ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72308— 2025/ IEC TS 63394:2023

Безопасность оборудования

РУКОВОДСТВО ПО ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ, СВЯЗАННОЙ С БЕЗОПАСНОСТЬЮ

(IEC TS 63394:2023, IDT)

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») и Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 058 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 сентября 2025 г. № 1129-ст

4 Настоящий стандарт идентичен международному документу IEC TS 63394:2023 «Безопасность оборудования. Руководство по функциональной безопасности системы управления, связанной с безопасностью» (IEC TS 63394:2023 «Safety of machinery — Guidelines on functional safety of safety-related control system», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© IEC, 2023
© Оформление. ФГБУ «Институт стандартизации», 2025

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 2
3 Термины и определения 2
3.1 Термины и определения 2
3.2 Алфавитный список терминов, определений и сокращений 12
4 Типовая классификация функций безопасности в области безопасности машин и механизмов 14
4.1 Общие положения 14
4.2 Основные допущения по безопасности для проектирования и интеграции SCS или SRP/CS . . . 15
4.3 Функции безопасности 16
4.4 Взаимосвязь между ИСО 12100 и МЭК 62061 или ИСО 13849-1 18
4.5 Функции безопасности для защиты людей 19
4.6 Прочие функции безопасности для предотвращения опасных ситуаций 20
4.7 Функции безопасности для обеспечения полноты безопасности машины 21
4.8 Функции безопасности и стандарты типа С 21
5 Режим работы по запросу, связанный с функциями безопасности 22
5.1 Общие положения 22
5.2 Режим работы с высокой частотой запросов или с непрерывными запросами 23
5.3 Режим работы с низкой частотой запросов 25
6 Процесс проектирования функций безопасности 25
6.1 Общие положения 25
6.2 Процедура проектирования 26
6.3 Оценка требуемой полноты безопасности 26
6.4 Декомпозиция функции безопасности 26
6.5 Проектирование подсистем 26
6.6 Примеры функций безопасности 29
7 Процедуры верификации функций безопасности 29
7.1 Общие положения 29
7.2 Верификация интервала диагностических проверок функции безопасности 29
7.3 Процедуры верификации 29
7.4 Начальная верификация 30
7.5 Периодическая верификация 31
7.6 Отчеты о верификации 32
Приложение А (справочное) Оценка рисков и снижение рисков в соответствии с ИСО 12100 33
Приложение В (справочное) Методология проектирования SCS или SRP/CS 45
Приложение С (справочное) Примеры значений $MTTF_D$ для отдельных компонентов 60
Приложение D (справочное) Примеры охвата диагностикой (DC) 61
Приложение Е (справочное) Меры достижения функциональной безопасности в отношении электромагнитных явлений 65
Приложение F (справочное) Руководство по программному обеспечению 67
Приложение G (справочное) Примеры функций безопасности 73
Приложение Н (справочное) Оценка значения PFH подсистемы 77
Приложение I (справочное) Примеры действующих норм с комментариями 97
Приложение J (справочное) Комбинация режимов работы 100
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов межгосударственным и национальным стандартам 106
Библиография 107

Введение

В контексте безопасности машин базовый стандарт МЭК 62061 вместе с ИСО 13849-1 для изготовителей машин содержит требования и рекомендации по проектированию, разработке и интеграции систем управления, связанных с безопасностью (SCS) или связанных с безопасностью частей систем управления (SRP/CS) соответственно, включая устройства ввода и исполнительные устройства независимо от технологии (механической, пневматической, гидравлической и электрической).

Актуальны следующие аспекты:

- классификация функций безопасности,
- архитектура реализации функций безопасности,
- режимы работы функций безопасности,
- расчеты, основанные на используемой технологии.

Таким образом, функции безопасности можно классифицировать следующим образом:

- функции безопасности, которые останавливают опасное(ые) движение(я) машины и которые в основном выполняются SCS или SRP/CS машин для защиты людей. Типичными примерами являются блокировочные устройства для ограждений, чувствительное защитное оборудование, двуручные системы управления и системы аварийного останова;
- функции безопасности, которые защищают целостность машины от ее разрушения и которые на втором этапе могут повлиять на защиту людей. Типичными примерами являются защитные устройства, устройства для ограничения давления или температуры (также определяемые как параметры, связанные с безопасностью, например положение, скорость, температура или давление, отклоняющиеся от пределов, определенных в системе управления;
- другие функции безопасности, не охваченные двумя предыдущими случаями.

Примечание 1 — Определены различные виды функций безопасности, которые соответствуют классификациям и определениям ИСО 12100 и ИСО 13849-1.

Рассмотрены архитектуры подсистем для выполнения функций безопасности.

Примечание 2 — В МЭК 62061:2021 представлена информация для сопоставления классификации SIL (уровня полноты безопасности) по МЭК 62061/МЭК 61508 и классификации по ИСО 13849-1 с точки зрения категорий, архитектур, специальных архитектур и PL (уровня эффективности защиты). В настоящем стандарте рассматриваются эти различные критерии, чтобы обеспечить обратную совместимость.

В зависимости от режима работы функции безопасности будут учтены критерии и расчеты для выполнения требований настоящего стандарта, действующих норм (например, таких как рекомендации по использованию в Европе) и других уже существующих требований, определенных в существующих стандартах, например, по периодичности испытаний.

Чтобы рассмотреть механические, пневматические, гидравлические и электрические технологии, применение функций безопасности, архитектуру и режим работы, выполняются соответствующие расчеты.

Примечание 3 — Например, большинство расчетов в стандартах основано на экспоненциальном законе, который, как правило, применим к электронной технологии. Для механических или других технологий применяется распределение Вейбулла, а экспоненциальное распределение не используется, за исключением ограничений.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность оборудования

РУКОВОДСТВО ПО ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ, СВЯЗАННОЙ С БЕЗОПАСНОСТЬЮ

Safety of machinery. Guidelines on functional safety of safety-related control system

Дата введения — 2026—01—01

1 Область применения

В контексте безопасности машин базовый стандарт МЭК 62061 вместе с ИСО 13849-1 для изготовителей машин содержит требования и рекомендации по проектированию, разработке и интеграции систем управления, связанных с безопасностью (SCS) или связанных с безопасностью частей систем управления (SRP/CS), в зависимости от используемой технологии (механической, пневматической, гидравлической или электрической) для выполнения функций безопасности. Настоящий стандарт не заменяет ИСО 13849-1 и МЭК 62061, а устанавливает дополнительные рекомендации по применению МЭК 62061 или ИСО 13849-1. Настоящий стандарт:

- содержит рекомендации и определяет дополнительные требования к конкретным функциям безопасности на основе методологии ИСО 12100, которые применимы к машинам и удовлетворяют типичным граничным условиям машин;
- рассматривает функции безопасности, которые предназначены для режима работы с высокой частотой запросов, но используются редко и называются редко активируемыми функциями безопасности.

Примечание 1 — МЭК 62061:2021 полностью охватывает режим работы с высокой частотой запросов. Однако другие функции безопасности, связанные с защитой самой машины и косвенно с защитой людей, в настоящем стандарте рассматриваются более подробно;

- предоставляет дополнительную информацию для расчета интенсивности отказов при использовании других (неэлектронных) технологий, основанных, например, на распределении Вейбулла, поскольку все формулы, определенные в МЭК 62061 и ИСО 13849-1, используют экспоненциальное распределение.

Таким образом, рекомендации и дополнительные требования включают:

- типовую классификацию функций безопасности;
- рассмотрение типичных архитектур, используемых для проектирования функций безопасности;
- рассмотрение режимов работы функций безопасности;
- вывод и оценку формул PFH для подсистем с учетом используемой технологии.

Примечание 2 — Эти рекомендации также можно использовать для применения ИСО 13849-1 в процессе проектирования SRP/CS.

В настоящем стандарте не рассматривается режим работы с низким энергопотреблением в соответствии с МЭК 61508.

В настоящем стандарте не рассматриваются ни анализ слоев защиты (LOPA), ни базовая система управления процессом (BPCS) согласно МЭК 61511 в качестве меры снижения риска.

В настоящем стандарте рассмотрены все этапы жизненного цикла машины для обеспечения функциональной безопасности, а также SCS или SRP/CS.

Примечание 3 — Пользователю машины необходима информация от ее изготовителя для безопасной эксплуатации машины, например срок эксплуатации компонентов, информация по техническому обслуживанию, тестирование функций безопасности при необходимости.

Издание официальное

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)]:

IEC 62061:2021, Safety of machinery — Functional safety of safety-related control systems (Безопасность машин. Функциональная безопасность электрических, электронных и программируемых электронных систем управления, связанных с безопасностью)

IEC TR 63074:2019[1)], Safety of machinery — Security aspects related to functional safety of safety-related control systems (Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности)

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

ISO 13849-1:2015[2)], Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design (Безопасность машин. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования)

ISO 13850:2015, Safety of machinery — Emergency stop function — Principles for design (Безопасность машин. Аварийный останов. Принципы проектирования)

ISO 13851:2019, Safety of machinery — Two-hand control devices — Principles for design and selection (Безопасность машин. Двуручные устройства управления. Принципы проектирования и выбора)

ISO 14118:2017, Safety of machinery — Prevention of unexpected start-up (Безопасность машин. Предупреждение неожиданных пусков)

ISO 14119:2013[3)], Safety of machinery — Interlocking devices associated with guards — Principles for design and selection (Безопасность машин. Блокировочные устройства для ограждений. Принципы конструкции и выбора)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных, используемые в целях стандартизации по следующим адресам:

- платформа онлайн-просмотра ИСО: доступна по адресу gost.e-ecolog.ru
- Электропедия МЭК: доступна по адресу gost.e-ecolog.ru

3.1 Термины и определения

3.1.1 **прикладное программное обеспечение** (application software): Определенное для применения программное обеспечение, реализованное разработчиком SCS или SRP/CS, как правило, содержащее последовательность логических операций, ограничения и выражения и управляющее соответствующей входящей и исходящей информацией, вычислениями и решениями, удовлетворяющими функциональные требования SCS или SRP/CS.

[МЭК 62061:2021, пункт 3.2.59, изменено — к определению добавлено «или SRP/CS»]

3.1.2 **архитектурное ограничение** (architecture constraint): Набор требований к архитектуре, ограничивающих SIL, который может быть востребован для подсистемы.

[МЭК 62061:2021, пункт 3.2.46]

3.1.3 **архитектура** (architecture): Конкретная конфигурация элементов аппаратных средств и программного обеспечения SCS или SRP/CS.

[МЭК 61508-4:2010, пункт 3.3.4, изменено — терминология адаптирована к машинному оборудованию]

3.1.4 **средняя частота опасного отказа в час;** PFH (average frequency of a dangerous failure per hour, PFH): Средняя частота опасного отказа SCS или SRP/CS, выполняющей указанную функцию безопасности в течение заданного периода времени.

[1)] Заменен на IEC/TS 63074:2023. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[2)] Заменен на ISO 13849-1:2023. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[3)] Заменен на ISO 14119:2024. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

Примечание 1 — Термин PFH соответствует вероятности опасных отказов в час (PFH_D) в соответствии с МЭК 62061:2005, МЭК 62061:2005/AMD1:2012 и МЭК 62061:2005/AMD2:2015.

Примечание 2 — Термин «средняя вероятность опасного отказа в час» PFH_D используется в ИСО 13894-1 и может считаться идентичным PFH в соответствии с комплексом стандартов МЭК 61508.

[МЭК 61508-4:2010, пункт 3.6.19, изменено — терминология адаптирована к машинному оборудованию, существующие примечания удалены, добавлены новые примечания]

3.1.5 **отказ по общей причине;** CCF (common cause failure, CCF): Отказ, являющийся результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной системе, ведущих к отказу функции безопасности.

[МЭК 61508-4:2010, пункт 3.6.10, изменено — добавлено сокращение, словосочетание «отказу системы» заменено на «отказу функции безопасности»]

3.1.6 **управление конфигурацией** (configuration management): Дисциплина идентификации компонентов примененных систем для осуществления контролируемых изменений этих компонентов и поддержания преемственности и прослеживания на протяжении всего жизненного цикла.

[МЭК 61508-4:2010, пункт 3.7.3, изменено — удалено примечание]

3.1.7 **непрерывный режим работы** (continuous mode of operation): Режим работы, в котором функция безопасности поддерживает машинное оборудование в безопасном состоянии, как и при нормальном функционировании.

Примечание 1 — Непрерывный режим означает, что функция безопасности выполняется непрерывно, то есть SCS непрерывно управляет машиной, и (опасный) отказ ее функции может привести к опасности.

Примечание 2 — Различие между непрерывным режимом работы и режимом с высокой частотой запросов связано с квалификацией диагностических мер (см. МЭК 62061:2021, пункты 7.4.3 и 7.4.4) и не связано с целевой мерой отказа и определением SIL.

[МЭК 61508-4:2010, пункт 3.5.16, изменено — определение к термину «непрерывный режим работы» взято из более широкого определения «режим работы», добавлены примечания]

3.1.8 **опасный отказ** (dangerous failure): Отказ SCS или SRP/CS, подсистемы или элемента подсистемы, влияющий на выполнение функции безопасности:

a) препятствует выполнению функции безопасности, если необходимо ее выполнение (в режиме запроса), или вызывает прекращение выполнения функции безопасности (в непрерывном режиме), переводя машинное оборудование в опасное или потенциально опасное состояние, или

b) снижает вероятность корректного выполнения функции безопасности, если необходимо ее выполнение.

[МЭК 61508-4:2010, пункт 3.6.7, изменено — терминология адаптирована к машинному оборудованию]

3.1.9 **запрос** (demand): Событие, которое инициирует SCS или SRP/CS выполнять свою функцию безопасности.

Примечание 1 — Режим работы по запросу означает, что функция безопасности выполняется только по требованию (запросу), чтобы перевести машину в указанное состояние. SCS или SRP/CS не влияют на работу машины, пока не возникнет потребность в функции безопасности.

Примечание 2 — Интенсивность запросов (DR) или частота запросов является одним из основных факторов, который учитывается при оценке режима работы по запросу, низкого или высокого. Для данной цели интенсивность запросов (DR) может быть связана с интенсивностью событий, при которых может быть нанесен вред без вмешательства функции безопасности. Эта интенсивность может быть ниже, чем фактическая скорость запуска функции безопасности в процессе эксплуатации.

Примечание 3 — Для функции аварийного останова режим запросов не определен. Для определения значения SIL, как правило, применяется принцип оценки выбранного режима запросов для других функций.

[МЭК 62061:2021, пункт 3.2.25, изменено — добавлено «или SRP/CS»]

3.1.10 **охват диагностикой;** DC (diagnostic coverage, DC): Доля опасных отказов, выявляемая автоматическими диагностическими проверками в неавтономном режиме.

Примечание 1 — Доля опасных отказов рассчитывается как отношение интенсивности опасных отказов, связанных с выявленными опасными отказами, к общей интенсивности опасных отказов.

