системы рулевого управления, реализованной с использованием двух разных технологий.

Примечание — Один из способов рассмотреть границы входа, логики и выхода в системе — рассмотреть, где энергия в сигнальном процессе меняет тип.

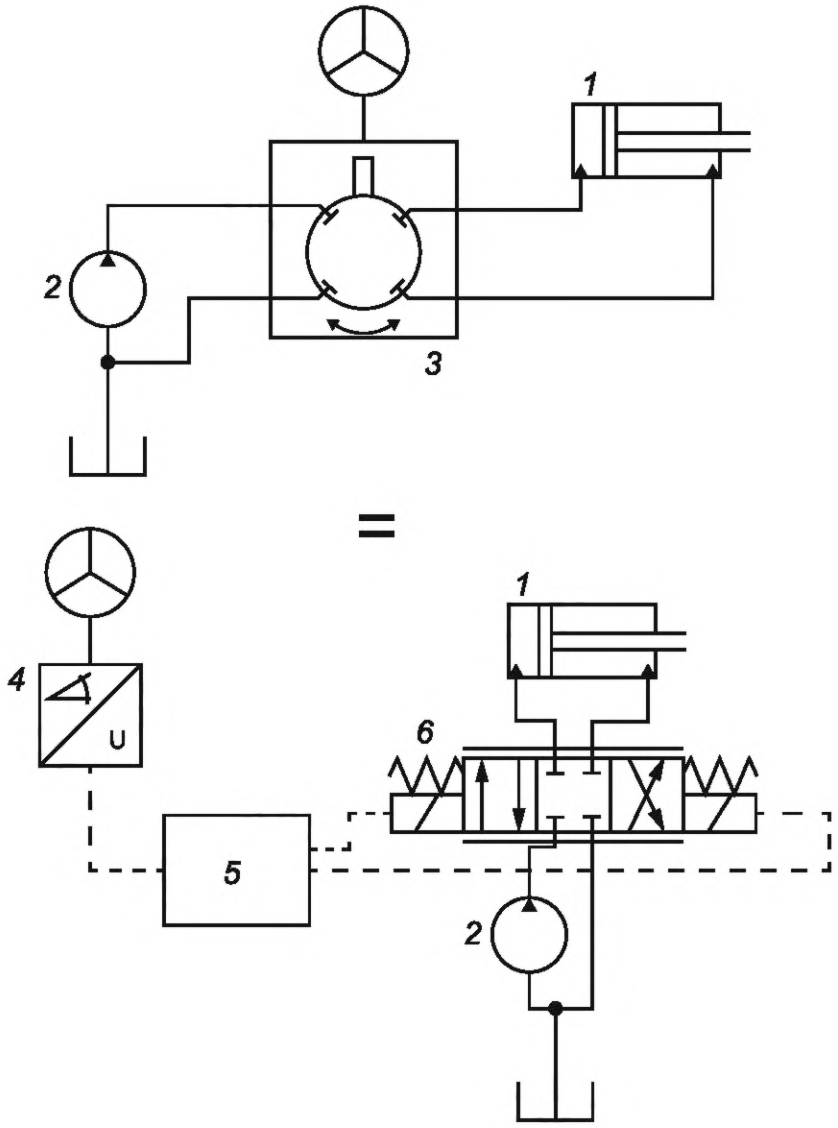
Неполный список общих примеров:

а) оператор нажимает на педаль — энергия меняется с кинетической на гидравлическую;

b) оператор нажимает на педаль — кинетическая энергия превращается в электрическую. Сигнал остается электрическим через элементы I—L и затем преобразуется в гидравлическое давление;

c) управляемая гидравликой система очень похожа на b). Управляющий сигнал представляет собой низкое гидравлическое давление. На выходе используется гидравлическая энергия высокого давления.

7.5.2.2 Примеры применения категории B/категории 1



1 — поворотный гидроцилиндр; *2* — насос; *3* — планетарный клапан; *4* — датчик рулевого управления; *5* — ECU; *6* — клапан рулевого управления

Примечание 1 — Электронные системы обычно решают, как распределяется входная мощность, и управляют выходной энергией на основе этого. N/ESCS имеет выходную мощность, направляемую через основной канал, и либо отправляет энергию обратно в резервуар, либо использует ее для управления машиной.

Примечание 2 — Электронная система может относиться к категории 2, если ECM имеет входную/выходную диагностику и выход для снижения опасности.

Рисунок 2 — Пример двух аналогичных систем рулевого управления категории B/категории 1 с различными технологиями: гидравлическая система рулевого управления (вверху) и аналогичная электронная система рулевого управления (внизу)

7.5.3 Категория 2

7.5.3.1 Общие положения

Руководство по ISO 13849-1:2015 (пункт 6.2.5) применяется с исключениями и разъяснениями, изложенными в настоящем пункте.

a) Когда в результате оценки риска установлено, что у оператора достаточно времени для реагирования, индикатор предупреждения о немедленных действиях может использоваться в качестве OTE в MPL_r = d SCS.

Примечание — Часто оператор лучше, чем SCS подходит для определения подходящей реакции для снижения опасности.

b) OTE должен быть в состоянии перевести машину в безопасное состояние в течение приемлемого времени. Безопасное состояние должно уменьшать опасность, на которую направлена функция безопасности.

c) Если в функциональном блоке (ILO) имеется два или более элементов, включенных параллельно, и требуется отказ более чем одного элемента, чтобы вызвать потерю функции безопасности, этот блок можно рассматривать как функцию категории 3 (см. 7.6 для параллельного добавления).

7.5.3.2 Изменение категории 2 на гидравлические системы (категория 2M)

Применение архитектуры категории 2M соответствует принципам и требованиям архитектуры категории 2, однако выглядит несколько иначе из-за характеристик гидравлических элементов и их применения в EMM, например, в системах рулевого управления и торможения. Категория 2M используется для обозначения другого подхода, принятого в ISO 13849 для стационарных машин.

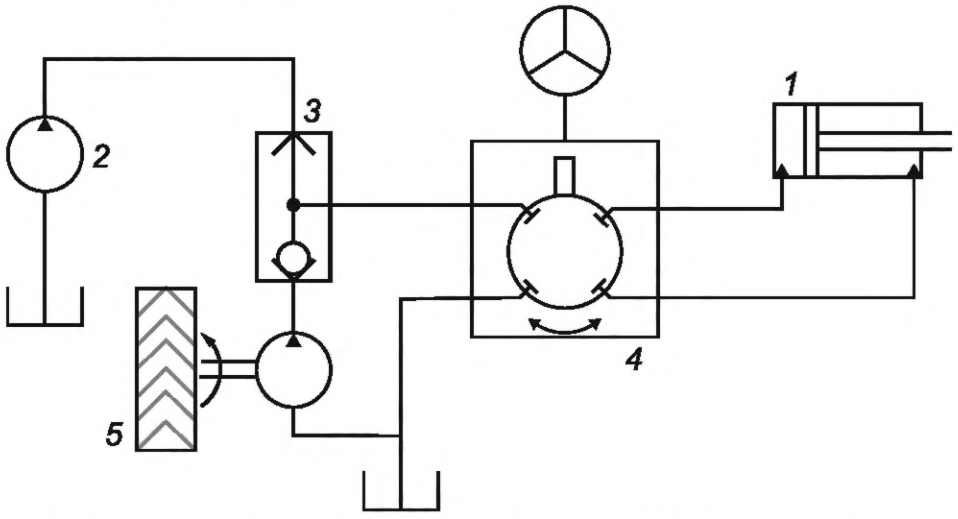
Тестовые каналы систем категории 2M не контролируют основной канал на наличие отказов напрямую; вместо этого они контролируют и поддерживают способность системы выполнять свою функцию (например, когда подача масла недостаточна — переключаются на вторичную подачу). Поскольку их режимы отказов хорошо изучены, а их надежность доказана, отказы в основном канале рассматриваются с использованием оценки HSR в 7.4; эта оценка используется для определения DC-системы.

Примечание 1 — Подача масла обычно контролируется электронной системой, челночным клапаном или подобным устройством и дополняется аккумулятором или резервным насосом при отказе основного источника масла.

Примечание 2 — Это пример «отказоустойчивой» системы. Безопасное состояние заключается в сохранении возможности управления при помощи вторичной подачи масла. В этом случае подача масла и рулевое управление объединены в единую функцию безопасности.

Система категории 2M считается эквивалентной системе категории 2 в отношении процесса и требований к расчету MPL_a согласно ISO 13849-1:2015 (таблица 6). На рисунке 3 показан пример системы рулевого управления категории 2M, а на рисунке 4 показана система в виде блок-схемы.

7.5.3.3 Примеры гидравлических систем категории 2M



1 — поворотный гидроцилиндр; *2* — насос; *3* — челночный клапан; *4* — планетарный клапан; *5* — насос с приводом от ходового колеса

Рисунок 3 — Пример гидравлической системы категории 2M

Примечание 1 — Текст в скобках обозначает функции системы, не входящие в SRP/CS.
Примечание 2 — Термины «шаровый клапан» и «челночный клапан» взаимозаменяемы.

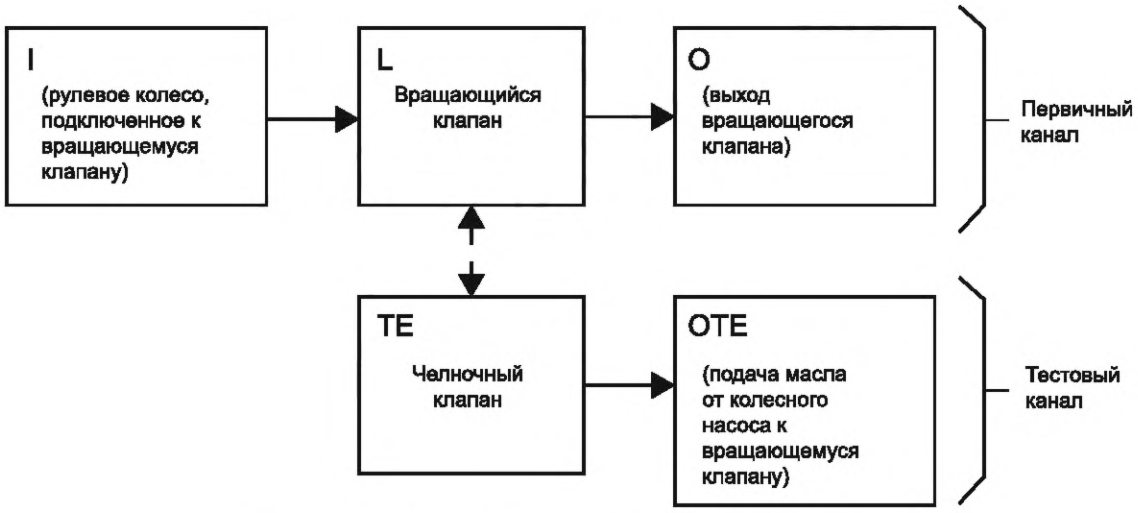


Рисунок 4 — Пример блок-схемы гидравлической системы

7.5.4 Конфликтующие функции безопасности

В случае конфликтующих функций безопасности должны быть рассмотрены безопасные состояния для некоторых неуправляемых применений по сравнению с функциями отказа при использовании. В этом случае оба типа отказов должны иметь свои собственные функции безопасности, каждый со своим собственным MPL_r. Одна из функций безопасности, вероятно, будет иметь более низкий MPL_r, чем другая, и переход в безопасное состояние может переводить машину в наиболее безопасное состояние в соответствии с самым высоким MPL_r.

Примером этого является тормозная система на высокоскоростной машине, где самопроизвольное включение тормоза и отказ при использовании тормоза являются функциями безопасности. В то время как более высокий MPL_r относится к отказу тормозной системы при использовании, самопроизвольное торможение также может быть опасным.

Поскольку отказ при использовании более опасен, максимально безопасным состоянием является остановка машины.

Безопасным состоянием функции безопасности самопроизвольной активации может быть остановка без команды оператора, но через тестовый канал; однако следует уделить внимание тому, как SCS останавливает машину (т. е. таким образом, чтобы снизить опасность неконтролируемого заноса).

Примечание — Конфликтующие функции безопасности могут быть отказоустойчивыми системами.

Если MPL_r конфликтующей функции безопасности одинаковы, может использоваться архитектура категории 3.

7.5.5 Рассмотрение SRP/CS отказоустойчивых систем

Системы категории 2 могут использоваться для отказоустойчивых SCS при условии, что время отклика реакции на отказ соответствующим образом оценено с точки зрения риска (т. е. соответствует уровню эффективности защиты, указанному в применимом стандарте типа С) и меньше, чем частота использования.

Системы категории 3, используемые в отказоустойчивых приложениях, могут функционировать как система с полным резервированием. В случаях, когда единичный отказ может привести к конфликту выходных сигналов, может использоваться избыточная обработка функции безопасности с функцией переключения между основным и вторичным каналами, в зависимости от отказов каждого канала.

Примечание — При использовании такой функции переключения уменьшение частоты тестирования не приводит к уменьшению диагностического охвата, поскольку вторичный канал не работает постоянно.

Примером SCS с постоянным использованием является электрогидравлическая система рулевого управления.

7.6 Комбинация SCS для достижения общего MPL

Для параллельного объединения систем можно использовать приведенные далее положения. Это может быть полезно для оценки архитектур, которые не соответствуют тем, которые указаны для категорий с 1 по 4. См. ISO 13849-1:2015 (подраздел 6.3) для последовательного объединения систем.

Данное сокращение архитектуры относится к качественным требованиям; количественные требования (например, $MTTF_d$, DC, CCF) должны проверяться отдельно. Между объединенными элементами не должно быть отказов по общей причине. Пример снижения MPL_a с использованием последовательно-параллельной комбинации показан на рисунке 5.

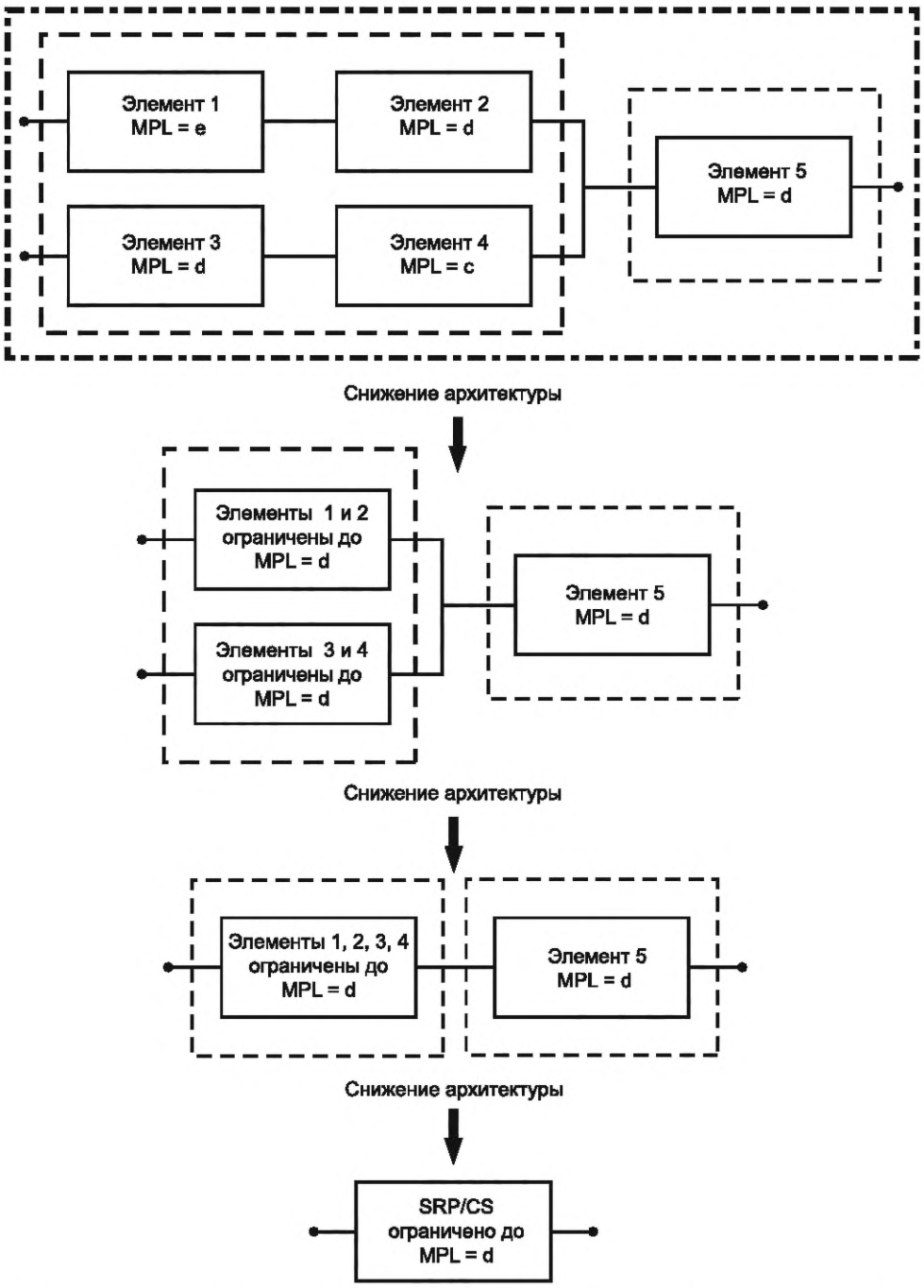


Рисунок 5 — Пример последовательно-параллельной комбинации сокращения MPL_a

В качестве альтернативы параллельному добавлению элементов два параллельных канала HFT = 0 (категория B, 1, 2) могут рассматриваться как система категории 3. Действия оператора по

активации двух каналов должны соответствовать требованиям AR3 в ISO 19014-1:2018 (подраздел 6.5), из-за естественной реакции оператора это выполнимо только в том случае, если два канала действительно избыточны. Несмотря на отсутствие перекрестного мониторинга между двумя каналами, поддерживается HFT = 1.

Этот процесс также относится к параллельным избыточным элементам в функциональных блоках внутри категорий при последовательном добавлении. Рассмотрение блоков таким образом может учитывать дополнительный запас надежности, а рассмотрение блоков как неизбыточных элементов или исключение одного из них из расчета — нет.

8 Информация по эксплуатации и обслуживанию

8.1 Общее

Информация по эксплуатации должна быть предоставлена в соответствии с ISO 12100:2010 (пункт 6.4.5).

8.2 Руководство по эксплуатации

Требования к содержанию руководства по эксплуатации установлены в ISO 6750-1.

Кроме того, может быть предоставлена следующая информация относительно функциональной безопасности EMM, соответствующих настоящему стандарту. Эта информация может быть включена в руководства или другую документацию, предоставляемую конечному пользователю:

- перечень функций безопасности на машине;
- перечень частей систем управления, связанных с безопасностью; особенно если изменения в этих частях могут привести к нарушению функциональной безопасности машины;
- любые задачи по техническому обслуживанию, испытаниям или проверкам, которые необходимы для поддержания целостности SCS в течение всего жизненного цикла машины.