Примечание 2 — Охват диагностикой опасных отказов рассчитывается с использованием следующего уравнения, где DC — охват диагностикой, λ_{DD} — интенсивность выявленных опасных отказов, а λ_{Dtotal} — общая частота опасных отказов:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}. \quad (1)$$

Примечание 3 — Данное определение справедливо при условии, что рассматриваемые компоненты имеют постоянную интенсивность отказов.

[МЭК 61508-4:2010, пункт 3.8.6, изменено — вторая часть определения была перенесена в примечание]

3.1.11 **функция диагностики** (diagnostic function): Функция, предназначенная для обнаружения отказов в SCS или SRP/CS и формирования заданной выходной информации при обнаружении сбоя.

Примечание 1 — Данная функция предназначена для обнаружения сбоев, которые могут привести к опасному отказу функции безопасности и запуску заданной функции реакции на сбой.

[МЭК 62061:2021, пункт 3.2.19, изменено — добавлено «или SRP/CS»]

3.1.12 **интервал диагностических проверок** (diagnostic test interval): Интервал между неавтономными проверками, предназначенными для обнаружения отказов в подсистеме с заданным охватом диагностикой.

[МЭК 61508-4:2010, пункт 3.8.7, изменено — словосочетание «системах, связанных с безопасностью» заменено на «подсистеме»]

3.1.13 **встроенное программное обеспечение** (embedded software): Программное обеспечение, поставляемое как часть предварительно разработанной подсистемы, которое недоступно для модификации и которое обеспечивает функционирование и услуги, предоставляемые SCS, или SRP/CS, или подсистемой, в отличие от прикладного программного обеспечения.

Примечание 1 — Программное обеспечение программируемой электроники, а также системное программное обеспечение — примеры встроенного программного обеспечения.

[МЭК 62061:2021, пункт 3.2.60, изменено — добавлено «или SRP/CS»]

3.1.14 **отказ** (failure): Прекращение способности устройства (SCS или SRP/CS, подсистемы или элемента подсистемы) выполнять требуемую функцию.

Примечание 1 — Отказы являются либо случайными (в технических средствах), либо систематическими (в технических средствах или программном обеспечении).

Примечание 2 — Отказ устройства приводит к сбою в его работе.

Примечание 3 — «Отказ» — событие, в отличие от «сбоя», являющееся состоянием.

Примечание 4 — Рассматриваемое понятие не распространяется на программное обеспечение.

[ИСО 12100:2010, пункт 3.34, изменено — добавлены «(SCS или SRP/CS, подсистема или элемент подсистемы)» и примечание 1]

3.1.15 **сбой** (fault): Ненормальный режим, который может вызвать снижение или потерю способности SCS или SRP/CS, подсистемы или элемента подсистемы выполнять требуемую функцию.

Примечание 1 — В МЭК 60050-192:2015, пункт 192-04-01, сбой устройства описывается как неспособность выполнять необходимую функцию в соответствии с требованиями из-за внутреннего состояния.

[МЭК 61508-4:2010, пункт 3.6.1, изменено — терминология адаптирована к машинному оборудованию, сокращено примечание]

3.1.16 **функция реакции на сбой** (fault reaction function): Функция, которая запускается, когда в SCS или SRP/CS обнаружен сбой с помощью функции диагностики SCS или SRP/CS.

[МЭК 62061:2021, пункт 3.2.20, изменено — к определению добавлено «или SRP/CS»]

3.1.17 **устойчивость к отказам** (fault tolerance): Способность SCS или SRP/CS, подсистемы или элемента подсистемы продолжать выполнять необходимую функцию при наличии сбоев или отказов.

[МЭК 61508-4:2010, пункт 3.6.3, изменено — терминология адаптирована к машинному оборудованию, примечание удалено]

3.1.18 **язык программирования с полной изменчивостью; ЯПИ** (full variability language; FVL): Тип языка, предоставляющий возможность реализовать широкий диапазон функций и прикладных задач.

Примечание 1 — Типичными примерами систем, использующих ЯПИ, являются компьютеры общего назначения.

Примечание 2 — Как правило, ЯПИ используется во встроенном программном обеспечении и реже — в прикладном.

Примечание 3 — Примерами ЯПИ являются Ada, C, Pascal, список инструкций, языки ассемблера, C++, Java, SQL.

[МЭК 61511-1:2016, пункт 3.2.75.3, изменено — удалены первая часть определения и связь с перерабатывающей промышленностью]

3.1.19 **функциональная безопасность** (functional safety): Часть общей безопасности, обусловленная применением машины и системы управления машиной и зависящая от правильности функционирования SCS или SRP/CS и других средств по снижению риска.

[МЭК 61508-4:2010, пункт 3.1.12, изменено — использованы термины «машина», «система управления машиной», «SCS и SRP/CS»]

3.1.20 **отказоустойчивость аппаратных средств;** HFT (hardware fault tolerance, HFT): Свойство подсистемы, приводящее к возможной потере функции безопасности при как минимум *N* + 1 сбоях.

Примечание 1 — Отказоустойчивость аппаратных средств *N* означает, что *N* + 1 сбоев подсистемы могут привести к потере функции безопасности.

[МЭК 62061:2021, пункт 3.2.35]

3.1.21 **полнота безопасности аппаратных средств** (hardware safety integrity): Составляющая полноты безопасности SCS или ее подсистем, связанная со случайными отказами аппаратных средств, проявляющихся в опасном режиме.

Примечание 1 — Данный термин относится к отказам, проявляющимся в опасном режиме, т. е. к тем отказам системы, связанной с безопасностью, которые могут ухудшить полноту ее безопасности.

Примечание 2 — Полнота безопасности аппаратных средств включает в себя архитектурные ограничения.

[МЭК 61508-4:2010, пункт 3.5.7, изменено — терминология адаптирована к машинному оборудованию, примечание 1 сокращено, примечание 2 добавлено]

3.1.22 **вред** (harm): Нанесение физической травмы или причинение вреда здоровью человека.

[ИСО 12100:2010, пункт 3.5]

3.1.23 **опасность** (hazard): Потенциальный источник угрозы.

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

Примечание 2 — Виды опасностей:

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

Примечание 3 — Французский термин «phénomène dangereux» не следует путать с термином «risque», который раньше иногда использовался вместо него.

[ИСО 12100:2010, пункт 3.6]

3.1.24 **опасная ситуация** (hazardous situation): Обстоятельства, при которых люди подвергаются одной или нескольким опасностям.

Примечание 1 — Воздействие обстоятельств может привести к причинению вреда немедленно или в течение определенного периода времени.

[ИСО 12100:2010, пункт 3.10]

3.1.25 **опасная зона** (hazard zone, danger zone): Любое пространство внутри машины или вокруг нее, в котором человек может подвергаться опасности.

[ИСО 12100:2010, пункт 3.11]

3.1.26 **режим работы с высокой частотой запросов** (high demand mode of operation): Режим работы, при котором частота запросов функции безопасности превышает одного в год.

Примечание 1 — Непрерывный режим означает, что функция безопасности выполняется непрерывно, то есть SCS непрерывно управляет машиной, и (опасный) отказ ее функции может привести к опасности.

Примечание 2 — Различие между непрерывным режимом работы и режимом с высокой частотой запросов связано с квалификацией диагностических мер (см. МЭК 62061:2021, пункты 7.4.3 и 7.4.4) и не связано с целевой мерой отказа и определением SIL.

[МЭК 61508-4:2010, пункт 3.5.16, изменено — определение «режим работы с высокой частотой запросов» взято из более широкого определения «режим работы», добавлены примечания]

3.1.27 **язык с ограниченной изменчивостью;** LVL (limited variability language, LVL): Тип языка, который предоставляет возможность комбинировать предопределенные, ориентированные на приложение библиотечные функции для реализации спецификаций требований к безопасности.

Примечание 1 — LVL обеспечивает тесное функциональное соответствие с функциями, необходимыми для реализации приложения.

Примечание 2 — Типичные примеры LVL приведены в МЭК 61131-3. Они включают в себя язык лестничных диаграмм, язык функциональных блоков и язык последовательных функциональных схем. Перечень инструкций и структурированный текст не считаются LVL.

Примечание 3 — Типичный пример систем, использующих LVL: программируемый логический контроллер (PLC), настроенный для управления машиной.

3.1.28 **режим работы с низкой частотой запросов** (low demand mode of operation): Режим работы, при котором частота запросов функции безопасности не превышает одного в год.

[МЭК 61508-4:2010, пункт 3.5.16, изменено — определение «режим работы с низкой частотой запросов» взято из более широкого определения «режим работы»]

3.1.29 **машина (оборудование)** (machine, machinery): Агрегат, оборудованный системой привода или предназначенный для установки системы привода, состоящий из связанных деталей или компонентов, по крайней мере один из которых двигается, и соединенных вместе для конкретного применения.

Примечание 1 — Термин «оборудование» распространяется также на совокупность машин, которые для достижения конкретной цели компонуются и управляются таким образом, чтобы функционировать как единое целое.

[ИСО 12100:2010, пункт 3.1, изменено — примечание 2 исключено]

3.1.30 **система управления машиной;** MCS (machine control system, MCS): Система, реагирующая на входные сигналы, поступающие от оборудования и/или от оператора, и генерирующая выходные сигналы, которые заставляют управляемое оборудование работать в необходимом режиме.

Примечание 1 — Система управления машиной включает в себя устройства ввода и исполнительные элементы.

[МЭК 61508-4:2010, пункт 3.3.3, изменено — изменен определяемый термин, слово «процесс» было изменено на «оборудование»]

3.1.31 **средняя продолжительность ремонта;** MRT (mean repair time, MRT): Ожидаемая полная продолжительность ремонта от обнаружения неисправности в функции безопасности и до продолжения работы машины.

Примечание 1 — MRT включает в себя:
- время, прошедшее до начала восстановления;
- время, фактически затраченное на ремонт;
- время возвращения компонента в работу.

Примечание 2 — В зависимости от типа обнаруженного сбоя и реакции на сбой числовые значения для MRT и MTTR могут быть разными.

[МЭК 61508-4:2010, пункт 3.6.22, изменено — терминология адаптирована к машинному оборудованию, к определению добавлена более подробная информация, примечание 1 аналогично МЭК 62061:2021, пункт 3.2.39, добавлено примечание 2]

3.1.32 **среднее время наработки на отказ;** MTTF (mean time to failure, MTTF): Среднее значение времени ожидания до отказа.

[МЭК 60050-192, пункт 192-05-11, изменено — из термина исключено слово «эксплуатация», добавлены слова «среднее значение», а оригинальные примечания исключены]

3.1.33 **среднее время работы до опасного отказа;** $MTTF_D$ (mean time to dangerous failure, $MTTF_D$): Ожидаемое среднее время до опасного отказа.

Примечание 1 — Определение, заимствованное из МЭК 60050-192:2015, 192-05-11, но ограниченное опасными отказами.

3.1.34 **среднее время восстановления;** MTTR (mean time to restoration, MTTR): Ожидаемое время восстановления после сбоя функции безопасности.

Примечание 1 — MTTR включает в себя:
a) время выявления отказа;
b) время, прошедшее до начала восстановления;
c) время, фактически затраченное на ремонт;
d) время возвращения компонента в работу.

Начало времени перечисления b) совпадает с окончанием времени перечисления a); начало времени перечисления c) совпадает с окончанием времени перечисления b); начало времени перечисления d) совпадает с окончанием времени перечисления c).

[МЭК 61508-4:2010, пункт 3.6.21, изменено — терминология адаптирована к машинному оборудованию и к определению добавлена более подробная информация]

3.1.35 **предварительно спроектированная SCS или подсистема** (pre-designed SCS or subsystem): SCS или подсистема, отвечающая соответствующим требованиям стандарта функциональной безопасности.

[МЭК 62061:2021, пункт 3.2.5]

3.1.36 **вероятность опасного отказа по запросу;** PFD (probability of dangerous failure on demand, PFD): Неготовность SCS или SRP/CS обеспечить безопасность (см. МЭК 60050-192), т. е. выполнить указанную функцию безопасности, когда происходит запрос от оборудования или системы управления оборудования.

Примечание 1 — [Мгновенная] неготовность (согласно МЭК 60050-192) является вероятностью ненахождения устройства в состоянии выполнения необходимой функции при данных условиях в данный момент времени; предполагается, что элемент обеспечен всеми необходимыми внешними ресурсами. Как правило [мгновенную], неготовность обозначают как $U(t)$.

Примечание 2 — [Мгновенная] готовность не зависит от состояний (выполнения или отказа), в которых находилось устройство до момента времени t. Она только характеризует устройство, которое должно быть в работоспособном состоянии, когда это необходимо, например SCS, работающая в режиме с низкой интенсивностью запросов.

Примечание 3 — Если происходит периодическое тестирование, то PFD SCS для заданной функции безопасности представляется в виде зубчатой кривой с большим диапазоном значений вероятностей от низкого значения сразу после теста, до максимального непосредственно перед тестом.

[МЭК 61508-4:2010, пункт 3.6.17, изменено — терминология адаптирована к машинному оборудованию]

3.1.37 **время безопасности процесса** (process safety time): Промежуток времени между моментом появления отказа, имеющего возможность дать начало опасному событию в оборудовании или системе управления оборудования, и моментом времени, к которому в оборудовании должно быть завершено действие по предотвращению появления опасного события.

Примечание 1 — Предполагается, что функция безопасности обнаруживает отказ и завершает свое действие достаточно быстро, чтобы предотвратить опасное событие с учетом любой задержки процесса (например, времени остановки).

[МЭК 61508-4:2010, пункт 3.6.20, изменено — терминология адаптирована к машинному оборудованию, добавлено примечание 1]

3.1.38 **контрольная проверка** (proof test): Периодическая проверка, проводимая для того, чтобы обнаружить опасные скрытые отказы или ухудшение характеристик в SCS или SRP/CS и ее подсистемах, чтобы при необходимости части SCS или SRP/CS и ее подсистем могли быть восстановлены настолько близко к «исходному» состоянию, насколько это возможно в данных условиях.

Примечание 1 — Контрольная проверка предназначена для подтверждения того, что соответствующие части SCS или SRP/CS находятся в состоянии, которое обеспечивает заданную полноту безопасности.

Примечание 2 — Эффективность контрольных проверок будет зависеть как от охвата отказов тестами, так и от эффективности ремонта. На практике обнаружить 100 % ухудшенных характеристик, которые в дальнейшем могут привести к скрытым опасным отказам, непросто. Для сложных элементов или характеристик безопасности, которые трудно проверить, 100 %-ный охват контрольными проверками, как правило, невозможен.

[МЭК 61508-4:2010, пункт 3.8.5, изменено — терминология адаптирована к машинному оборудованию, примечания 1, 3 и 4 исключены, добавлено новое примечание 1 и сокращено примечание 2]

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

[ИСО 12100:2010, пункт 3.19, изменено — исключены перечисления]

3.1.40 **случайный отказ аппаратных средств** (random hardware failure): Отказ, возникающий в случайный момент времени, который является результатом одного или нескольких возможных механизмов ухудшения характеристик в аппаратных средствах.