Нет необходимости указывать MPL или категории, когда эти системы поставляются как полноценная SCS, интегрированная в машину.

Приложение А
(справочное)

Примеры систем и оценки

А.1 Общее

Примеры в настоящем приложении предназначены для иллюстрации методик расчета систем с различными MPL, категориями и технологиями и не обязательно отражают реальные системы. Таким образом, эти примеры могут не соответствовать требованиям к уровню эффективности защиты машины, изложенным в ISO/TS 19014-5, а также не предполагают, что безопасное состояние для функции безопасности подходит для данной машины.

Данные примеры развиваются от относительно простых к более сложным. Примеры включают элементы SCS, варьирующиеся от только гидравлических до элементов, включающих электрогидравлические SCS. Краткое описание примеров в настоящем приложении приведено в таблице А.1.

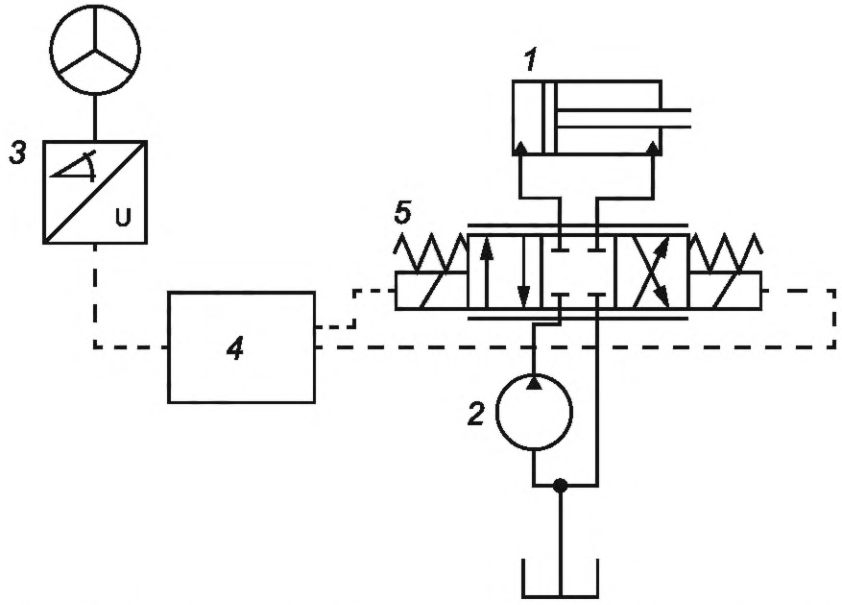
Таблица А.1 — Примеры расчета MPL_a, представленные в этом приложении

MPL_a	Категория	Гидравлика/ гидравлика	Электрика/ гидравлика	Электрогидравлика	Параллельное добавление
b	B			А.1 Рулевое управление	
c	1	А.2 Рулевое управление	А.3 Стояночный тормоз		
c	2			А.4 Рулевое управлении и автоматический стояночный тормоз	
d	2	А.5 Рулевое управление			
d	3			А.6 Тормоза	X

Примечание — Значения $MTTF_d$ для NES/CS можно рассчитать с помощью значений $MTTF_d$ от поставщика элементов или производителя оборудования или значения B_{10d} в соответствии с ISO 13849-1:2015 (пункт C.4).

А.2 Пример 1 — Электрогидравлическое рулевое управление, категория B

Опасное событие: отказ рулевого управления при использовании.
Безопасное состояние: N/A (не применяется), категория B не имеет реакции на отказ.
Функция безопасности: изменение направления движения в соответствии с действиями оператора.
Отказ (инициирующее событие) с использованием TE: N/A, категория B не имеет тестового канала.
Реакции на отказ (OTE): N/A, категория B не имеет тестового канала.
На рисунке А.1 показана схема электрогидравлической системы рулевого управления категории B.



1 — поворотный гидроцилиндр; *2* — насос; *3* — датчик рулевого управления; *5* — ECU; *5* — клапан рулевого управления

Рисунок А.1 — Схема электрогидравлического рулевого управления категории В

Составляют логическую схему.

Логическая схема электрогидравлического рулевого управления SCS категории В представлена на рисунке А.2.

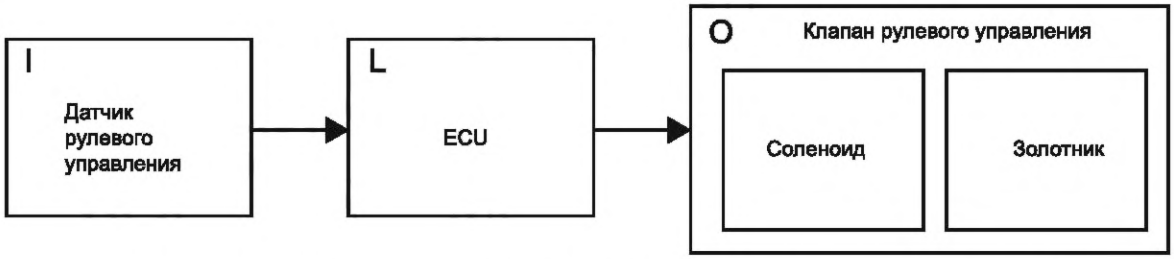


Рисунок А.2 — Логическая схема электрогидравлического рулевого управления категории В

Рассчитывают $MTTF_d$ для системы (ограниченной элементами, показанными выше).

В таблице А.2 показан расчет $MTTF_d$ методом подсчета элементов для электрогидравлической системы рулевого управления категории В.

Таблица А.2 — Пример расчета $MTTF_d$ методом подсчета элементов

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
1	Датчик рулевого управления	50	50	100	0,010	1	0,010
2	ECU	25	50	50	0,020	1	0,020
3	Соленоид	34	50	67	0,015	2	0,030
4	Золотник	75	50	150	0,007	1	0,007
$\Sigma(1/MTTF_{di})$							0,067
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							14,9

Определяют DC для каждого элемента.

Система категории B: DC = N/A для всех элементов.

Выбирают MPL_a из ISO 13849-1:2015 (таблица 6).

Примечание 1 — $MTTF_d$ общее = 16,7 = средний, DC = 0, категория = B; следовательно, MPL_a = b.

Примечание 2 — Соленоид и золотник могут быть единым узлом, если соленоид не является обслуживаемым элементом; в этом случае для назначения соответствующего значения $MTTF_d$ анализируют сборку.

А.3 Пример 2 — Гидрогидравлическое рулевое управление, категория 1

Примечание 1 — Чтобы проиллюстрировать процесс расчета MPL_a одноканальной гидравлической системы, для этого примера не использовался ISO 13849-2. Элементы были оценены как хорошо зарекомендовавшие себя в соответствии с ISO 13849-2.

Опасность: самопроизвольное изменение направления движения машины.

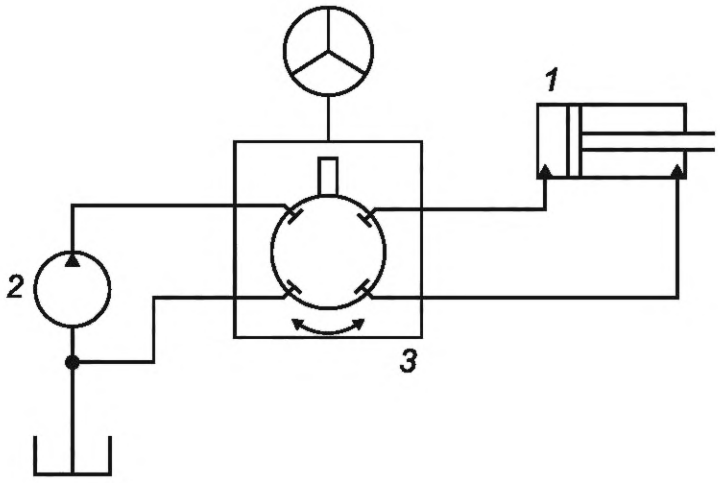
Безопасное состояние: N/A, категория 1 не имеет реакции на отказ.

Функция безопасности: изменение направления движения машины только в соответствии с действиями оператора.

Отказ (инициирующее событие) с использованием TE: N/A, категория 1 не имеет тестового канала.

Реакции на отказ (OTE): — категория 1 не имеет тестового канала.

На рисунке А.3 показана схема гидравлической системы рулевого управления категории 1.



1 — поворотный гидроцилиндр; *2* — насос; *3* — планетарный клапан

Рисунок А.3 — Схема гидрогидравлического рулевого управления категории 1

Составляют логическую схему.

Логическая схема гидравлического рулевого управления SCS категории 1 показана на рисунке А.4.



Рисунок А.4 — Логическая схема гидрогидравлического рулевого управления, категория 1

Рассчитывают $MTTF_d$.

В таблице А.3 показан расчет $MTTF_d$ по эмпирическим данным для гидравлической системы рулевого управления категории 1.

Таблица А.3 — Расчет $MTTF_d$ гидрогидравлического рулевого управления, категория 1

Элемент	$MTTF_d$	DC
Планетарный клапан	167 лет эмпирических данных	0

$MTTF_d$ канала = 100 лет, сокращено по ISO 13849-1:2015 (пункт 4.5.2).
Определяют DC для каждого элемента.
Система категории 1; DC = N/A для всех элементов.
Выбирают MPL_a из ISO 13849-1:2015 (таблица 6).