[МЭК 61508-4:2010, пункт 3.6.5, изменено — исключены примечания]

3.1.41 **редко активируемая функция безопасности** (rarely activated safety function): Функция безопасности, предназначенная для режима работы с высокой частотой запросов, когда предполагается, что частота запросов составляет не менее одного раза в год, но иногда может быть менее одного раза в год.

Примечание 1 — При оценке режима работы по запросу предполагается, что частота запросов составляет не менее одного раза в год. Тем не менее, не исключено, что функция безопасности не будет запрошена в течение одного года. Термин «редко активируемая функция безопасности» отражает это особое обстоятельство.

3.1.42 **доля опасных отказов;** RDF (ratio of dangerous failure, RDF): Доля от общей интенсивности отказов элемента, которая может привести к опасному отказу.

[МЭК 62061:2021, пункт 3.2.55]

3.1.43 **риск** (risk): Сочетание вероятности события причинения вреда и тяжести этого вреда.

[Руководство ИСО/МЭК 51:2014, пункт 3.9, изменено — исключено примечание]

3.1.44 **безопасный отказ** (safe failure): Отказ SCS или SRP/CS, подсистемы или элемента подсистемы, играющий определенную роль в реализации функции безопасности, который:

a) приводит к ложному выполнению функции безопасности, переводящей машину (или ее часть) в безопасное состояние или поддерживающей безопасное состояние; или

b) увеличивает вероятность ложного выполнения функции безопасности, переводящей машину (или ее часть) в безопасное состояние или поддерживающей безопасное состояние.

[МЭК 61508-4:2010, пункт 3.6.8, изменено — терминология адаптирована к машинному оборудованию]

3.1.45 **доля безопасных отказов;** SFF (safe failure fraction, SFF): Доля общей интенсивности отказов подсистемы, которые не приводят к опасному отказу.

Примечание 1 — Диагностический охват (при наличии) каждой подсистемы в SCS учитывается при расчете вероятности случайных отказов аппаратных средств. Доля безопасных отказов учитывается при определении влияния архитектурных ограничений на полноту безопасности аппаратных средств обеспечения (см. МЭК 62061:2021, пункт 7.4).

Примечание 2 — «Невлияющий отказ» и «пустой отказ» (см. МЭК 61508-4) не используется для расчетов SFF.

[МЭК 62061:2021, пункт 3.2.54, изменено — сокращение «SFF» было отформатировано как неизменяющийся термин]

3.1.46 **безопасное состояние** (safe state): Состояние машины при достижении безопасности.

Примечание 1 — Безопасное состояние не включает восстановление первоначальных отказов оборудования.

Примечание 2 — МЭК 62061 рассматривает «функцию реакции на сбой» в контексте «безопасного состояния» машины. Для HFT = 0 и SFF < 60 %, если при обнаружении опасного отказа невозможно достичь «безопасного состояния», то для информирования пользователя, подверженного риску, может быть достаточно предупреждений (или аварийных сигналов).

[МЭК 62061:2021, пункт 3.2.68, изменено — добавлено примечание 2]

3.1.47 **безопасность** (safety): Отсутствие неприемлемого риска.

[МЭК 61508-4:2010, пункт 3.1.11]

3.1.48 **функция безопасности** (safety function): Функция, реализуемая SCS или SRP/CS с заданным уровнем полноты, предназначенная для поддержания безопасного состояния машины или предотвращения немедленного увеличения риска(ов) по отношению к конкретному опасному событию.

Примечание 1 — Этот термин используется вместо термина «функция управления, связанная с безопасностью (SRCF)», из МЭК 62061:2015. Определение отличается от ИСО 12100, т. к. в настоящем стандарте рассматривается снижение риска, выполняемое SCS или SRP/CS.

Примечание 2 — Функция безопасности, как правило, начинается с обнаружения и оценки «инициирующего события» и заканчивается выходом, вызывающим реакцию «исполнительного механизма машины».

Примечание 3 — Части функции(й) работы машины, например реакция исполнительного механизма машины, также могут быть частью функции(й) безопасности.

[МЭК 61508-4:2010, пункт 3.5.1, изменено — терминология адаптирована к машинному оборудованию, исключены другие меры по снижению риска, исключен пример, добавлены примечания]

3.1.49 **полнота безопасности** (safety integrity): Вероятность того, что SCS или SRP/CS, или ее подсистема будут удовлетворительно выполнять требуемую функцию безопасности при всех оговоренных условиях в течение заданного интервала времени.

Примечание 1 — Чем выше уровень полноты безопасности устройства, тем ниже вероятность того, что это устройство не сможет выполнить требуемую функцию безопасности.

Примечание 2 — Полнота безопасности включает в себя полноту безопасности аппаратных средств и полноту безопасности по отношению к систематическим отказам.

[МЭК 61508-4:2010, пункт 3.5.4, изменено — терминология адаптирована к машинному оборудованию, примечания 2, 3 и 5 исключены]

3.1.50 **уровень полноты безопасности;** SIL (safety integrity level, SIL): Дискретный уровень (один из возможных трех), описывающий способность выполнять функцию безопасности, где уровень 3 является высшим уровнем полноты безопасности, а уровень 1 — низшим.

[МЭК 62061:2021, пункт 3.2.24]

3.1.51 **система управления, связанная с безопасностью;** SCS (safety-related control system, SCS): Часть системы управления машины, которая реализует функцию безопасности, используя одну или несколько подсистем.

[МЭК 62061:2021, пункт 3.2.3]

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

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

[ИСО 13849-1:2015, пункт 3.1.1]

3.1.53 **программное обеспечение, связанное с безопасностью** (safety-related software): Программное обеспечение, которое используется для реализации функций безопасности в системе, связанной с безопасностью.

[МЭК 62061:2021, пункт 3.2.63]

3.1.54 **защита информации** (security):

a) меры, предпринимаемые для защиты системы;

b) состояние системы, которое является результатом разработки и проведения мер защиты системы;

c) состояние ресурсов системы, которые защищены от несанкционированного доступа к ним и несанкционированного или случайного их изменения, уничтожения, а также утери;

d) возможность компьютерной системы гарантировать в достаточной степени, что неавторизованные лица и системы не смогут ни видоизменять программное обеспечение и данные о нем, ни получать доступ к функциям системы, но в то же время гарантировать, что это возможно для авторизованных лиц и систем;

e) предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля.

Примечание 1 — Указанные меры могут представлять собой меры защиты, относящиеся к физической безопасности (управление физическим доступом к вычислительным объектам), или логической защиты информации (возможность входа в конкретную систему и приложение).

[IEC TS 62443-1-1:2009, пункт 3.2.99]

3.1.55 **подфункция** (sub-function): Часть функции безопасности, отказ которой может привести к отказу функции безопасности.

[МЭК 62061:2021, пункт 3.2.36, изменено — исключено примечание]

3.1.56 **подсистема** (subsystem): Объект высокоуровневого проектирования архитектуры системы, связанной с безопасностью, в котором опасный отказ подсистемы приводит к опасному отказу функции безопасности.

Примечание 1 — Это определение отличается от общеизвестного, где «подсистема» может означать любую подчасть сущности; термин «подсистема» используется в настоящем стандарте в рамках строго определенной терминологической иерархии: «подсистема» — это элемент первого уровня деления системы. Части, возникающие в результате дальнейшего разделения подсистемы, называются «элементами подсистемы».

Примечание 2 — Полная подсистема может состоять из нескольких идентифицируемых и отдельных элементов подсистемы.

Примечание 3 — Спецификация подсистемы включает ее роль в функции безопасности и ее взаимодействие с другими подсистемами SCS.

Примечание 4 — Одна подсистема может быть частью нескольких функций безопасности, например, одна и та же комбинация электромагнитных пускателей может использоваться для обесточивания двигателя либо в случае обнаружения человека в опасной зоне, либо в случае открытия защитного устройства с блокировкой.

[МЭК 61508-4:2010, пункт 3.4.4, изменено — исключены перекрестные ссылки, добавлены примечания]

3.1.57 **элемент подсистемы** (subsystem element): Часть подсистемы, включающая отдельный компонент или группу компонентов.

Примечание 1 — Элемент подсистемы может содержать аппаратные средства и программное обеспечение.

Примечание 2 — Элементы, которые не являются непосредственно необходимыми для функции безопасности, не включены, но могут поддерживать ее (например, элементы фильтров, защита от перенапряжения).

Примечание 3 — Элемент подсистемы — это самый низкий уровень детализации, который следует учитывать при обеспечении выполнения требований подфункции.

[МЭК 62061:2021, пункт 3.2.6]

3.1.58 **систематический отказ** (systematic failure): Отказ, связанный детерминированным образом с какой-либо причиной, которая может быть исключена только путем модификации проекта, производственного процесса, операций, документации либо других факторов.

Примечание 1 — Корректирующее сопровождение без модификации, как правило, не устраняет причину отказа.

Примечание 2 — Систематический отказ может быть вызван имитацией причины отказа.

Примечание 3 — Примерами причин систематических отказов являются ошибки человека:

- в спецификации требований к безопасности;
- в проекте, изготовлении, установке и/или эксплуатации аппаратных средств;
- при проектировании и/или реализации и т. п. программного обеспечения.

[МЭК 61508-4:2010, пункт 3.6.6, изменено — примечание 3 незначительно изменено, примечание 4 исключено]

3.1.59 **полнота безопасности, касающаяся систематических отказов** (systematic safety integrity): Составляющая полноты безопасности SCS или SRP/CS или ее подсистем относительно ее устойчивости к систематическим отказам в режиме опасного отказа.

Примечание 1 — Полнота безопасности, касающаяся систематических отказов, как правило, не может быть точно определена количественно.

Примечание 2 — Требования полноты безопасности, касающейся систематических отказов, распространяются как на аппаратные, так и на программные аспекты SCS или ее подсистем.

[МЭК 61508-4:2010, пункт 3.5.6, изменено — терминология адаптирована к машинному оборудованию, примечание 1 сокращено, примечание 2 добавлено]

3.1.60 **целевая величина отказов** (target failure measure): Предполагаемое значение PFH или PFD_{avg}, которое должно быть достигнуто для обеспечения соответствия конкретным требованиям к полноте безопасности.

Примечание 1 — Целевая величина отказов определяется в терминах:

- средней вероятности опасного отказа при выполнении функции безопасности по запросу (для режима работы с низкой частотой запросов);
- средней частоты возникновения опасных отказов в час (для режима с высокой частотой запросов или непрерывного режима работы).

[МЭК 61508-4:2010, пункт 3.5.17, изменено — слова «целевая вероятность отказов в опасном режиме» заменены на «предполагаемое значение PFH или PFD_{avg}», перечисления перенесены в примечание 1, существующее примечание исключено]

3.1.61 **полезный срок службы** (useful lifetime): Минимальный период времени между установкой SCS или SRP/CS, подсистемы или элемента подсистемы и моментом времени, когда интенсивности отказов компонентов SCS или SRP/CS, подсистемы или элемента подсистемы больше не могут быть предсказаны с какой-либо точностью.

Примечание 1 — Вероятнее всего, полезный срок службы будет составлять 20 лет или меньше, если только изготовители SCS и ее подсистем не смогут обосновать более длительный срок службы, предоставив доказательства, основанные на расчетах, показывающие, что данными о надежности обоснованы более длительные сроки.

[МЭК 61131-6:2012, пункт 3.57, изменено — термин «наихудший случай» опущен, терминология адаптирована к машинному оборудованию, добавлено примечание 1, пример исключен]

3.1.62 **валидация** (validation): <функции безопасности> Подтверждение путем проверки (например, испытания, анализа) того, что SCS или SRP/CS соответствует требованиям функциональной безопасности для конкретного применения.

[МЭК 61508-4:2010, пункт 3.8.2, изменено — добавлена предметная область «функции безопасности», терминология адаптирована к машинному оборудованию, примечания исключены]

3.1.63 **верификация** (verification): Подтверждение проверкой (например, тестами, анализом), что SCS или SRP/CS, ее подсистемы или элементы подсистемы удовлетворяют требованиям, установленным соответствующей спецификацией.

Примечание 1 — Первоначальная верификация системы управления, связанной с безопасностью (SCS), в соответствии с МЭК 62061 или частей системы управления, связанных с безопасностью (SRP/CS), в соответствии с ИСО 13849-1 выполняется перед вводом в эксплуатацию. Первоначальная верификация соответствует процессу валидации, описанному в МЭК 62061:2021, раздел 9, или в ИСО 13849-1:2015, раздел 10.

Примечание 2 — Периодическая верификация системы управления, связанной с безопасностью (SCS), в соответствии с МЭК 62061 или частей системы управления, связанных с безопасностью (SRP/CS), в соответствии с ИСО 13849-1 выполняется через регулярные промежутки времени в процессе эксплуатации SCS или SRP/CS. МЭК 62061:2021, пункт 6.9 «периодические испытания» является частью периодической верификации.

Пример — Процессы верификации включают:

- просмотр выходных данных (документов, относящихся ко всем стадиям жизненного цикла системы безопасности), чтобы убедиться в соответствии задачам и требованиям определенной стадии с учетом конкретных входных данных для этой стадии;

- просмотр проектов;

- тестирование, выполняемое для проектируемых изделий, чтобы убедиться, что они работают в соответствии с их спецификацией;

- интеграционные тесты, выполняемые там, где различные части системы объединяются в пошаговом режиме, и проведение экологических испытаний, необходимых для того, чтобы убедиться, что все части работают вместе в соответствии со спецификацией.

[МЭК 62061:2021, пункт 3.2.64, изменено — добавлены слова «или SRP/CS», примечание 1 и примечание 2]

3.1.64 **достоверно испытанный компонент** (well-tried component): Компонент для связанного с безопасностью приложения, который или

a) широко использовался в прошлом и демонстрировал успешные результаты в аналогичных связанных с безопасностью приложениях, как указано для достоверно испытанных компонент в справочных приложениях ИСО 13849-2, или

b) изготовлен и верифицирован с использованием принципов, которые демонстрируют его пригодность и надежность для применений, связанных с безопасностью.

Примечание 1 — В ИСО 13849-2 перечислены различные компоненты и условия для конкретных технологий, при которых компонент можно считать достоверно испытанным.

Примечание 2 — Вновь разработанные компоненты можно считать эквивалентными «достоверно испытанным», если они удовлетворяют условиям перечисления b).

Примечание 3 — Решение признать конкретный компонент «достоверно испытанным» зависит от применения, например из-за влияния окружающей среды, на компонент также могут повлиять изменения изделия или изготовителя.

Примечание 4 — Сложные электронные компоненты (например, PLC, микропроцессор, специализированная интегральная схема) не могут считаться «достоверно испытанными».

Примечание 5 — Достоверно испытанный компонент не является проверенным в эксплуатации компонентом.

[МЭК 62061:2021, пункт 3.2.43]

3.1.65 **проверенные принципы безопасности** (well-tried safety principles): Принципы, которые в прошлом доказали свою эффективность при проектировании или интеграции систем управления, связанных с безопасностью, в предотвращении или управлении критическими сбоями или отказами, которые могут повлиять на выполнение функции безопасности.

Примечание 1 — Вновь разработанные принципы безопасности могут рассматриваться как эквивалентные «проверенным», если они верифицированы с использованием принципов, которые демонстрируют их пригодность и надежность для приложений, связанных с безопасностью.

Примечание 2 — Проверенные принципы безопасности эффективны не только против случайных отказов аппаратных средств, но и против систематических отказов, которые могут проникнуть в изделие в какой-то момент в течение жизненного цикла изделия, например сбои, возникающие во время проектирования, интеграции, модификации или ухудшения характеристик изделия.

Примечание 3 — Таблицы A.2, B.2, C.2 и D.2 в справочных приложениях ИСО 13849-2:2012 касаются проверенных принципов безопасности для различных технологий.

[МЭК 62061:2021, пункт 3.2.44]

3.2 Алфавитный список терминов, определений и сокращений

Термины, используемые в настоящем стандарте, приведены в таблице 1. В таблицу 1 также включены некоторые общие сокращения, связанные с безопасностью машинного оборудования.

Таблица 1 — Термины, используемые в настоящем стандарте

Термин	Номер определения
архитектура	3.1.3
архитектурное ограничение	3.1.2
безопасное состояние	3.1.46
безопасность	3.1.47
безопасный отказ	3.1.44
валидация	3.1.62
верификация	3.1.63
вероятность опасного отказа по запросу; PFD	3.1.36
вред	3.1.22
время безопасности процесса	3.1.37
встроенное программное обеспечение	3.1.13
доля безопасных отказов; SFF	3.1.45
доля опасных отказов; RDF	3.1.42
достоверно испытанный компонент	3.1.64
запрос	3.1.9
защита информации	3.1.54
защитная мера	3.1.39
интервал диагностических проверок	3.1.12
контрольная проверка	3.1.38
машина (оборудование)	3.1.29
непрерывный режим работы	3.1.7
опасная зона	3.1.25
опасная ситуация	3.1.24
опасность	3.1.23
опасный отказ	3.1.8
отказ	3.1.14
отказ по общей причине; CCF	3.1.5
отказоустойчивость аппаратных средств; HFT	3.1.20
охват диагностикой; DC	3.1.10

Окончание таблицы 1

Термин	Номер определения
подсистема	3.1.56
подфункция	3.1.55
полезный срок службы	3.1.61
полнота безопасности	3.1.49
полнота безопасности аппаратных средств	3.1.21
полнота безопасности, касающаяся систематических отказов	3.1.59
предварительно спроектированная SCS или подсистема	3.1.35
прикладное программное обеспечение	3.1.1
проверенные принципы безопасности	3.1.65
программное обеспечение, связанное с безопасностью	3.1.53
редко активируемая функция безопасности	3.1.41
режим работы с высокой частотой запросов	3.1.26
режим работы с низкой частотой запросов	3.1.28
риск	3.1.43
сбой	3.1.15
система управления машиной; MCS	3.1.30
система управления, связанная с безопасностью; SCS	3.1.51
систематический отказ	3.1.58
случайный отказ аппаратных средств	3.1.40
среднее время восстановления; MTTR	3.1.34
среднее время наработки на отказ; MTTF	3.1.32
среднее время работы до опасного отказа; $MTTF_D$	3.1.33
средняя продолжительность ремонта; MRT	3.1.31
средняя частота опасного отказа в час; PFH	3.1.4
управление конфигурацией	3.1.6
уровень полноты безопасности; SIL	3.1.50
устойчивость к отказам	3.1.17
функциональная безопасность	3.1.19
функция безопасности	3.1.48
функция диагностики	3.1.11
функция реакции на сбой	3.1.16
целевая величина отказа	3.1.60
элемент подсистемы	3.1.57
элемент системы управления, связанный с безопасностью; SRP/CS	3.1.52
язык программирования с полной изменчивостью; ЯПИ	3.1.18
язык с ограниченной изменчивостью; LVL	3.1.27

4 Типовая классификация функций безопасности в области безопасности машин и механизмов

4.1 Общие положения

4.1.1 Обзор

Процесс оценки риска реализуется путем применения ИСО 12100 для определения функций безопасности.

Примечание — Дополнительные указания, приведенные в настоящем стандарте, основаны на функциях безопасности, разработанных в соответствии с МЭК 62061 или ИСО 13849-1.

4.1.2 Оценка рисков и снижение рисков в соответствии с ИСО 12100

ИСО 12100 является фундаментальным стандартом безопасности, который обеспечивает общую основу и руководство для проектирования машин, безопасных при их предполагаемом использовании. В нем содержатся положения:

- по идентификации опасностей, а также по оценке и анализу рисков, связанных с машиной;
- о том, как устранить опасности или обеспечить достаточное снижение риска;
- и руководство по документированию и верификации оценки рисков и достижению снижения рисков.

Если опасность не может быть устранена, то необходимо снижение риска, связанного с опасностью, путем применения защитных мер. Такие защитные меры должны применяться в следующей последовательности, называемой трехэтапной стратегией снижения риска:

- этап 1 «Разработка безопасной конструкции самой машины»;
- этап 2 «Мероприятия по защите и/или дополнительные защитные меры»;
- этап 3 «Информация для использования».

ИСО 12100 также предусматривает стратегию для разработчиков стандартов при подготовке согласованных и соответствующих стандартов типа В и типа С.

ИСО 12100 является стандартом типа А, и, согласно этой классификации, МЭК 62061 и ИСО 13849-1, а также ИСО 13849-2 являются стандартами типа В1.

Примечание 1 — ИСО 12100 является основой для набора стандартов, который имеет следующую структуру:

- стандарты типа А (базовые стандарты безопасности), содержащие основные концепции, принципы проектирования и общие аспекты, которые могут применяться к машинам и механизмам;
- стандарты типа В (общие стандарты безопасности), касающиеся одного аспекта безопасности или одного типа защиты, которые могут использоваться в широком спектре машин и механизмов:
- стандарты типа В1 по конкретным аспектам безопасности (например, безопасные расстояния, температура поверхности, шум);
- стандарты типа В2 по защитным приспособлениям (например, двуручные органы управления, блокировочные устройства, чувствительные к давлению устройства, ограждения);
- стандарты типа С (стандарты безопасности машин), касающиеся подробных требований безопасности для конкретной машины или группы машин.

Примечание 2 — Дополнительную информацию о взаимосвязи между ИСО 13849-1 и ИСО 12100 можно найти в ISO/TR 22100-2. Эта взаимосвязь также действительна для МЭК 62061.

Примечание 3 — Многие региональные правила связаны с ИСО 12100, МЭК 62061 или ИСО 13849-1 или ссылаются на них. В приложении I приводится обзор различных нормативных подходов к обеспечению безопасности машин и механизмов.

Если стандарт типа С отклоняется от одного или нескольких технических положений, рассматриваемых в настоящем стандарте или в стандарте типа В, то приоритет имеет стандарт типа С.

Приложение А описывает базовый подход ИСО 12100 в контексте функциональной безопасности.

4.1.3 Снижение риска и взаимосвязь с SCS и SRP/CS

МЭК 62061, ИСО 13849-1, ИСО 13849-2 и настоящий стандарт используются в контексте трехэтапного процесса снижения риска, как описано в ИСО 12100.

Эти стандарты содержат требования:

- к проектированию SCS или SRP/CS и связанных с ними функций безопасности;
- расчету SIL или PL функции безопасности на основе используемой технологии;
- верификации и валидации достигнутого SIL или PL;
- инструкции по безопасному применению;
- руководству по определению требуемой полноты безопасности.

На рисунке 1 показана интеграция SCS или SRP/CS в процесс снижения риска, как описано в ИСО 12100.

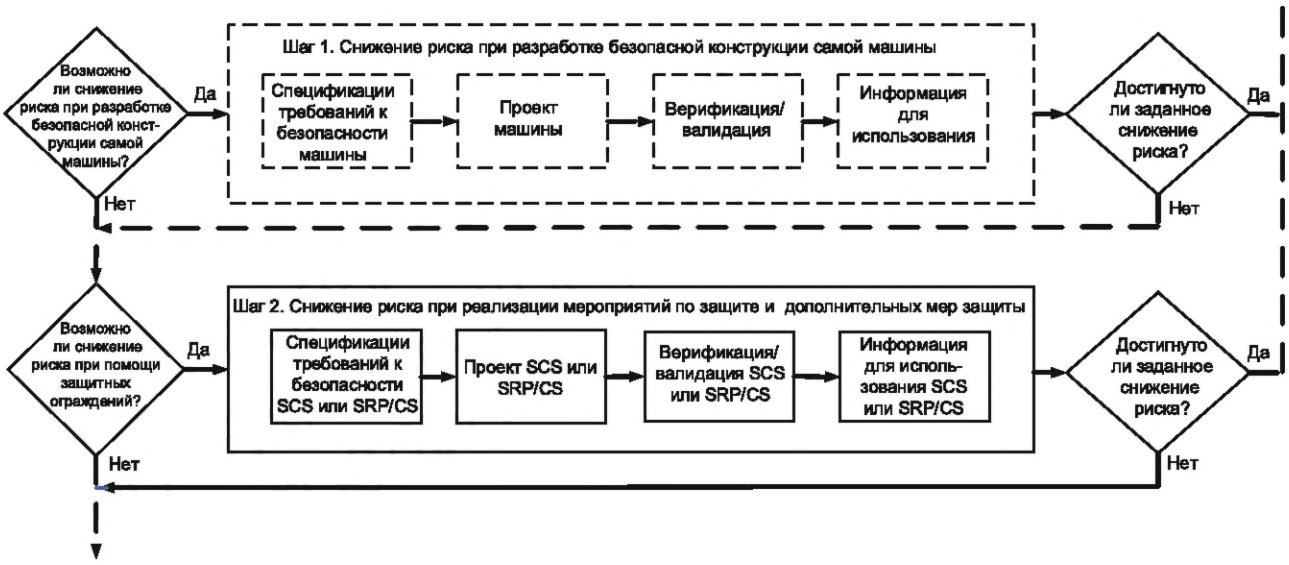


Рисунок 1 — Интеграция в процесс снижения рисков в ИСО 12100

4.1.4 Основные допущения для снижения риска в машинном оборудовании

Выделяют следующие основные допущения для применения снижения риска в машинном оборудовании:

- не связанные с безопасностью части системы управления машиной (MCS) не рассматриваются в контексте какого-либо снижения риска;
- для прямой или косвенной защиты людей оценивается потребность в функциях безопасности и за основу оценки берется режим работы с высокой частотой запросов;
- SCS или SRP/CS является мерой защиты, базирующейся на системе управления, для снижения рисков;
- повторный пуск машинного оборудования допускается только при условии обеспечения безопасных условий.

4.2 Основные допущения по безопасности для проектирования и интеграции SCS или SRP/CS

Для проектирования SCS или SRP/CS могут использоваться любые из доступных технологий (электрические, гидравлические, пневматические, механические и т. д.) по отдельности или в комбинации.

SCS или SRP/CS, как правило, состоят из одного или нескольких датчиков (или кнопок/переключателей), логического устройства принятия решений и одного или нескольких устройств действия.

На рисунке 2 показан типичный пример SCS или SRP/CS, разделенной на три подсистемы, выполняющие соответственно задачи обнаружения, оценки и инициирования действия.



Рисунок 2 — Декомпозиция SCS или SRP/CS

Для интеграции SCS или SRP/CS должны применяться следующие принципы:

- SCS или SRP/CS отделены и независимы от не связанных с безопасностью частей системы управления машиной (MCS).

Примечание — За некоторыми исключениями SCS или SRP/CS могут выполнять функции безопасности, которые также управляют процессом, например управление двумя руками;

- SCS или SRP/CS предназначены только для прямой или косвенной защиты лиц; они не принимают активного участия в процессах работы машины и активируются только при возникновении опасной ситуации;
- безотказность не связанных с безопасностью частей системы управления машиной (MCS) не включена в оценку функции безопасности. Речь идет о безотказности SCS или SRP/CS;
- при обнаружении опасного сбоя в SCS или SRP/CS машина переводится в безопасное состояние. Перезапуск процесса машины выполняется только после ремонта и восстановления SCS или SRP/CS.

4.3 Функции безопасности

4.3.1 Общие положения

SCS или SRP/CS, которая выполняет одну или несколько защитных мер, считается выполняющей функцию безопасности.

При активации функции безопасности машина должна быть переведена в безопасное состояние до возникновения опасной ситуации.

4.3.2 Процесс снижения риска функциями безопасности

На рисунке 3 показан этап 2 итеративного процесса снижения риска по ИСО 12100 с помощью функций безопасности в качестве мер защиты. Дополнительная информация приведена в приложении А.

4.3.3 Типовая классификация функций безопасности

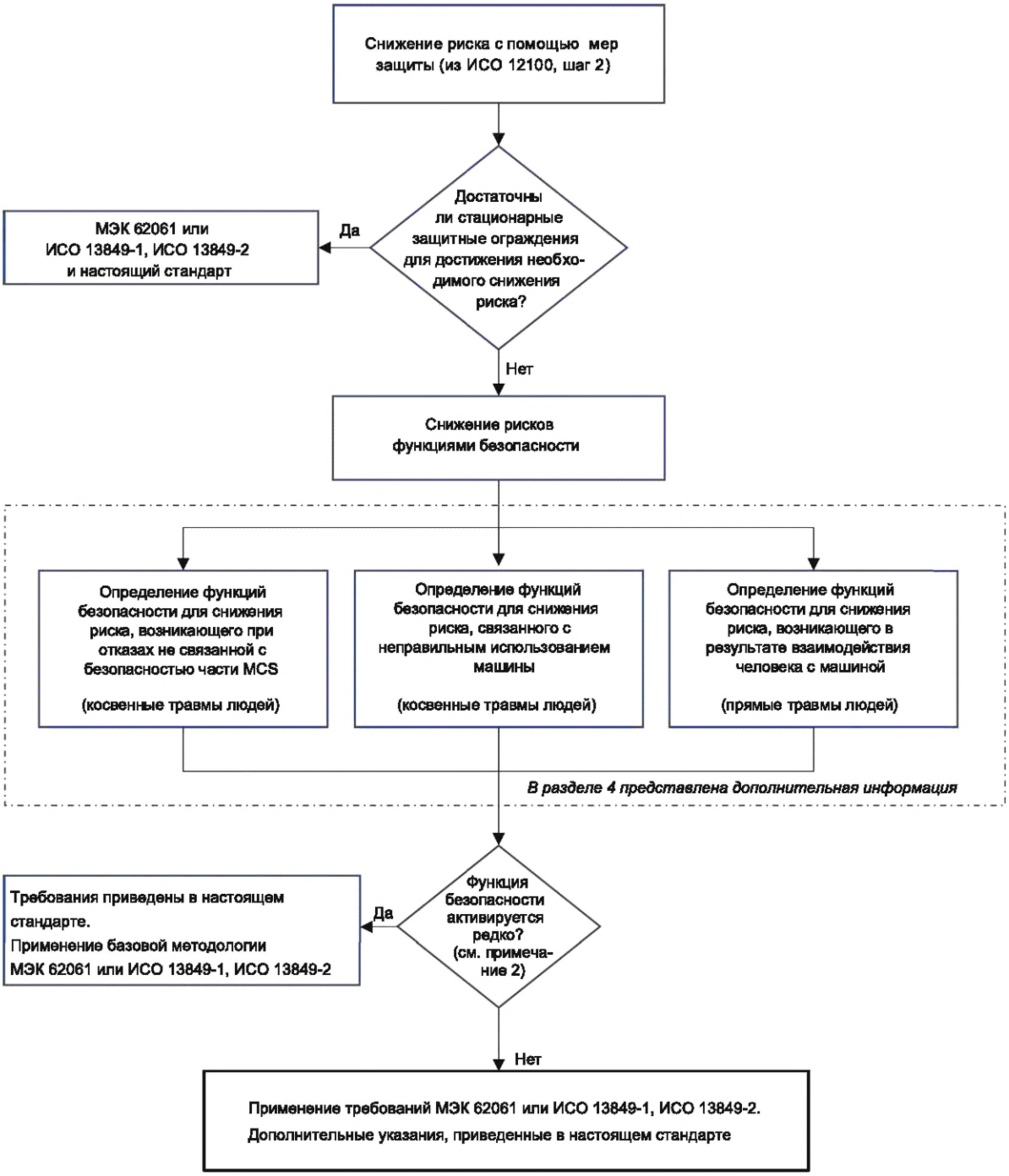
В целом все меры защиты или дополнительные меры защиты, реализуемые в соответствии с ИСО 12100, можно отнести к трем типам функций безопасности:

- функции безопасности для снижения рисков, возникающих в результате взаимодействия человека и машины. Они используются как средство защиты тела человека или частей его тела и предназначены для работы сразу после конкретного исходного события. Их роль заключается в обеспечении того, чтобы опасные части машины не травмировали человека (функции безопасности для защиты людей, см. 4.5);
- функции безопасности для снижения рисков, вызванных отказами MCS. Они используются в качестве средства предотвращения и предназначены для работы до того, как произойдет конкретное инициирующее событие. Их роль заключается в обеспечении того, чтобы авария не произошла, или, по крайней мере, снизилась скорость ее развития, или отклонения процесса были ограничены до приемлемого уровня (другие функции безопасности для предотвращения опасных ситуаций, см. 4.6);
- функции безопасности для снижения рисков, связанных с неправильным использованием машины. Они предназначены для снижения риска механических катастрофических отказов, вызванных высоким напряжением или чрезмерной рабочей нагрузкой (функции безопасности для обеспечения полноты безопасности машины, см. 4.7).

Функции безопасности могут быть реализованы индивидуально или в комбинации в зависимости от машины и процесса.

Для сложных машин человек может подвергаться риску перемещения, вращения, зажима из-за неисправностей, возникающих в MCS. Могут ли неисправности привести к опасной ситуации, зависит от взаимного положения человека и опасных движений машины.

Результат оценки риска определит, какая функция безопасности или комбинация функций безопасности должна быть реализована и в какой последовательности.



MCS — система управления машиной

Примечание — В зависимости от выбранной меры защиты для проектирования SCS или SRP/CS может потребоваться применение дополнительных стандартов, таких как МЭК 62046, ИСО 13851, ИСО 14119, ИСО 13856.

Рисунок 3 — Процесс снижения риска функциями безопасности

4.4 Взаимосвязь между ИСО 12100 и МЭК 62061 или ИСО 13849-1

4.4.1 Общие положения

Для правильного применения МЭК 62061 или ИСО 13849-1 необходима входная информация, полученная в результате применения общей оценки риска и процесса снижения риска для конкретной конструкции машины. На основе этой входной информации можно соответствующим образом спроектировать SCS или SRP/CS. Информация, полученная в результате детального проектирования SCS или SRP/CS для ее интеграции в конструкцию машины, должна затем учитываться в общей оценке риска и процессе снижения риска в соответствии с ИСО 12100.

4.4.2 Входная информация в соответствии с МЭК 62061 или ИСО 13849-1

В таблице 2 представлен обзор требуемой входной информации для проектирования SCS или SRP/CS в соответствии с МЭК 62061 или ИСО 13849-1.

Эта входная информация будет использоваться для создания спецификации требований безопасности (SRS).

Примечание — Таблицы 2—6 могут использоваться в качестве шаблонов для документации, в которой пустые поля могут содержать конкретную информацию, относящуюся к приложению.

Таблица 2 — Входная информация для спецификации требований безопасности (SRS)

Информация (пункт ИСО 12100)	Основные элементы, которые должны рассматриваться	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Ограничения машины (ИСО 12100:2010, пункт 5.3)	1) эксплуатационные ограничения, 2) пространственные ограничения, 3) временные ограничения, 4) другие ограничения (например, условия окружающей среды).		
Риск, связанный с конкретной опасной ситуацией (ИСО 12100:2010, пункты 5.4, 5.5.2)	1) тяжесть вреда; 2) вероятность возникновения вреда, возникающего в результате: - подверженности лица (лиц) опасности, - возникновения опасного события, - технических и человеческих возможностей избежать вреда или ограничить его		
Спецификации для предполагаемой эффективности соответствующего снижения риска/меры защиты	1) общая рекомендация предполагаемой функции по снижению риска/мере защиты (соответствующие функциональные требования); 2) конкретные характеристики, связанные с безопасностью, по снижению риска/мерам защиты (например, время реакции, режимы работы, запрос); 3) рекомендация условий окружающей среды, релевантных для снижения риска/меры защиты (например, ограничение пространства, температура, влажность, вибрация); 4) рекомендация другой машины и/или особых условий процесса (например, компоненты, связанные с безопасностью)		

4.4.3 Выходная информация из МЭК 62061 или ИСО 13849-1

В таблице 3 представлен обзор необходимой выходной информации при проектировании SCS или SRP/CS в соответствии с МЭК 62061 или ИСО 13849-1.

Таблица 3 — Выходные данные SCS или SRP/CS проекта по оценке общего риска

Информация (разделы МЭК 62061 и ИСО 13849-1)	Основные элементы, которые должны рассматриваться	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Подтверждение того, что намеченное снижение риска достигается техническим решением (МЭК 62061:2021, раздел 9) (ИСО 13849-1:2015, раздел 9)	Результаты верификации и валидации SCS в соответствии с МЭК 62061 или SRP/CS ИСО 13849-1		
Техническая документация (МЭК 62061:2021, раздел 10) (ИСО 13849-1:2015, раздел 10)	Техническая документация для интеграции/сборки технического решения конструкции машины		
Информация для использования (МЭК 62061:2021, раздел 10) (ИСО 13849-1:2015, раздел 11)	Вся соответствующая информация, предоставляемая разработчиком машины пользователю машины для обеспечения правильного использования SCS или SRP/CS и взаимосвязанного снижения риска/меры защиты		

4.5 Функции безопасности для защиты людей

4.5.1 Общие положения

Если проектные меры с внутренне присущей безопасностью не устраняют опасности или не снижают в достаточной степени риски, то всегда для защиты людей должны использоваться защитные ограждения и защитные устройства. Возможно, придется принять дополнительные защитные меры, включающие дополнительное оборудование (например, оборудование аварийной остановки).

Примечание — В таблицах 4—6 список функций безопасности основан на ИСО 12100, но другие стандарты типа В (например, ИСО 13849-1), стандарты типа С или другие международные стандарты МЭК также имеют аналогичные определения или требования.

4.5.2 Функции безопасности для защиты людей на основе защитных ограждений и защитных устройств

Функции безопасности на основе защитных ограждений и защитных устройств, предназначенные для защиты людей, могут включать функции, указанные в таблице 4, но не ограничиваться ими.

Таблица 4 — Функции безопасности для защиты людей

Функции безопасности для защиты людей	Основные элементы, которые должны рассматриваться. Запуск	Интенсивность запросов (низкая, высокая, редко происходящие запросы)	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Остановка, связанная с безопасностью. Защитные ограждения (ИСО 12100:2010, пункт 6.3.2.3)	При нормальной эксплуатации требуется доступ в опасную зону: - блокировочная защита; - блокировочное ограждение с его блокировкой; - блокировочная защита с функцией пуска (с функцией ручного сброса)		ИСО 14119	
Остановка, связанная с безопасностью. Защитные устройства (ИСО 12100:2010, пункт 6.3.2.2)	При нормальной эксплуатации может потребоваться доступ в опасную зону: - чувствительное средство защиты (SPE); - чувствительное защитное оборудование (SPE), отключение звука; - чувствительные к давлению защитные устройства		МЭК 61496, IEC TS 62998-1, МЭК 62046, ИСО 13856	

Окончание таблицы 4

Функции безопасности для защиты людей	Основные элементы, которые должны рассматриваться. Запуск	Интенсивность запросов (низкая, высокая, редко происходящие запросы)	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Система с ручным управлением. Ручная обработка (ИСО 12100:2010, пункт 6.3.2.3)	При нормальной эксплуатации требуется доступ в опасную зону: - устройство со сбросом (кнопка); - удерживающее устройство управления; - двухручное контрольное устройство		ИСО 11161, МЭК 60947-5-8, ИСО 13851	
Регулировка, обучение, переоснащение, поиск сбоев, техническое обслуживание, очистка. Ручное управление (ИСО 12100:2010, пункт 6.3.2.4)	Доступ в опасную зону необходим во время конкретной операции, такой как настройка машины, обучение и т. д.: - устройство включения; - устройство управления, ограничивающее движение для снижения скорости или мощности/силы		МЭК 60947-5-8, МЭК 61800-5-2	

4.6 Прочие функции безопасности для предотвращения опасных ситуаций

4.6.1 Общие положения

В дополнение к функциям безопасности, которые защищают людей непосредственно при взаимодействии, существуют прочие функции безопасности, которые могут быть косвенно важны для предотвращения опасных ситуаций и которые должны рассматриваться в дополнение к функциям безопасности для защиты людей.

4.6.2 Прочие функции безопасности

Прочие функции безопасности могут включать, но не ограничиваться перечисленными в таблице 5.

Таблица 5 — Прочие функции безопасности

Прочие функции безопасности	Основные элементы, которые должны рассматриваться. Запуск	Интенсивность запросов (низкая, высокая, редко происходящие запросы)	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Функция локального управления. Выбор локального управления (ИСО 13849-1:2015, пункт 5.2.4)	Доступ в опасную зону необходим во время нормальной эксплуатации или конкретной операции, такой как настройка машины, обучение и т. д.: - устройство (и процедура) ручного местного управления			
Параметры, связанные с безопасностью. Выбор параметров (ИСО 12100:2010, пункт 6.3.2.7)	Доступ в опасную зону необходим во время нормальной эксплуатации или конкретной операции, такой как настройка машины, обучение и т. д.: - дополнительные меры защиты; - устройство (и процедура) ручного выбора параметров			
Требования к выбору режима эксплуатации. Режимы управления и эксплуатации (ИСО 12100:2010, пункт 6.2.11.10)	Доступ в опасную зону необходим во время нормальной эксплуатации или конкретной операции, такой как настройка машины, обучение и т. д.: - устройство (и процедура) ручного выбора режима эксплуатации			

Окончание таблицы 5

Прочие функции безопасности	Основные элементы, которые должны рассматриваться. Запуск	Интенсивность запросов (низкая, высокая, редко происходящие запросы)	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Функции аварийного останова. Аварийная ситуация (ИСО 12100:2010, пункт 6.3.5.2)	Новая дополнительная мера защиты для предотвращения аварийных ситуаций (рассматривается как функция безопасности): - устройство аварийного останова		ИСО 13850	
Колебания, потеря и восстановление источников питания. Меры контроля, связанные с источниками питания (ИСО 12100:2010, пункты 6.2.11.5, 6.3.2.4, 6.3.5.4)	Доступ в опасную зону необходим во время нормальной эксплуатации или конкретной операции, такой как настройка машины, обучение и т. д.; общее рассмотрение мер контроля, связанных с источниками питания: - устройство (и процедура) контроля питания		ИСО 14118	

4.7 Функции безопасности для обеспечения полноты безопасности машины

4.7.1 Общие положения

Если машина требует непрерывного управления со стороны оператора (например, мобильные машины, краны) и ошибка оператора может создать опасную ситуацию, то эта машина должна быть оснащена необходимыми устройствами, которые обеспечивают ее эксплуатацию в заданных пределах характеристик машины, в частности:

- при недостаточной видимости оператором опасной зоны;
- когда оператору неизвестно фактическое значение параметра, связанного с безопасностью (расстояние, скорость, масса, угол и т. д.);
- когда опасности могут возникнуть в результате операций, отличных от тех, которые контролируются оператором.

Автоматические защитные меры, приводимые в действие такими устройствами, которые выводят машинное оборудование из-под контроля оператора (например, автоматическая остановка опасного движения), должны предшествовать или сопровождаться предупреждающим сигналом, позволяющим оператору предпринять соответствующие действия (см. ИСО 12100:2010, пункт 6.3.2.7).

4.7.2 Функции безопасности для обеспечения полноты безопасности машины

Функции безопасности для обеспечения полноты безопасности машины могут включать, помимо прочего, функции, перечисленные в таблице 6.

4.8 Функции безопасности и стандарты типа С

Стандарты типа С могут определять функции безопасности там, где технические требования могут отличаться от ИСО 12100. В этом случае приоритет имеют стандарты типа С.

Таблица 6 — Функции безопасности для обеспечения полноты безопасности машины

Функции безопасности для обеспечения полноты безопасности машины	Основные элементы, которые должны рассматриваться. Запуск	Интенсивность запросов (низкая, высокая, редко происходящие запросы)	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Работа с ограничениями. Другие устройства защиты (ИСО 12100:2010, пункт 6.3.2.7)	Опасности могут возникнуть в процессе эксплуатации и автоматически (независимо от оператора) срабатывают меры защиты: - устройства для предотвращения помех или столкновений с другими машинами; - устройства для обеспечения того, чтобы компоненты находились в безопасном положении перед движением			

Окончание таблицы 6

Функции безопасности для обеспечения полноты безопасности машины	Основные элементы, которые должны рассматриваться. Запуск	Интенсивность запросов (низкая, высокая, редко происходящие запросы)	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Действие остается в указанных пределах. Другие защитные устройства (ИСО 12100:2010, пункт 6.3.2.7)	В результате действий, которые неявно могут причинить вред людям, могут возникнуть опасности и автоматически (независимо от оператора) срабатывают меры защиты: - устройства, ограничивающие крутящий момент и места повреждений для предотвращения чрезмерной нагрузки на узлы и компоненты; - устройства, ограничивающие параметры движения (расстояние, угол, скорость, ускорение); - устройства, ограничивающие перегрузки и момент; - устройства, ограничивающие давление или температуру; - устройства для мониторинга выбросов			

5 Режим работы по запросу, связанный с функциями безопасности

5.1 Общие положения

Каждая функция безопасности, выполняемая SCS (спроектированной в соответствии с МЭК 62061) или SRP/CS (спроектированной в соответствии с ИСО 13849-1), работает либо в режиме с высокой частотой запросов (см. 5.2), либо в режиме с низкой частотой запросов (см. 5.3).