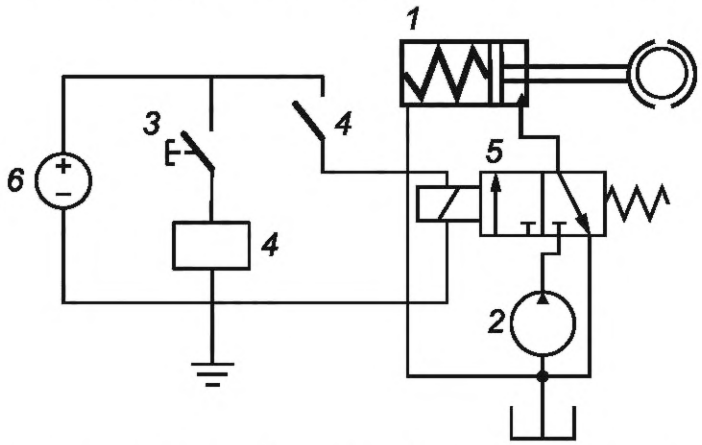
Примечание 2 — $MTTF_d$ общее = 100 = высокая, DC = 0, категория = 1. Следовательно, MPL_a = c; ссылка на ISO 13849-1:2015 (таблица 6).

А.4 Пример 3 — Электрогидравлический стояночный тормоз, категория 1

Опасность: отказ при использовании стояночного тормоза.
Безопасное состояние: тормоз срабатывает силой пружины.

Примечание 1 — Это система категории 1 из-за использования проверенных элементов без сложной электроники.

Функция безопасности: включение стояночного тормоза по команде оператора. При потере гидравлического или электрического питания стояночный тормоз включается автоматически.
Отказ (инициирующее событие) с использованием TE: N/A, категория 1 не имеет тестового канала.
Реакции на отказ (OTE): N/A — категория 1 не имеет тестового канала.
На рисунке А.5 показана схема электрогидравлического стояночного тормоза категории 1.



1 — цилиндр привода стояночного тормоза; *2* — насос; *3* — кулачковый выключатель (в данном случае кулачковый выключатель должен соответствовать требованиям ISO 13849-2 и быть проверенным элементом); *4* — реле; *5* — электромагнитный клапан; *6* — батарея

Рисунок А.5 — Схема электрогидравлического стояночного тормоза, категория 1

Составляют логическую схему.
Логическая схема электрогидравлического стояночного тормоза категории 1 представлена на рисунке А.6.

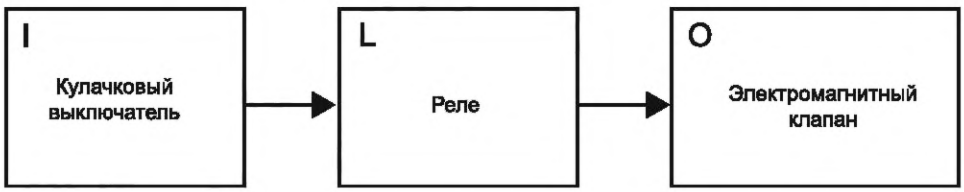


Рисунок А.6 — Логическая схема электрогидравлического стояночного тормоза, категория 1

Рассчитывают $MTTF_d$ системы.
В таблице А.4 показан расчет $MTTF_d$ методом подсчета элементов для электрогидравлического стояночного тормоза категории 1.

Таблица А.4 — Пример расчета $MTTF_d$ методом подсчета элементов

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$ 1/год	Количество	Итого
1	Кулачковый выключатель	200	50	400	0,0025	1	0,0025
2	Реле	200	50	400	0,0025	1	0,0025
3	Электромагнитный клапан	100	50	200	0,005	2	0,005
$\Sigma(1/MTTF_{di})$							0,01
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							100

Определяют DC для каждого элемента.

DC = 0 для всех элементов в данном примере.

Выбирают MPL_a по ISO 13849-1:2015 (таблица 6).

Примечание 2 — $MTTF_d$ общее = 100 = высокая, DC = 0, категория = 1 (проверенные элементы). Следовательно, MPL_a = c; ссылка на ISO 13849-1:2015 (таблица 6).

А.5 Пример 4 — Электрогидравлическое рулевое управление с автоматическим стояночным тормозом, категория 2

Опасность: самопроизвольное изменение направления движения машины, отказ рулевого управления.

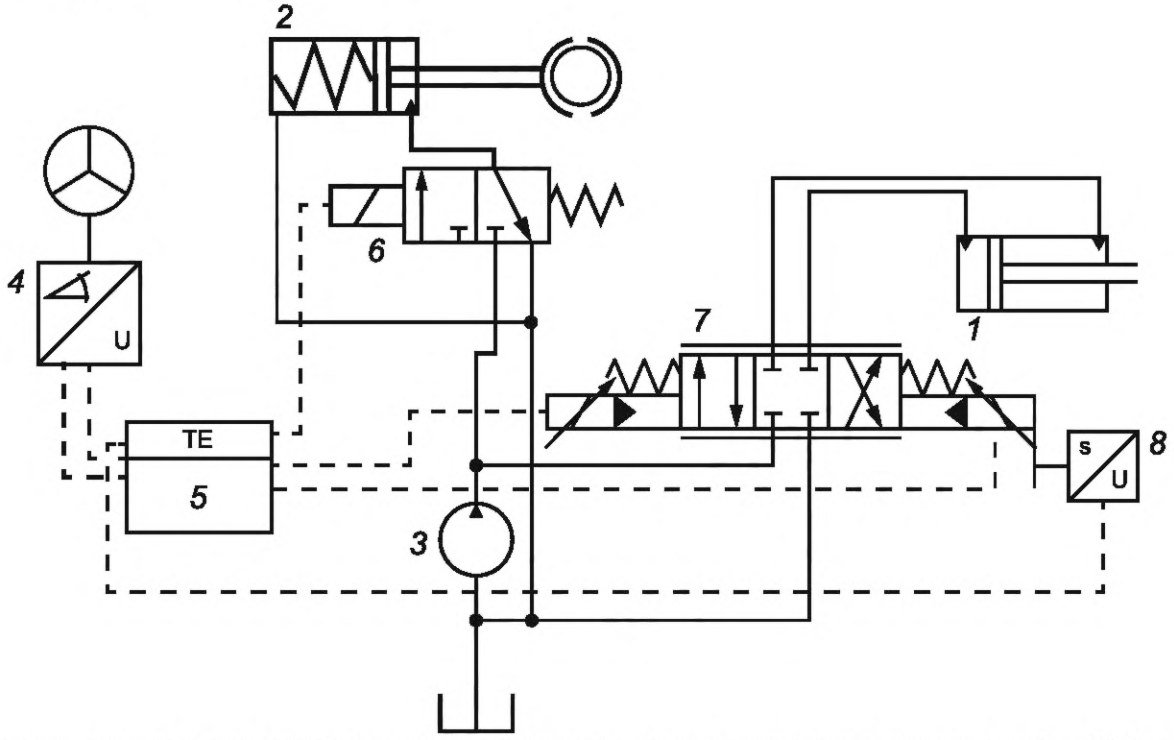
Безопасное состояние: остановка машины.

Функция безопасности: включение стояночного тормоза.

Отказ (инициирующее событие) с помощью ТЕ: датчик положения соленоида рулевого управления.

Реакции на отказ (ОТЕ): N/A — остановка машины с помощью стояночного тормоза.

На рисунке А.7 показана схема электрогидравлической системы рулевого управления категории 2 с автоматическим стояночным тормозом.



1 — гидроцилиндр рулевого управления; *2* — стояночный тормоз; *3* — насос; *4* — датчик рулевого управления; *5* — ECU (содержит и основной и тестовый функционал); *6* — клапан стояночного тормоза; *7* — клапан рулевого управления; *8* — датчик положения золотника (для идентификации отказа, если клапан реагирует не соответствующим образом)

Рисунок А.7 — Схема электрогидравлического рулевого управления с автоматическим стояночным тормозом, категория 2

Составляют логическую схему.

Логическая схема электрогидравлического стояночного тормоза категории 1 представлена на рисунке А.2.

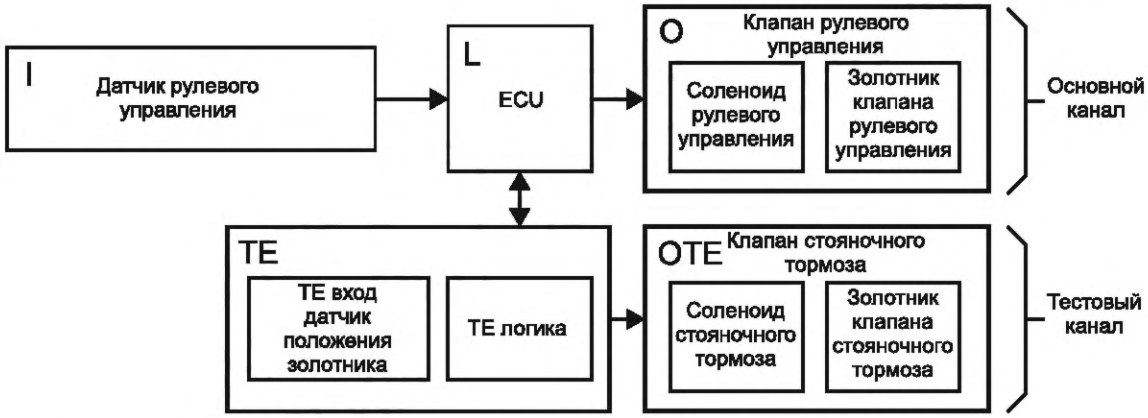


Рисунок А.8 — Логическая схема электрогидравлического рулевого управления с автоматическим стояночным тормозом, категория 2

Рассчитывают $MTTF_d$ системы.