Примечание 1 — Информация, приведенная в разделе 5, основана на функциях безопасности, разработанных в соответствии с МЭК 62061 или ИСО 13849-1.

Примечание 2 — Из-за разнообразия машин частота запросов к функции безопасности для защиты людей неизвестна (она варьируется от нескольких в час до одного в год). Поэтому предполагается, что функции безопасности находятся в режиме с высокой частотой запросов.

Функции защиты машины, как правило, запрашиваются менее одного раза в год, поскольку машина спроектирована с учетом ряда основных принципов безопасности, чтобы соответствовать требованиям ИСО 12100.

Эти функции защиты можно классифицировать как функции безопасности, если последствием существующего риска является явная или неявная травма людей, находящихся рядом с машиной.

Примечание 3 — Предполагается, что эти функции защиты/безопасности работают в режиме с высокой частотой запросов, поскольку опасная ситуация должна быть немедленно предотвращена, например, путем остановки опасных движений машины, а также потому, что эти функции безопасности в оборудовании являются единственной мерой снижения риска, и никакой другой «слой защиты» не рассматривается.

Из-за этих различий между функциями безопасности для защиты людей от явных травм и функциями защиты для защиты людей от неявных травм критерии испытаний функций безопасности/защиты могут отличаться от критериев, определенных в МЭК 62061:2021, пункт 7.3.3.4.

Примечание 4 — Если для неэлектронной технологии функциональное испытание необходимо для обнаружения возможного накопления сбоев или невыявленного сбоя до следующего запроса, то МЭК 62061, пункт 7.3.3.4, требует следующих интервалов испытаний:

- не реже одного раза в месяц для SIL 3;
- не реже одного раза в 12 месяцев для SIL 2.

5.2 Режим работы с высокой частотой запросов или с непрерывными запросами

5.2.1 Общие положения

Система управления машиной (MCS), выполняющая производственный процесс, считается независимой от SCS или SRP/CS. Взаимодействие может происходить, но система управления машиной не учитывается при оценке снижения риска SCS или SRP/CS и не является частью мер по снижению риска.

Предполагается, что взаимодействие с оператором машины не является частью какого-либо слоя защиты, применяемого в режиме работы с низкой частотой запросов (см. рисунок 4).

Применяются следующие обоснования:

- функции безопасности, реализованные для машин, в основном предназначены для защиты людей;
- операторам не нужна подробная информация о проекте функции безопасности и связанной с ней SCS или SRP/CS;
- функциями безопасности можно управлять вручную, например двуручное управление;
- частота запросов к функции безопасности высокая, не реже одного раза в год;
- время реакции функции безопасности, как правило, невелико.

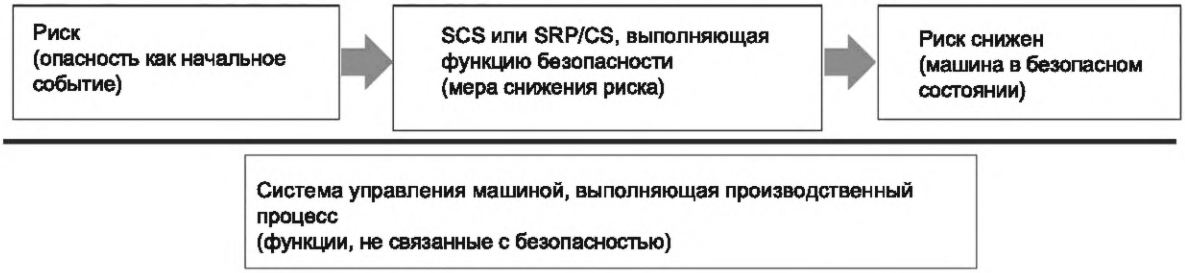


Рисунок 4 — Режим работы с высокой частотой запросов

5.2.2 Подход МЭК 62061 и ИСО 13849-1

Проектирование, интеграция и установка SCS или SRP/CS выполняются для режима работы с высокой частотой запросов или непрерывного режима работы. Оценка значений PFH или PFH_D для подсистем выполняется для режима работы с высокой частотой запросов или непрерывного режима работы.

5.2.3 Редко активируемые функции безопасности

5.2.3.1 Общие положения

Если используется режим работы с высокой частотой запросов, то предполагается, что высокая частота запросов к функции безопасности определяется как «средняя». Тем не менее может случиться так, что предполагаемый запрос к функции безопасности не произойдет в течение одного года; это может случиться, если изготовитель машины задает среднюю частоту запросов для обеспечения полноты безопасности как своего рода наихудший случай при определении требуемой полноты безопасности.

Те функции безопасности, которые предназначены для режима работы с высокой частотой запросов, но к которым иногда в течение одного года не происходит ни одного запроса, называются «редко активируемыми функциями безопасности».

Редко активируемые функции безопасности проектируются, реализуются и интегрируются в качестве функций безопасности для режима работы с высокой частотой запросов.

Редко активируемые функции безопасности (см. В.12.2.5), запускаемые по событию, требуют принятия специальных мер, связанных с накоплением сбоев и с необнаруженными сбоями.

Для обеспечения полноты безопасности таких функций, к которым запросы еще не происходили, необходима периодическая проверка, см. также 7.5.2.

О режиме работы для редко активируемых функций безопасности в разделах 6 и 7 представлена дополнительная информация.

5.2.3.2 Основные требования

Примечание 1 — Для редко активируемых функций безопасности оценка значения PFH на основе значения B_{10}/B_{100} не ограничивает достижимый SIL или PL, поскольку $MTTF_D$ превышает 2000 лет или λ_D меньше 5E-08, см. МЭК 62061:2021, таблица H.2.

Интервал диагностических проверок функции безопасности связан с частотой запросов, и диагностика происходит только тогда, когда функция безопасности запрашивается. Поэтому для обнаружения накопления необнаруженных сбоев необходимы периодические процедуры верификации, см. раздел 7.

Для функций безопасности, обеспечивающих защиту машины, может использоваться интервал диагностических проверок до двух лет, если выполняются следующие условия, чтобы свести к минимуму возможность накопления сбоев или необнаруженные сбои до следующего запроса:

a) предоставлено обоснование того, что воздействие окружающей среды не уменьшает срок службы компонентов, например от коррозии, утечки, проблем с уплотнениями;

И

b) для каждой подсистемы при значениях SIL 1/PL_r c и SIL 2/PL_r d использована минимальная архитектура HFT = 1/категория 3;

ИЛИ

c) для каждой подсистемы при значении SIL 3/PL_r e использована минимальная архитектура HFT = 1/категория 3 и применены дополнительные проектные меры, например разнообразие между каналами или непрерывное обнаружение сбоев с использованием динамических сигналов.

Пример — «Непрерывное обнаружение сбоев с использованием динамических сигналов» означает, что мониторинг скорости осуществляется с помощью датчиков, обеспечивающих цифровые или аналоговые значения (не двоичные), которые постоянно сравниваются с номинальным значением (скорость), а не только в момент, когда происходит превышение скорости (событие срабатывания).

При использовании упрощенных формул приложения H значение T_2 составляет 17 520 часов (два года).

Примечание 2 — В ИСО 13849-1:2015, приложение K, не рассматриваются граничные условия интервала диагностических проверок, если этот интервал проверок превышает один год.

На рисунке 5 показан общий вид процесса определения режима работы с высокой частотой запросов.

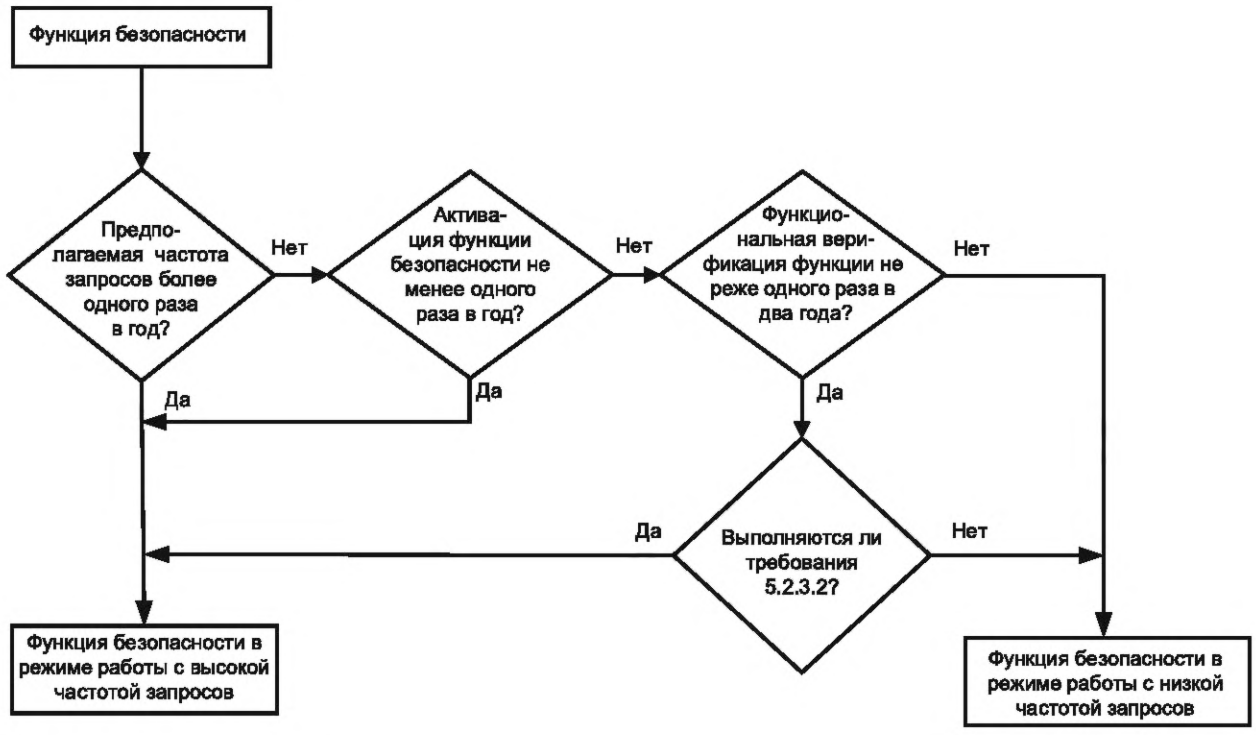


Рисунок 5 — Процесс определения режима работы с высокой частотой запросов

Редко активируемая функция безопасности должна верифицироваться в соответствии с требованиями раздела 7.

5.2.3.3 Подход МЭК 62061 и ИСО 13849-1

МЭК 62061 и ИСО 13849-1 не рассматривают редко активируемые функции безопасности.

5.3 Режим работы с низкой частотой запросов

5.3.1 Общие положения

Этот режим работы, как правило, используется в перерабатывающей промышленности (см. МЭК 61511). Предполагается, что взаимодействие оператора является частью своего рода представления слоя защиты.

Основными причинами такого подхода являются (см. представление на рисунке 6):

- функции безопасности приборной системы безопасности (SIF), реализованные в соответствии с МЭК 61511, в основном предназначены для защиты технологического процесса;
- операторы имеют подробную информацию о разработке функций безопасности приборной системы безопасности (SIF), системы управления и самого управления технологическим процессом;
- применяется подход слоев защиты, основанный на использовании и оценке системы управления, осуществляющей управление технологическим процессом;
- частота запросов к функциям безопасности приборной системы безопасности (SIF) может быть низкой, и ожидается, что один такой запрос будет происходить в течение одного года или нескольких лет;
- время реакции функций безопасности приборной системы безопасности (SIF) намного выше, чем в режиме работы с высокой частотой запросов.

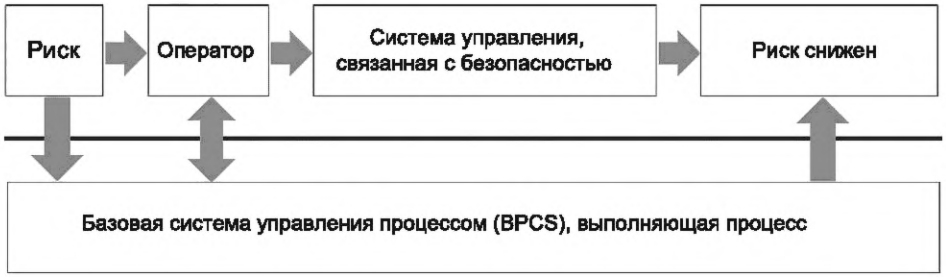


Рисунок 6 — Режим работы с низкой частотой запросов

5.3.2 Подход МЭК 62061 и ИСО 13849-1

МЭК 62061 и ИСО 13849-1 исключают режим работы с низкой частотой запросов.

Примечание — В будущих поправках к МЭК 62061 планируется рассмотреть возможность интеграции режима работы с низкой частотой запросов.

В приложении J даны указания о том, как проектировать функции безопасности приборной системы безопасности (SIF) путем объединения подсистем, работающих в режиме с низкой частотой запросов, и подсистем, работающих в режиме с высокой частотой запросов.

6 Процесс проектирования функций безопасности

6.1 Общие положения

В настоящем разделе определяются основные мероприятия по проектированию SCS (разработанной в соответствии с МЭК 62061) или SRP/CS (разработанной в соответствии с ИСО 13849-1), выполняющей функцию безопасности.

Примечание — Информация, приведенная в настоящем разделе, основана на функциях безопасности, разработанных в соответствии с МЭК 62061 или ИСО 13849-1.

Изготовитель машины интегрирует некоторые требования, основанные на процессе проектирования, в информацию для применения машины.

Принципы действий по верификации, описанные в настоящем разделе, связаны с основными требованиями к контрольной проверке, как описано в серии стандартов МЭК 61508. Термин «контрольная проверка» не используется, поскольку он тесно связан с серией стандартов МЭК 61508, и рекомендуется использовать нейтральный термин в контексте машин и механизмов.

6.2 Процедура проектирования

SCS или SRP/CS, выполняющие функцию безопасности, спроектированы с использованием методологии для режима работы с высокой частотой запросов, см. основную процедуру, подробно описанную в приложении B.

Примечание — Руководство по проектированию программного обеспечения см. в приложении F.

6.3 Оценка требуемой полноты безопасности

В приложении A представлен обзор различных методологий оценки требуемой полноты безопасности функции безопасности.

В таблице H.1 МЭК 62061:2021 представлена оценка PFH на основе $MTTF_D$ для всех технологий. В таблице H.2 МЭК 62061:2021 представлена взаимосвязь между B_{10D} и $MTTF_D$ для неэлектронных технологий. Если расчеты выполняются в соответствии с таблицей H.2 МЭК 62061:2021 с рабочим циклом (на основе критериев B_{10D}) ниже, чем один цикл за четыре часа, то оценка PFH (таблица H.1 МЭК 62061:2021) не является ограничивающим фактором для достижения требуемого SIL.

Примечание — Пример одиночного контактора с B_{10D} = 1 300 000 (циклов) и рабочим циклом один раз в час приводит к $MTTF_D$ = 1 484 года и PFH = 7,70E-08 << 1,0E-05 (SIL 1), и если рабочий цикл составляет один раз в день, то $MTTF_D$ = 35 616 лет и PFH = 3,20E-09 << 1,0E-05 (SIL 1).

6.4 Декомпозиция функции безопасности

Выполняющие SCS или SRP/CS функции безопасности, которые декомпозируются на подсистемы, рассмотрены в разделе 5.

В приложении B представлен обзор методологии проектирования SCS или SRP/CS.

6.5 Проектирование подсистем

6.5.1 Архитектурные ограничения

Поскольку интервал диагностических проверок связан с частотой запросов, определенная диагностика возможна только тогда, когда функция безопасности запрашивается (см. примеры охвата диагностикой в приложении D). На основе накопления сбоев (см. 6.5.2) должны оцениваться архитектурные ограничения в зависимости от режима работы. В режиме работы с высокой частотой запросов применяется таблица 7, основанная на таблице 6 МЭК 62061:2021.

Таблица 7 — Ограничения архитектуры для режима работы с высокой частотой запросов

	Отказоустойчивость аппаратных средств (HFT) [a]				Основные требования[d]
	Одноканальная подсистема HFT = 0 [c]		Двухканальная подсистема HFT = 1		
DC_{avg} (ИСО 13849-1)[b]	Макс. PL	Категория (ИСО 13849-1)	Макс. PL	Категория (ИСО 13849-1)	
SFF (МЭК 62061)	Макс. SIL	Базовая архитектура подсистемы (МЭК 62061)	Макс. SIL	Базовая архитектура подсистемы (МЭК 62061)	
«Нет»	PL a	Категория B	—	—	Основные принципы безопасности[e]
—	Нет SIL (ОМ)	—	Нет SIL (ОМ)	—	
«Нет»	PL b	Категория B	—	—	
—	—	—	—	—	
«Нет»	PL c	Категория 1	—	—	Основные принципы безопасности и хорошо отработанные принципы безопасности
< 60 %	SIL 1	Архитектура A: - хорошо отработанные компоненты; - CCF нерелевантный	SIL 1	Архитектура B: - хорошо отработанные компоненты; - CCF релевантный	
«Низкий»	PL c	Категория 2	PL d	Категория 3	

Окончание таблицы 7

От 60 % до < 90 %	SIL 1	Архитектура C: - CCF релевантный	SIL 2	Архитектура D: - CCF релевантный	Основные принципы безопасности и хорошо отработанные принципы безопасности
«Средний»	PL d	Категория 2 (см. примечание 6)	PL e	Категория 3	
От 90 % до < 99 %	SIL 2	Архитектура C: - CCF релевантный	SIL 3	Архитектура D: - CCF релевантный	
«Высокий»	—	Нет эквивалентной категории	PL e	Категория 4	
≥ 99 %	SIL 3	Архитектура C: - CCF релевантный	SIL 3	Архитектура D: - CCF релевантный	

ОМ — другие меры будут применяться там, где не требуется SIL.

CCF — отказы по общей причине будут рассматриваться независимо от того, HFT = 0 и DC > 60 % или HFT = 1.

[a] Отказоустойчивость аппаратных средств *N* означает, что отказы *N* + 1 могут привести к потере функции безопасности.

[b] «Низкий», «средний» и «высокий» — это обозначения, используемые в ИСО 13849-1 в контексте количественной оценки и классификации диапазонов DC_{avg}.

[c] Для HFT 0 и SFF ≥ 99 % могут быть применимы следующие ограничения:

- настоятельно рекомендуется ограничить максимальное значение SIL 2, где исключение сбоя было применено к сбоям, которые могут привести к опасному отказу; для некоторых применений не ожидается, что все отказы могут быть исключены с достаточной уверенностью для SIL 3 (см. МЭК 62061:2021, пункт 7.3.3.3); SIL 3 может быть заявлен только при условии непрерывного контроля правильности функционирования элемента. Как правило, для этого потребуется электронная технология.

[d] Основные принципы безопасности и хорошо отработанные принципы безопасности требу-ются независимо от выбранной архитектуры. Основные требования см. также в ИСО 13849-2:2012, приложение A — приложение D. Примерами являются:

- для основных принципов безопасности — выбор и использование подходящих материалов;
- для хорошо проверенных принципов безопасности — применение принципа обесточивания;
- для хорошо проверенных компонентов — использование контакторов или переключателей положения.

[e] При использовании стандартов на изделия, например МЭК 61800-5, МЭК 61131-2 и т.д., можно предположить, что основные принципы безопасности могут быть соблюдены.

[f] Согласно ИСО 13849-1 PL d может быть достигнут только тогда, когда выход (OTE как функция реакции на сбой) инициирует безопасное состояние, которое поддерживается до тех пор, пока сбой не будет устранен. Недостаточно, чтобы на OTE контрольно-измерительного оборудования выдавалось только предупреждение. О «безопасном состоянии» см. в 3.1.46.

Для одноканальной подсистемы (HFT = 0):

$$SFF \approx DC_{avg} = \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1 \cdot \lambda_{D1}}{\lambda_{D1}} = DC_1,$$

для двухканальной подсистемы (HFT = 1):

$$SFF \approx DC_{avg} = \frac{\lambda_{DD1} + \lambda_{DD2}}{\lambda_{D1} + \lambda_{D2}} = \frac{DC_1 \cdot \lambda_{D1} + DC_2 \cdot \lambda_{D2}}{\lambda_{D1} + \lambda_{D2}} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}},$$

где λ_{DD1}, λ_{DD2} — интенсивности опасных отказов элементов подсистемы 1 и 2, определяемые функциями диагностики;

λ_{D1}, λ_{D2} — интенсивности опасных отказов элементов подсистемы 1 и 2;

DC_1, DC_2 — охваты диагностикой элементов подсистемы 1 и 2.

6.5.2 Накопление сбоев и необнаруженные сбои

В режиме работы с высокой частотой запросов для обнаружения опасных сбоев и при их накоплении требуется функциональное тестирование (см. также B.12.1).

Для функций безопасности, защищающих людей (прямо или косвенно) с помощью подсистем на основе неэлектронной технологии и с автоматическим мониторингом для достижения необходимого охвата диагностикой для требуемых характеристик безопасности, функция мониторинга невозможна до тех пор, пока не произойдет изменение состояния, например, на каждом рабочем цикле. При нечастой эксплуатации увеличивается вероятность накопления необнаруженных сбоев.

Если функциональное испытание необходимо для обнаружения возможного накопления сбоев или необнаруженного сбоя до следующего запроса, оно должно проводиться в течение следующих интервалов испытаний:

- не реже одного раза в месяц для SIL 3;
- не реже одного раза в 12 месяцев для SIL 2.

Примечание — Данные правила в разных государствах могут требовать других периодических интервалов испытаний, см. также приложение I.

Инициируемые событием редко активируемые функции безопасности (см. B.12.2.5) определяют меры, противодействующие накоплению сбоев и необнаруженным сбоям. Необходимо проводить периодическую верификацию, см. также пункт 7.5.2.

Следует учитывать отказы по общей причине CCF. В МЭК 62061:2021 (приложение E), ИСО 13849-1:2015 (приложение E) и в приложении E даны рекомендации по мерам предотвращения и управления отказами по общей причине.

6.5.3 Оценка PFH

6.5.3.1 Общие положения

В приложении H приведена информация по оценке значения PFH подсистемы и соответствующих граничных условий. Формулы могут использоваться для режима работы с высокой частотой запросов.

Примечание — Ограничивающим фактором будет являться систематическая полнота безопасности, и процедуры верификации станут более актуальными.

В приложении C приводятся примеры значений $MTTF_D$ для отдельных компонентов, которые также могут использоваться для редко активируемых функций безопасности.

Частота запросов к функции безопасности оказывает существенное влияние на оценку значений PFH подсистемы.

6.5.3.2 Влияние значений B_{10D}

На практике значение PFH, основанное на B_{10D} и рабочих циклах, не ограничивает достигаемое значение SIL или PL:

- при одном рабочем цикле в сутки значение PFH << максимального значения PFH, требуемого значением SIL или PL;
- ограничения архитектуры являются ограничивающим фактором при достижении SIL.

Когда рабочий цикл превышает один раз в час, то T_{10D} становится важным, см. 6.5.3.3.

Таблица H.7 показывает типичные значения с использованием наихудшего случая B_{10D} = 1 000 000 циклов (например, контактор или переключатель положения).

6.5.3.3 Влияние величины T_{10D}

Срок службы ограничен T_{10}, и компоненты должны быть заменены по истечении T_{10}, если никакая другая информация не предоставляется стандартами на изделие.

Для определенных условий в H.6 дается обоснование ограничения от T_1 до T_{10} для компонентов, основанных на любом виде интегральной функции распределения (CDF), использующих неэлектронные технологии, см. также H.5.2.

Значение T_{10D} ограничивает полезный срок службы компонентов, которые характеризуются распределением Вейбулла. Недоступность компонента значительно возрастает после времени T_{10D}.

Примечание — T_{10} — это предельное значение, до которого, как предполагается, значение λ является постоянной величиной (так называемая «ваннообразная кривая»). Данные B_{10} об изделии (число циклов, при которых достигается T_{10}), как правило, относятся к компонентам, основанным на распределении Вейбулла.

Формулы PFH справедливы до T_{10D}, поскольку формулы PFH основаны на экспоненциальном распределении, см. H.6 и H.7. Срок службы T_1, как правило, принимается равным 20 годам (или 175 200 ч).

Если T_{10D} меньше, чем T_1, то формулы PFH используются, ограничивая T_1 до

$$T_1 = T_{10D}. \quad (2)$$

T_{10D} можно оценить как:

$$\lambda_D \approx 0{,}1 \cdot C / B_{10D} = 0{,}1 \cdot C / B_{10} \cdot \text{RDF [1/час]}, \quad (3)$$

$$\text{MTTF}_D \approx B_{10D} / (0{,}1 \cdot n_{op}) = B_{10} / (0{,}1 \cdot n_{op} \cdot \text{RDF}) \text{ [ц]}, \quad (4)$$

$$T_{10D} \approx 0{,}1 / \lambda_D \text{ [1/час] или } T_{10D} \approx 0{,}1 / (8760 \cdot \lambda_D) \text{ [ц]}, \quad (5)$$

$$T_{10D} \approx 0{,}1 \cdot \text{MTTF}_D \text{ [ц]}, \quad (6)$$

где λ_D — интенсивность опасных отказов компонента, выраженная в отказах в час;
C — рабочий цикл, выраженный в циклах в час;
B_{10D} — среднее число циклов до опасного отказа 10 % компонентов, выраженное в циклах;
B_{10} — среднее число циклов до отказа 10 % компонентов, выраженное в циклах;
RDF — относительное число опасных отказов B_{10} / B_{10D}, выраженное в процентах;
n_{op} — среднее число годовых циклов, выраженное в циклах.

Пример представлен в таблице Н.8.

6.6 Примеры функций безопасности

В приложении G приведены примеры функций безопасности, включая:
- основную информацию;
- оценку значений PFH с использованием значений MTTF_D, перечисленных в приложении С.

Эти примеры классифицируются в соответствии с разделом 4.

7 Процедуры верификации функций безопасности

7.1 Общие положения

Различают часто запрашиваемые функции безопасности и редко активируемые функции безопасности, разработанные в соответствии с МЭК 62061 или ИСО 13849-1. «Частыми» считаются запросы не реже одного раза в год, «редкими» — запросы с частотой менее одного раза в год.

Примечание 1 — Информация, приведенная в настоящем разделе, основана на функциях безопасности, разработанных в соответствии с МЭК 62061 или ИСО 13849-1.

В зависимости от проекта функции безопасности редкое срабатывание может привести к потере функции безопасности, например, из-за залипания, загрязнения, условий окружающей среды, масел, смазки или также из-за влияния напряжения питания.

Примечание 2 — Например, опасная зона доступна через несколько часто открывающихся защитных дверей, но есть одна, которая используется редко (менее одного раза в год).

При частых запросах риск накопления сбоев будет снижен, если будет реализована диагностика, зависящая от изменения состояния. Это относится ко всем функциям безопасности при режиме работы с высокой частотой запросов или с непрерывными запросами.

7.2 Верификация интервала диагностических проверок функции безопасности

Современная технология позволяет документировать требование устройства, связанного с безопасностью, в SCS или SRP/CS. Если документально оформленные результаты можно сравнить с реальными значениями, то допускается указать операторам, что они должны протестировать определенные функции безопасности.

Если это не реализовано, то в соответствии с планом технического обслуживания или информацией для пользователя через регулярные промежутки времени должны выполняться требования о диагностических проверках функции безопасности.

7.3 Процедуры верификации

Каждая функция безопасности должна быть протестирована с целью правильного функционирования перед первоначальным запуском (см. 7.4, начальная верификация), через регулярные (частые) промежутки времени и после ремонта (и технического обслуживания) (см. 7.5, периодическая верификация). Степень и объем испытания определяются требованиями инструкции по эксплуатации (информация по применению).

Примечание 1 — Термины «начальная верификация» или «периодическая верификация» используются в контексте электрооборудования машин (см. МЭК 60204-1: 2016, раздел 18, МЭК 60204-1:2016/AMD1:2021, раздел 18, и МЭК 60364-1:2005, пункты 134.1 и 134.2). Эти термины также используются в контексте ввода машины в эксплуатацию.

Общее различие проводится между двумя типами испытаний:

- испытание функции безопасности лицом, компетентным в области верификации функции безопасности. Во время этого испытания проверяется только результат, то есть реакция системы безопасности;
- испытание эффективности функции безопасности лицом, компетентным в вопросах функциональной безопасности и отвечающим за процесс верификации; во время этого испытания проверяется вся система, связанная с безопасностью; лицо, отвечающее за верификацию, определяет степень и объем испытания на основе, например, инструкций изготовителя по обеспечению безопасности.

Примечание 2 — Требования к квалификации лиц, компетентных в области функциональной безопасности, отвечающих за верификацию, могут быть включены в национальные правила.

Примечание 3 — Лицом, компетентным в вопросах функций безопасности, может быть представитель компетентного органа, лицо, представляющее изготовителя машины, или лицо, не связанное с компанией изготовителя машины; целесообразно документировать компетенцию лица и органа (или обоих).

7.4 Начальная верификация

Машина должна быть осмотрена во время установки, насколько это практически осуществимо, и по завершении, перед вводом в эксплуатацию.

Начальная верификация должна включать сравнение результатов с соответствующими критериями для подтверждения того, что требования МЭК 62061 или ИСО 13849-1 были выполнены. Эта деятельность соответствует процессу валидации (см. МЭК 62061:2021, раздел 9, и ИСО 13849-1:2015, раздел 10) и предназначена для подтверждения того, что SCS или SRP/CS соответствуют спецификации требований безопасности (SRS).