В таблице А.5 показан расчет $MTTF_d$ методом подсчета элементов для основного канала, в таблице А.6 — для тестового канала электрогидравлического рулевого управления с автоматическим стояночным тормозом категории 2.

Таблица А.5 — Пример расчета $MTTF_d$ методом подсчета элементов для основного канала

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
1	Датчик рулевого управления	100	50	200	0,0050	1	0,0050
2	ECU (основной функционал)	50	50	100	0,0100	1	0,0100
3	Соленоид клапана рулевого управления	200	50	400	0,0025	2	0,0050
4	Золотник клапана рулевого управления	75	50	150	0,0067	1	0,0067
$\Sigma(1/MTTF_{di})$							0,0267
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							37,5

Таблица А.6 — Пример расчета $MTTF_d$ методом подсчета элементов для тестового канала

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
1	ECU (тестовый функционал)	50	50	100	0,010	1	0,010
2	Датчик положения золотника	100	50	200	0,005	1	0,005

Окончание таблицы А.6

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
3	Соленоид клапана стояночного тормоза	100	50	200	0,005	1	0,005
4	Золотник клапана стояночного тормоза						
$\Sigma(1/MTTF_{di})$							0,020
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							50,0

Идентифицируют все общие причины отказов.

Стояночный тормоз приводится в действие пружиной и гидравлически растормаживается, требуя применения давления масла для отключения тормоза. Отказ источника питания приведет к отказу рулевого управления и автоматическому включению стояночного тормоза.

См. таблицу А.7 для оценки отказов по общим причинам.

Таблица А.7 — Оценка отказов по общим причинам

№	Меры против CCF	Баллы	Комментарий
1	**Разделение**		
	Физическое разделение путей прохождения сигнала: разделение проводки, достаточные зазоры на печатных платах	15/15	Все печатные платы спроектированы правильно. Соединительная проводка проверена в эксплуатации
2	**Разнообразие**		
	Используются различные технологии/конструкции или физические принципы, например: первый канал программируемый электронный, второй канал — проводной, вид инициации, давление и температура, измерение расстояния и давления, цифровые и аналоговые, комплектующие разных производителей	20/20	Все электронные элементы чувствительны к отказу источника питания, что приводит к отказу рулевого управления. Подпружиненный стояночный тормоз с гидравлическим отключением сработает автоматически
3	**Разработка/применение/опыт**		
3.1	Защита от перенапряжения, избыточного давления, перегрузки по току и т.д.	15/15	Питание от батареи, подаваемое на цепь, защищено предохранителем. ECU содержит внутренний регулятор напряжения и фиксирующие диоды
3.2	Используются проверенные элементы	0/5	ECU относительно новый и не считается проверенным
4	**Оценка/анализ**		
	Чтобы избежать отказов по общей причине в конструкции, рассматриваются результаты анализа вида отказа и его последствий	5/5	FMEA был проведен

Окончание таблицы А.7

№	Меры против CCF	Баллы	Комментарий
5	**Компетентность/обучение**		
	Разработчики/специалисты по обслуживанию обучены понимать причины и последствия отказов по общей причине	5/5	Персонал, занимающийся проектированием и техническим обслуживанием, прошел необходимое обучение
6	**Влияние окружающей среды**		
6.1	Система проверена на электромагнитную совместимость, как указано в соответствующих стандартах	25/25	Система прошла испытания на соответствие стандарту ISO 13766
6.2	Были учтены требования устойчивости ко всем соответствующим воздействиям окружающей среды, таким как температура, удары, вибрация и влажность	10/10	Система прошла испытания на соответствие стандарту ISO 19014-3
	Итого	95/100	

Результат выше 65 считается достаточным для успешного прохождения оценки. Меры против отказов по общим причинам применялись в достаточной мере.

Определяют любые исключения отказов.

Опасные элементы, используемые в данной системе, хорошо зарекомендовали себя в эксплуатации [см. ISO 13849-2:2012 (таблица D.4)]. При производстве используется система контроля качества. Элементы проверяются на качество в рамках процесса проектирования и производства. Все силовые цепи защищены предохранителями. Все функции управления индивидуально проверяются в конце сборочной линии. Опасности присоединения можно разумно исключить, поскольку очень маловероятно, что отказ проводки приведет к опасному отказу.

Определяют DC_{avg} для системы.

a) Определяют все опасные режимы отказа для каждого элемента.

b) Определяют все опасные режимы отказа, которые можно диагностировать.

c) Используют формулу, приведенную в ISO 13849-1:2015 (приложение E), для расчета DC.

В таблице А.8 показан расчет DC_{avg} для электрогидравлической системы рулевого управления категории 2 с автоматическим стояночным тормозом.

Таблица А.8 — Расчет DC_{avg} для системы

Номер элемента	Описание элемента	Возможно обнаружить?	Опасный отказ?	$DC_{элемента}$, %	$MTTF_d$, лет	$DC/MTTF_d$	$1/MTTF_d$
1	Датчик рулевого управления			90	200	0,45	0,005
	В допустимых пределах	Да	Да				
	Вне допустимых пределов	Да	Да				
2	ECU			60	100	0,6	0,01
	Остановка процессора	Нет	Да				
	Отказ выходного драйвера	Да	Да				
	Отказ входного шлюза	Да	Да				
3	Соленоид рулевого управления 1			90	400	0,225	0,0025

Окончание таблицы А.8

Номер элемента	Описание элемента	Возможно обнаружить?	Опасный отказ?	$DC_{элемента}$, %	$MTTF_d$, лет	$DC/MTTF_d$	$1/MTTF_d$
	Обрыв обмотки	Да	Да				
	Замыкание обмотки	Да	Да				
4	Соленоид рулевого управления 2			90	400	0,225	0,0025
	Обрыв обмотки	Да	Да				
	Замыкание обмотки	Да	Да				
5	Золотник клапана рулевого управления			99	150	0,66	0,00666667
	В допустимых пределах	Да	Да				
	Вне допустимых пределов	Да	Да				
						2,16	0,02666667
	DC_{avg}, %						81

$$d_{avg}\frac{\frac{d_1}{m_1}+\frac{d_2}{m_2}+\ldots+\frac{d_n}{m_n}}{\frac{1}{m_1}+\frac{1}{m_2}+\ldots+\frac{1}{m_n}}=\frac{\frac{90}{200}+\frac{60}{100}+2\cdot\frac{90}{400}+\frac{99}{150}}{\frac{1}{200}+\frac{1}{100}+2\cdot\frac{1}{400}+\frac{1}{150}}=81\,\%,$$

где d_n — диагностический охват DC n-го элемента;

m_n — среднее время до опасного отказа $MTTF_d$ n-го элемента.

В этом примере MPL_a выбран из ISO 13849-1:2015, таблица 6.

Примечание — Общее $MTTF_d$ = 37,5 = высокое, DC = низкое, категория = 2; следовательно, MPL_a = c.

А.6 Пример 5 — Гидравлическая система рулевого управления, категория 2М

Опасность: отказ рулевого управления при использовании.

Безопасное состояние: рулевое управление с вторичным источником масла.

Функция безопасности: изменение направления движения в соответствии с действиями оператора.

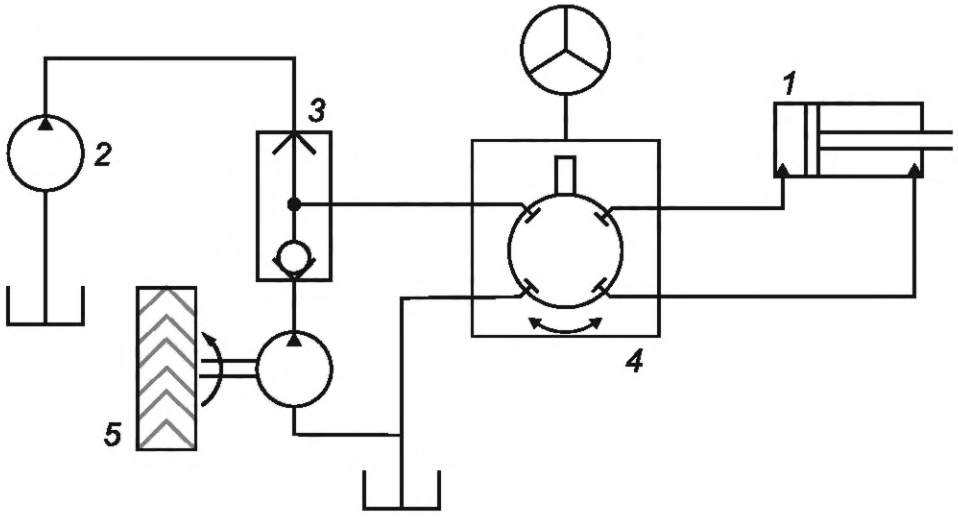
Отказ (инициирующее событие) с использованием ТЕ: используют масло из вторичного источника при падении давления масла из первичного источника. Все остальные отказы исключаются в соответствии с ISO 13849-2:2015 и устраняются с помощью средств, не связанных с системой управления.

Реакции на отказ (ОТЕ): рулевое управление с вторичным источником масла.

Примечание — Если отказ элемента исключен, нет необходимости рассчитывать $MTTF_d$ для этого элемента.

Однако расчет $MTTF_d$ был включен в таблицу А.9 для демонстрации процесса.

На рисунке А.9 показана схема гидравлической системы рулевого управления категории 2М.



1 — гидроцилиндр рулевого управления; *2* — насос; *3* — челночный клапан; *4* — планетарный клапан; *5* — насос с приводом от ходового колеса

Рисунок А.9 — Схема гидравлической системы рулевого управления, категория 2М

Составляют логическую схему.

Логическая схема гидравлической системы рулевого управления категории 2М представлена на рисунке А.10.

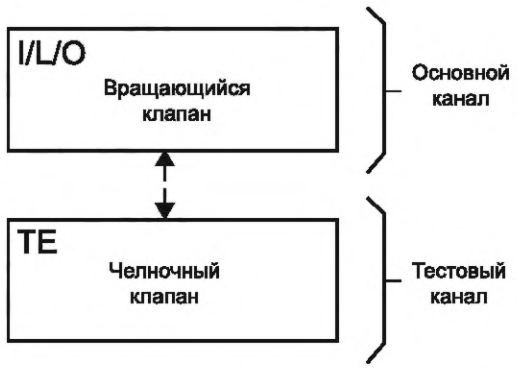


Рисунок А.10 — Логическая схема гидравлической системы рулевого управления, категория 2М

Рассчитывают $MTTF_d$ системы.

В таблице А.9 показан расчет $MTTF_d$ методом подсчета элементов для основного канала, в таблице А.10 — для тестового канала гидравлической системы рулевого управления категории 2М.

Таблица А.9 — Пример расчета $MTTF_d$ методом подсчета элементов для основного канала

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
1	Планетарный клапан	200	50	400	0,0025	1	0,0025
$\Sigma(1/MTTF_{di})$							0,0025
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							400

Таблица А.10 — Пример расчета $MTTF_d$ методом подсчета элементов для тестового канала

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$ 1/год	Количество	Итого
1	Челночный клапан	100	50	200	0,005	1	0,005
$\Sigma(1/MTTF_{di})$							0,005
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							200

Среднее время наработки на отказ основного канала = 100 лет, сокращено по ISO 13849-1:2015, 4.5.2.

Определяют DC для каждого элемента.

DC = 99 % благодаря постоянному контролю, обеспечиваемому челночным клапаном первичного канала.

Выберают MPL_a из ISO 13849-1:2015, таблица 6.

Общее $MTTF_d$ = 100 = высокое, DC = высокое, категория = 2M; следовательно, MPL_a = d; ссылка на ИСО 13849-1:2015, таблица 6.

А.7 Пример 6 — Электрогидравлическая рабочая тормозная система, категория 3

Двухканальная тормозная система с аналоговым датчиком педали и датчиком конца хода.

На схеме далее приведена комбинация резервной тормозной системы, которая увеличивает MPL_a за счет параллельного добавления двух цепей.

Опасность: отказ при использовании тормозов.

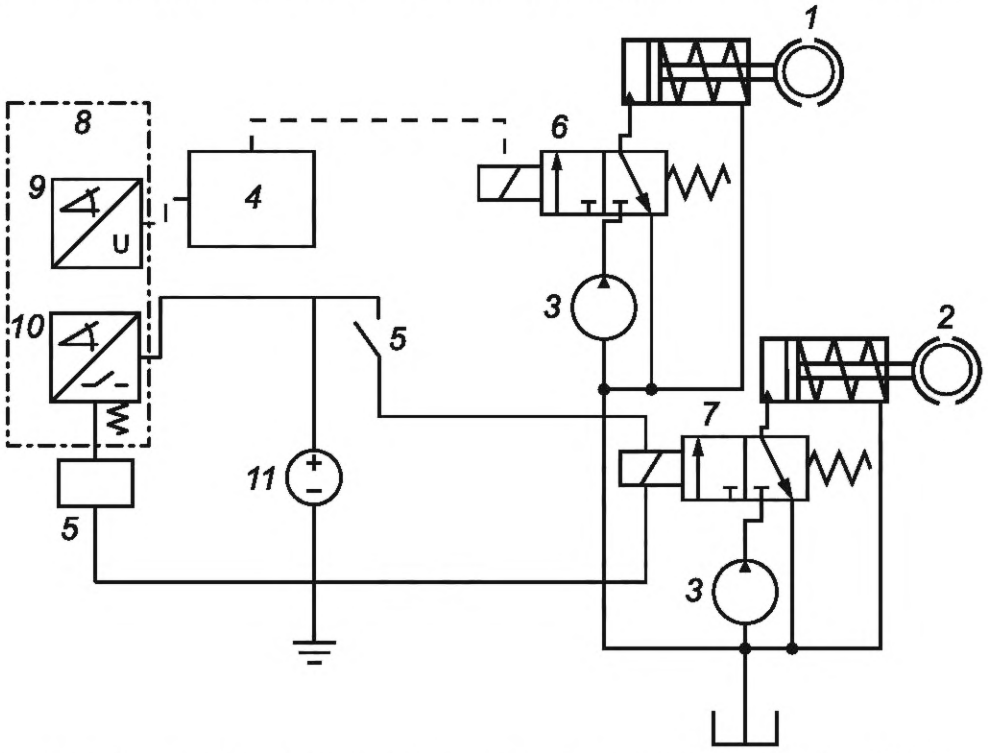
Безопасное состояние: торможение в соответствии с действиями оператора.

Функция безопасности: тормоз с вторичным каналом.

Отказ (инициирующее событие) с использованием ТЕ: педаль тормоза содержит концевой выключатель, активирующий вторичный тормозной канал, если первичный канал выходит из строя.

Реакция на отказ (ОТЕ): тормозная система с вторичным каналом, срабатывающим от концевого выключателя.

На рисунке А.11 показана схема электрогидравлической рабочей тормозной системы категории 3.



1 — основной тормозной цилиндр; *2* — дополнительный тормозной цилиндр; *3* — насос; *4* — ECU; *5* — реле тормоза; *6* — электромагнитный клапан основной тормозной системы; *7* — электромагнитный клапан дополнительной тормозной системы; *8* — педаль тормоза; *9* — датчик педали; *10* — концевой выключатель конца хода педали; *11* — аккумуляторная батарея

Рисунок А.11 — Схема электрогидравлической рабочей тормозной системы, категория 3

Рассчитывают $MTTF_d$ системы.

В настоящем примере значения MTTF получены от изготовителя.

В таблице А.11 показан расчет $MTTF_d$ методом подсчета элементов для основной тормозной системы, в таблице А.12 — для дополнительной тормозной системы.

Таблица А.11 — Пример расчета $MTTF_d$ методом подсчета элементов для основной тормозной системы

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
1	Датчик педали	200	50	400	0,0025	1	0,0025
2	ECU (основной функционал)	50	50	100	0,0100	1	0,0100
3	Электромагнитный клапан основной тормозной системы	200	50	400	0,0025	1	0,0025
$\Sigma(1/MTTF_{di})$							0,015
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							66,7

Таблица А.12 — Пример расчета $MTTF_d$ методом подсчета элементов для дополнительной тормозной системы

Номер элемента	Описание элемента	$MTTF_i$ (из базы данных), лет	Опасные отказы, %	$MTTF_{di}$, лет	$1/MTTF_{di}$, 1/год	Количество	Итого
1	Концевой выключатель конца хода педали	200	50	400	0,0025	1	0,0025
2	Реле	200	50	400	0,0025	1	0,0025
3	Электромагнитный клапан дополнительной тормозной системы	100	50	200	0,005	1	0,005
$\Sigma(1/MTTF_{di})$							0,010
$MTTF_d = 1/\Sigma(1/MTTF_{di})$, лет							100

Определяют MPL_a обоих контуров.

Основной тормозной контур MPL_a = c из аналогичного анализа в приведенном выше примере.

Дополнительный тормозной контур представляет собой контур категории 1 с высоким $MTTF_d$ с MPL_a = c.

Определяют общее MPL_a для комбинированного контура.

Параллельное добавление двух цепей MPL_a = c приводит к увеличению MPL_a до d.

SRP/CS: (MPL_a = c + параллельный MPL_a = c) = MPL_a = d.

Составляют логическую схему, идентифицирующую SCS.

Логическая схема электрогидравлического рабочего тормоза категории 3 показана на рисунке А.12.

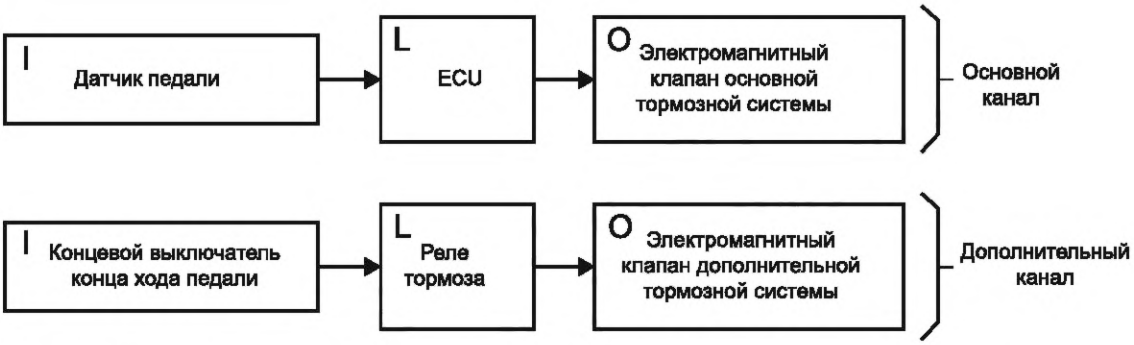


Рисунок А.12 — Логическая схема электрогидравлической рабочей тормозной системы категории 3

Приложение В
(справочное)

Примеры оценки с использованием баллов HSR

В.1 Контур гидравлического рулевого управления колесного погрузчика

Схема, приведенная ниже, демонстрирует использование HSR для установления MPL_a = d для полностью гидравлической SCS. Рулевое колесо управляет планетарным клапаном, который подает давление в гидравлический цилиндр, используемый для управления машиной.

Опасность: отказ рулевого управления, самопроизвольное изменение направления движения машины.

Безопасное состояние: поддержание функционирования рулевого управления.

Функция безопасности: управление машиной в соответствии с действиями оператора.

Отказ (инициирующее событие) с использованием ТЕ: челночный клапан определяет, какое из давлений подачи — основного насоса рулевого управления или насоса с приводом от ходового колеса, является наиболее высоким.

Реакции на отказ (ОТЕ): челночный клапан подает самое высокое давление на планетарный клапан.

Исключения отказов.

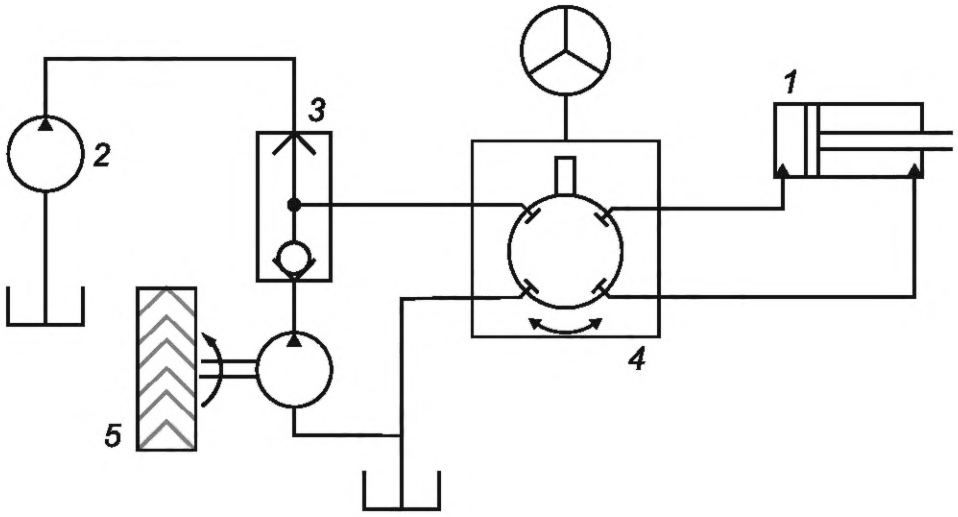
Все гидравлические элементы соответствуют условиям для следующих исключений отказов в соответствии с ISO 13849-2:2012 (приложение С), где это применимо:

- изменение времени переключения;
- непереключение или неполное переключение;
- самопроизвольное изменение исходного положения переключения;
- утечка;
- разрыв корпуса клапана или поломка подвижных элементов, а также поломка/разрушение контрольных или корпусных винтов;
- для пропорциональных клапанов: гидравлические отказы, вызывающие неконтролируемое поведение;
- для челночных клапанов: одновременное закрытие обоих входных патрубков.

Примечание 1 — Шланги и соединители также соответствуют требованиям исключения отказов, однако эти исключения отказов в данном примере не перечислены.

Примечание 2 — Обоснование, подтверждающее аргументы в пользу исключения отказа, является частью необходимой документации, подтверждающей заявление MPL.

На рисунке В.1 показана схема системы рулевого управления с планетарным клапаном.



1 — гидроцилиндр рулевого управления; *2* — насос; *3* — челночный клапан; *4* — планетарный клапан; *5* — насос с приводом от ходового колеса

Рисунок В.1 — Схема рулевого управления с планетарным клапаном

Баллы HSR для системы рулевого управления с планетарным клапаном приведены в таблице В.1.

Таблица В.1 — Баллы HSR для системы рулевого управления с планетарным клапаном

Критерий	Возможные баллы	Баллы системы	Включить в *q* (да/нет)
Избыточный размер (например, достаточный зазор золотника, прямолинейность и цилиндричность)	+10	+10	Нет
Меры противодействия залипанию золотника, прокручиванию	+10	+10	Нет
Меры противодействия нежелательному гидравлическому воздействию (например, мгновенное высокое давление на оба порта гидравлического двигателя)	+10	+10	Нет
Вторичный источник энергии (например, с пружинным аккумулятором) или отказоустойчивая конструкция при потере источника энергии	+20	+20	Нет
Медленно или ступенчато прогрессирующий отказ (например, уменьшение эффективности усилителя рулевого управления перед опасным отказом)	+10	+10	Нет
Снижение вероятности разрыва шлангов (например, отсутствие острых кромок)	+10	+10	Нет
В системе поддерживается необходимая чистота	+10	+10	Нет
Меры противодействия кавитации, вызванной аэрацией гидравлического масла	+10	+10	Нет
Меры по устранению проблем с передачей давления, вызванных аэрацией гидравлического масла (например, вентиляционный контур)	+10	0	Да
Итого баллов		90	

Расчет баллов HSR.

t = 90 (сумма столбца «Оценка системы»).

q = 10 (сумма столбца «Включить в q»).

$$r = \frac{t}{100 - q} \cdot 100 = \frac{90}{100 - 10} \cdot 100 = 100\,\%,$$

где r — HSR;

q — сумма критериев, которая не снижает вероятность опасного отказа для предполагаемой функции безопасности, которую функция безопасности смягчает;

t — сумма остальных применимых критериев, которым удовлетворяет система.

В данном примере системы рулевого управления с планетарным клапаном избыточные размеры, меры противодействия залипанию или вращению золотника, меры противодействия нежелательному гидравлическому входу, вторичный источник энергии, медленное или ступенчатое прогрессирование отказа, смягчение последствий разрыва шланга, система, предназначенная для поддержания требуемой чистоты гидравлической жидкости, и меры противодействия для кавитации, вызванной аэрацией, включаются в показатель t.

Меры по устранению проблем с передачей давления, вызванных аэрацией, включаются в оценку q.

В примере А.6 показано, что $MTTF_d$ этой системы составляет 100 лет.

Согласно таблице 2, HSR = 100, $MTTF_d$ = высокое, соответствует MPL_a = d.

В.2 Пример расчета показателя HSR для гидравлического стояночного тормоза с пружинным включением

Для пружинного гидравлического стояночного тормоза, показанного в А.4, расчет HSR показан в таблице В.2.

Таблица В.2 — Критерии оценки HSR для примера гидравлического стояночного тормоза с пружинным включением

Критерий	Возможные баллы	Баллы системы	Включить в *q* (да/нет)
Избыточный размер (например, достаточный зазор золотника, прямолинейность и цилиндричность)	+10	+10	Нет
Меры противодействия залипанию золотника, прокручиванию	+10	+10	Нет
Меры противодействия нежелательному гидравлическому воздействию (например, мгновенное высокое давление на оба порта гидравлического двигателя)	+10	0	Нет
Вторичный источник энергии (например, с пружинным аккумулятором) или отказоустойчивая конструкция при потере источника энергии	+20	0	Нет
Медленно или ступенчато прогрессирующий отказ (например, уменьшение эффективности усилителя рулевого управления перед опасным отказом)	+10	0	Нет
Снижение вероятности разрыва шлангов (например, отсутствие острых кромок)	+10	+10	Нет
В системе поддерживается необходимая чистота	+10	+10	Нет
Меры противодействия кавитации, вызванной аэрацией гидравлического масла	+10	+10	Нет
Меры по устранению проблем с передачей давления, вызванных аэрацией гидравлического масла (например, вентиляционный контур)	+10	0	Да
Итого баллов		90	

Расчет баллов HSR.

t = 50 (сумма столбца «Оценка системы»).

q = 10 (сумма столбца «Включить в q»).

$$r = \frac{t}{100 - q} \cdot 100 = \frac{50}{100 - 10} \cdot 100 = 56\ \%,$$

где r — HSR;

q — сумма критериев, которая не снижает вероятность опасного отказа для предполагаемой функции безопасности, которую функция безопасности смягчает;

t — сумма остальных применимых критериев, которым удовлетворяет система.

В данном примере гидравлического стояночного тормоза с пружинным приводом избыточные размеры, меры противодействия залипанию или вращению золотника, предотвращение разрыва шланга, система, предназначенная для поддержания требуемой чистоты гидравлической жидкости, и меры противодействия кавитации, вызванной аэрацией, включены в показатель t.

Меры противодействия проблемам с передачей давления, вызванным аэрацией гидравлической жидкости, включаются в показатель q, поскольку они присутствуют в системе, но не способствуют ее безопасности.

Контрмеры для нежелательного гидравлического ввода, вторичного источника энергии и медленного или ступенчатого прогрессирующего отказа в системе отсутствуют, поэтому они не оцениваются.

В примере А.4 показано, что $MTTF_d$ этой системы составляет 100 лет.

Согласно таблице 2, HSR = 56, $MTTF_d$ = высокое, соответствует MPL_a = c.

Приложение С
(обязательное)

Сопоставление с другими стандартами на функциональную безопасность

Чтобы продемонстрировать соответствие стандартам серии ISO 19014, системы, подсистемы и SRP/CS, разработанные и оцененные методами, отличными от стандартов серии ISO 19014, должны отвечать следующим требованиям:

- системы, подсистемы и SRP/CS должны соответствовать требованиям ISO 19014-3;
- PL, AgPL, SIL или ASIL должны считаться эквивалентными MPL, как показано в таблице С.1;
- системы, подсистемы и SRP/CS должны рассматриваться как элементы MPL в соответствии с процессом расчета, описанным в стандартах серии ISO 19014.

Таблица С.1 — MPL_r по сравнению с параметрами других стандартов

Требуемый MPL	Минимальный требуемый уровень			
	PL	AgPL	SIL	ASIL
a	a	a	1	A
b	b	b	1	A
c	c	c	1	B
d	d	d	3	C
e	e	e	4	D

Приложение D
(справочное)

Оценка функции безопасности

Данное приложение предназначено для дополнения информации, представленной в 6.3 (см. рисунок D.1).

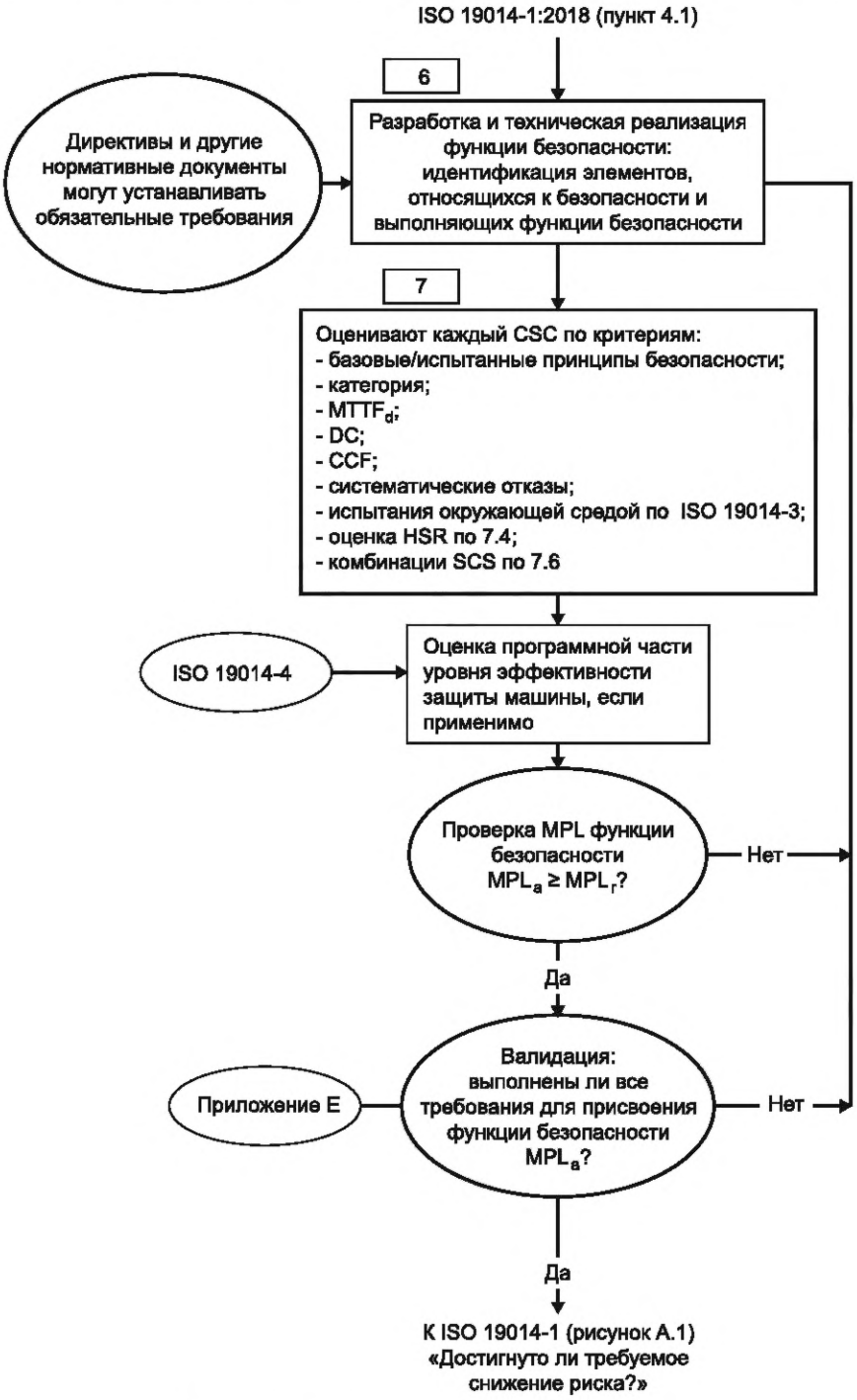


Рисунок D.1 — Оценка функции безопасности

Приложение E
(обязательное)

Исключения и дополнения к ISO 13849-1 и ISO 13849-2

В таблице E.1 показано сравнение приоритетов между ISO 13849-1 и серией стандартов ISO 19014, а в таблице E.2 показано сравнение приоритетов между ISO 13849-2 и серией стандартов ISO 19014.

Буквы в третьем столбце имеют следующее значение:

a — применяются требования серии стандартов ISO 13849;

b — применяются требования серии стандартов ISO 19014;

c — требования серии стандартов ISO 19014 имеют приоритет над требованиями серии стандартов ISO 13849;

d — применяются как требования серии стандартов ISO 19014, так и требования серии стандартов ISO 13849;

e — обычно не применяется к мобильным машинам.

Таблица E.1 — Сравнение приоритетов между ISO 13849-1:2015 и серией стандартов ISO 19014

Элемент стандарта ISO 13849-1:2015	Элемент стандарта ISO 19014-2 или другого стандарта серии ISO 19014	Выбор
Предисловие	Предисловие	b
Введение	Введение	b
1	1	b
2	2	b
3	—	
3.1	3	c
3.2	4	c
—	5	b
—	6	b
4	—	
4.1	ISO 19014 и приложение D	c
4.2	—	
4.2.1	—	a
4.2.2	—	a
4.3	—	a
4.4	—	a
4.5	—	
4.5.1	7.1	c
—	7.1	b
—	7.2.1	b
4.5.2	7.2.4	d
4.5.3	7.3.1	a
—	7.3.2	b
—	7.4	b

Продолжение таблицы Е.1

Элемент стандарта ISO 13849-1:2015	Элемент стандарта ISO 19014-2 или другого стандарта серии ISO 19014	Выбор
4.5.4	7.1	d
4.5.5	7.5.1	c
4.6	—	—
4.6.1	ISO 19014-4	b
4.6.2	ISO 19014-4	b
4.6.3	ISO 19014-4	b
4.6.4	ISO 19014-4	b
4.7	—	a
4.8	—	a
5	—	e
6	—	
6.1	—	a
6.2	—	
6.2.1	—	a
6.2.2	7.5.1	c
6.2.3	—	a
6.2.4	—	a
—	7.5.2.1	b
—	7.5.2.2	b
6.2.5	7.5.3.1	d
—	7.5.3.2	b
—	7.5.3.3	b
6.2.6	—	a
6.2.7	—	a
—	7.5.4	b
—	7.5.5	b
6.3	—	a
—	7.6	b
7	—	
7.1	—	a
7.2	7.2.2	d
7.3	7.2.3	c
8	—	a
9	8	c

Окончание таблицы Е.1

Элемент стандарта ISO 13849-1:2015	Элемент стандарта ISO 19014-2 или другого стандарта серии ISO 19014	Выбор
10	—	a
11	8	b
Приложение A	ISO 19014-1, ISO/TS 19014-5	b
Приложение B	—	e
Приложение C	—	a
Приложение D	—	a
Приложение E	—	a
Приложение F	—	a
Приложение G	—	a
Приложение H	Приложение A	b
Приложение I	Приложение A	b
Приложение J	ISO 19014-4	b
Приложение K	—	a
—	Приложение B	b
—	Приложение C	b
—	Приложение E	b
Библиография	Библиография	c
—	ISO 19014-3	b

Таблица Е.2 — Сравнение приоритетов между ISO 13849-2:2012 и серией стандартов ISO 19014

Элемент стандарта ISO 13849-2:2012	Элемент стандарта ISO 19014-2 или другого стандарта серии ISO 19014	Выбор
Стандарт в целом	—	a

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO 12100:2010	IDT	ГОСТ ISO 12100—2013 «Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска»
ISO 13849-1:2015	—	*
ISO 13849-2:2012	—	*
ISO 19014-1	IDT	ГОСТ ISO 19014-1—2024 «Машины землеройные. Функциональная безопасность. Часть 1. Методика определения элементов систем управления, связанных с обеспечением безопасности, и технические требования»
ISO 19014-3	IDT	ГОСТ ISO 19014-3—2024 «Машины землеройные. Функциональная безопасность. Часть 3. Устойчивость к воздействию окружающей среды и методы испытаний электрических и электронных элементов, используемых в элементах систем управления, связанных с обеспечением безопасности»
ISO 19014-4:2020	IDT	ГОСТ ISO 19014-4—2024 «Машины землеройные. Функциональная безопасность. Часть 4. Разработка и оценка программного обеспечения и передачи данных для элементов систем управления, связанных с обеспечением безопасности»
ISO/TS 19014-5	—	*

* Соответствующий межгосударственный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

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

- IDT — идентичные стандарты.

Библиография

[1] ISO 6165 Earth-moving machinery — Basic types — Identification and terms and definitions

[2] ISO 13850 Safety of machinery — Emergency stop function — Principles for design

[3] ISO 26262-5 Road vehicles — Functional safety — Part 5: Product development at the hardware level

[4] IEC 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

УДК 631.3:006.354 МКС 53.100 IDT

Ключевые слова: машины землеройные, проектирование и оценка оборудования и структуры систем управления, связанных с обеспечением безопасности

Редактор *Е.Ю. Митрофанова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 02.10.2024. Подписано в печать 08.10.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,25.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru gost.e-ecolog.ru