Примечание 1 — Валидация, которая должна применяться к SCS, включает в себя проверку (например, путем анализа) и тестирование SCS или SRP/CS, чтобы убедиться, что они соответствуют требованиям, изложенным в спецификации требований безопасности (SRS). Поэтому начальная верификация может включать в себя вмешательство в систему управления машины, например моделируются сбои и оценивается результирующая реакция.

Должны быть приняты меры предосторожности для обеспечения того, чтобы верификация не создавала опасности для людей, животных или домашнего скота и не наносила ущерба имуществу и оборудованию.

Начальная верификация проводится лицом, компетентным в области верификации функций безопасности.

Примечание 2 — Требования к квалификации организации и лиц, выполняющих процесс верификации, могут быть рассмотрены на национальном уровне.

Примечание 3 — Требования к квалификации лиц, компетентных в области функциональной безопасности и отвечающих за процесс верификации, могут быть рассмотрены на национальном уровне.

Примечание 4 — Валидация состоит из выполнения анализа (также путем проверки) (см. МЭК 62061:2021, пункт 9.2, или ИСО 13849-1:2015, пункт 10.1.1) и выполнения функциональных испытаний (см. МЭК 62061:2021, пункт 9.3, или ИСО 13849-1:2015, пункт 10.3) при прогнозируемых обстоятельствах в соответствии с планом валидации. Баланс между анализом и испытаниями должен быть обоснован.

Начальная верификация должна предшествовать испытаниям и проводиться до первого применения машины в производстве.

Начальная верификация должна выполняться для подтверждения того, что SCS или SRP/CS, которая является частью системы управления машиной:

- соответствует спецификации требований безопасности (SRS);
- правильно реализована (установлена или смонтирована) согласно соответствующим требованиям МЭК 62061 или ИСО 13849-1 и согласно инструкциям изготовителя компонентов, если применимо;
- визуально не повреждена.

Процедура начальной верификации должна включать по крайней мере проверку следующего, где это уместно:

a) документации;

b) маркировки, закрепленной на машине (например, информация, связанная с безопасностью, показания, предупреждения, типовые таблички);

c) монтажа и информации о монтаже, предоставленной изготовителем компонентов, связанных с безопасностью, и изготовителем машины (на основе компонентов аппаратного обеспечения, связанных с безопасностью, в зависимости от используемой технологии, например защитную световую завесу, приборный блок или одинарные клапаны) (см. информацию о применении, предоставленную изготовителями);

d) времени отклика и поведения функции(й), связанной(ых) с безопасностью (например, параметры и параметризация, испытание динамики функций преобразователя частоты и т. д.);

i) предотвращения манипулирования или побуждения к нарушению средств защиты;

f) поведения, связанного с безопасностью, в условиях сбоя;

g) описания остаточных рисков.

Примечание 5 — Дополнительная информация приведена в МЭК 62061:2021, пункты 9.1.1, 9.1.4 и 9.4, или в ИСО 13849-1:2015, пункты 10.1.2, 10.1.5 и 10.5.

Начальная верификация должна включать все (особые) требования к специальным установкам оборудования или местам их установок.

7.5 Периодическая верификация

7.5.1 Общие положения

Все функции безопасности должны периодически проверяться.

Там, где функция безопасности не запрашивалась в течение одного года, систематические аспекты и накопление сбоев могут привести к потере функции безопасности, выполняемой SCS или SRP/CS.

Примечание 1 — Временные периоды реализуются путем внедрения национальных правил по охране труда и технике безопасности в конкретных странах. Местные власти могут потребовать дополнительной верификации, страховщик имущества также может потребовать дополнительной верификации.

По возможности должны учитываться записи и рекомендации предыдущих периодических процедур верификации.

Периодическая верификация, включающая детальное обследование установки, должна проводиться для подтверждения того, что требования МЭК 62061 или ИСО 13849-1 по-прежнему выполняются.

Степень и объем периодической верификации должны быть такими, чтобы можно было подтвердить отсутствие опасной ситуации, возникающей из-за машины. Периодическая верификация должна включать по крайней мере верификацию поведения, связанного с безопасностью, и остаточного риска.

Должны быть приняты меры предосторожности для обеспечения того, чтобы верификация не создавала опасности для людей, диких животных или домашнего скота и не наносила ущерба имуществу и оборудованию.

Процедура периодической верификации должна включать по крайней мере проверку следующего, где это уместно:

a) наличия документации;

b) маркировки, закрепленной на машине (например, информация, связанная с безопасностью, показания сигналов, предупреждения, типовые таблички);

c) наличия специальной процедуры (процедур) испытаний (например, на основе аппаратных средств, степени и объема испытаний, информации изготовителя машины);

d) времени отклика и поведения функции(й), связанной(ых) с безопасностью (например, параметры и параметризация, испытание динамики функций преобразователя частоты и т. д.);

e) предотвращения манипулирования, мотивации;

f) оценки и описания остаточных рисков в ходе верификации;

g) отсутствия изменений в аппаратном или программном обеспечении;

h) того, были ли изменения верифицированы и валидированы;

i) выполнения технического обслуживания, записей о техническом обслуживании;

j) наличия документов о (ежедневных) испытаниях, выполненных оператором в соответствии с требованиями изготовителя (испытание световой завесы с пробником и т. д.).

Примечание 2 — Дополнительные требования к испытаниям в условиях сбоя могут быть определены в стандартах типа С или в национальных нормативных документах.

Примечание 3 — Предыдущий отчет о расследовании может использоваться в качестве ссылки.

Объем и результаты периодической верификации SCS или SRP/CS или любой части SCS или SRP/CS должны регистрироваться.

Любое повреждение, порча, дефекты или опасное состояние необходимо регистрировать. Кроме того, в соответствии с настоящим стандартом должны регистрироваться существенные ограничения периодической верификации и причины таких ограничений.

Периодическая верификация должна проводиться лицом, компетентным в области верификации функций безопасности.

Примечание 4 — Требования, касающиеся соответствующих квалификаций для предприятий и лиц, могут быть рассмотрены на национальном уровне.

Примечание 5 — Требования, касающиеся соответствующей квалификации лиц, компетентных в области функциональной безопасности и отвечающих за верификацию, могут быть рассмотрены на национальном уровне.

7.5.2 Частота периодической верификации

7.5.2.1 Общие положения

Частота периодической верификации установки определяется с учетом типа установки и SCS или SRP/CS, ее использования и эксплуатации, частоты и качества технического обслуживания и внешних воздействий, которым она подвергается.

Примечание 1 — Максимальный интервал между периодическими верификациями может быть определен правовыми или другими национальными правилами.

Периодический отчет о верификации должен рекомендовать лицу, проводящему периодическую верификацию, интервал до следующей периодической верификации.

Интервал периодической верификации может превышать один год, за исключением следующих случаев, когда может существовать более высокий риск накопления сбоев для машин и механизмов и могут потребоваться более короткие периоды, например рабочие места или места размещения и строительные площадки.

Учитываются результаты и рекомендации предыдущих отчетов, если таковые имеются.

7.5.2.2 Интервал между периодическими верификациями

Условия, при которых интервал периодической верификации может быть определен до двух лет, описаны в 5.2.3.

Примечание — Определение временных интервалов зависит от параметров безопасности устройства защиты. Определение «адекватной» периодичности может быть выполнено в соответствии с формулами или таблицами приложения Н.

7.6 Отчеты о верификации

По завершении верификации существующей установки предоставляется отчет. Такая документация должна включать подробную информацию о таких частях установки, как SCS или SRP/CS, и о других ограничениях верификации, охватываемых отчетом, а также протокол верификации.

Отчет может содержать рекомендации по ремонту и усовершенствованиям, таким как модернизация установки или модернизация предприятия.

Отчет заполняется лицом, ответственным за проведение верификации, или лицом, уполномоченным действовать от имени лица, заказывающего верификацию.

Записи результатов испытаний должны регистрировать результаты соответствующих испытаний.

Отчеты составляются и подписываются.

Документация должна включать как минимум следующие сведения:

- дата испытания;
- кто проводил верификацию;
- участники верификации;
- документация по верификации;
- объем верификации;
- отклонения;
- результаты испытаний.

Результат верификации должен содержать сведения о возможности эксплуатации, связанной с безопасностью. Если это осуществимо только при определенных условиях, то оператор должен быть проинформирован об этом в письменной форме.

Приложение А
(справочное)

Оценка рисков и снижение рисков в соответствии с ИСО 12100

А.1 Общие положения

В настоящем приложении представлен связанный с функциональной безопасностью подход, который описан в ИСО 12100.

Таблицы в настоящем приложении могут помочь реализовать требования ИСО 12100.

Эти таблицы не являются исчерпывающими (за исключением таблицы А.4 и таблицы А.6), и может потребоваться другая информация в зависимости от конкретной машины.

Графа «Комментарии» в таблицах А.1 — А.5 может использоваться для ссылки на исходную информацию или для ссылки на документ в зависимости от обстоятельств.

Данный подход применяется к функциям безопасности, разработанным в соответствии с МЭК 62061 или ИСО 13849-1.

А.2 Принципы оценки рисков

А.2.1 Общие сведения

Для проведения оценки рисков и снижения рисков будут выполнены следующие мероприятия:

- по анализу рисков:
  a) определение пределов машин и механизмов, которые включают предполагаемое использование и их любое разумно предсказуемое неправильное использование;
  b) выявление опасностей и связанных с ними опасных ситуаций;
  c) оценка риска для каждой выявленной опасности и опасной ситуации;
- оценке рисков:
  d) оценка риска и принятие решений о необходимости снижения риска;
- снижению риска:
  e) устранение опасности или снижение риска, связанного с опасностью, посредством защитных мер.

А.2.2 Основная информация, необходимая для оценки риска (в качестве исходных данных для оценки рисков)

Информация, необходимая для оценки риска, представлена в таблице А.1.

Таблица А.1 — Основная информация для оценки риска в соответствии с ИСО 12100

Информация для оценки риска (ссылки на ИСО 12100:2010, пункт 5.2)	Комментарии (например, источник информации, ссылка на документ)
Описание машины: 5.2 a)	
Характеристики пользователя	
Техническое задание на машину: описание стадий жизненного цикла	
Техническое задание на машину: чертежи конструкции машины	
Техническое задание на машину: необходимые источники энергоснабжения	
Документация на ранее выпущенные и используемые аналогичные машины	
Информация по эксплуатации машины	
Директивы, стандарты и прочая действующая документация: 5.2 b)	
Свод применимых положений	
Соответствующие стандарты	
Соответствующие технические характеристики	
Соответствующие паспорта безопасности	
Информация, связанная с опытом эксплуатации: 5.2 c)	
Статистика несчастных случаев, поломок и сбоев	

Окончание таблицы А.1

Информация для оценки риска (ссылки на ИСО 12100:2010, пункт 5.2)	Комментарии (например, источник информации, ссылка на документ)
Статистика случаев причинения вреда здоровью	
Результаты опыта пользователей аналогичных машин	
Информация о соответствующих эргономических принципах: 5.2 d)	
Сравнение аналогичных опасных ситуаций, связанных с различными типами машин	

А.2.3 Анализ рисков

А.2.3.1 Определение ограничений, налагаемых на машины и механизмы

Ограничения на использование включают предполагаемое использование и разумно предсказуемое неправильное использование. Рассматриваемые аспекты перечислены в таблице А.2.

Таблица А.2 — Определение ограничений, налагаемых на машины и механизмы, в соответствии с ИСО 12100

Определение ограничений (ссылки на ИСО 12100:2010, пункт 5.3)	Комментарии (например, источник информации, ссылка на документ)
Эксплуатационные ограничения	
Различные режимы работы машины и разные процедуры вмешательства пользователей, в том числе и вмешательство, вызванное сбоем в работе	
Характер использования машины лицами определенного пола, возраста, с правой либо левой доминирующей рукой, либо с ограниченными физическими возможностями	
Предполагаемый уровень квалификации, опыта или способностей пользователей (операторов, обслуживающего персонала или техников, стажеров и учеников, а также рядовых граждан)	
Подверженность других лиц опасностям, связанным с машинами (лиц, которые, вероятно, хорошо осведомлены, лиц с низкой осведомленностью, лиц, которые, вероятно, очень мало осведомлены)	
Пространственные ограничения	
Диапазон перемещений машины или ее частей	
Пространственные требования для персонала, взаимодействующего с машиной как в процессе эксплуатации, так и при ее техническом обслуживании	
Взаимодействие человека с машиной, такое как интерфейс «оператор-машина»	
Интерфейс «машина-источник питания»	
Временные ограничения	
Предельный срок службы машины и/или некоторых ее компонентов (оснастки, изнашиваемых частей, электромеханических компонентов и т. д.) с учетом ее предполагаемого использования и разумно предсказуемого неправильного использования	
Рекомендуемые интервалы обслуживания	
Прочие ограничения	
Свойства обрабатываемых материалов	
Содержание помещения — необходимый уровень чистоты	
Окружающая среда (рекомендуемые минимальные и максимальные температуры, пониженная и повышенная влажность, воздействие прямых солнечных лучей, пыли и т. п.)	

А.2.3.2 Идентификация опасностей

Важным шагом в любой оценке риска машин и механизмов является систематическая идентификация разумно предсказуемых опасностей (постоянных опасностей и тех, которые могут появиться неожиданно), опасных ситуаций и/или опасных событий на всех этапах жизненного цикла машины. Таблица А.3 может помочь проектировщику определить опасности.

Таблица А.3 — Принципы идентификации опасностей в соответствии с ИСО 12100

Идентификация опасностей (ссылки на ИСО 12100:2010, пункт 5.4)	Комментарии (например, источник информации, ссылка на документ)
Взаимодействие человека с машиной на протяжении всего ее жизненного цикла	
Идентификация задачи должна рассматривать все задачи, возникающие на любом этапе жизненного цикла машины:	
наладка	
испытание	
обучение/программирование	
смена режимов/инструментов	
пуск	
все виды рабочих режимов	
торможение машины	
повторный пуск после незапланированной остановки	
очистка и содержание помещения	
профилактическое и корректирующее техническое обслуживание	
Возможные состояния машины	
Машина выполняет функции, для которых она предназначена (машина работает нормально)	
Машина не выполняет функции, для которых она предназначена (т.е. неисправна), по разным причинам (например, изменение свойств или размеров обрабатываемого материала, повреждение одной или нескольких составных частей машины или приспособлений, внешние воздействия, нарушение ее энергоснабжения и т. д)	
Непреднамеренное поведение оператора или разумно предсказуемое неправильное использование машины	
Предельный срок службы машины и/или некоторых ее компонентов (оснастки, изнашиваемых частей, электромеханических компонентов и т. д.) с учетом ее предполагаемого использования и разумно предсказуемого неправильного использования	
Рекомендуемые интервалы обслуживания	
Прочие ограничения	
Примеры:	
утрата оператором возможности управления машиной (особенно для переносных или движущихся машин)	
рефлекторное поведение оператора в случае неисправности машины	
поведение, возникающее из-за недостаточной концентрации или небрежности, из-за стремления поддерживать работоспособность машины	
поведение отдельных категорий людей	

А.2.3.3 Оценка рисков

После идентификации опасности оценка риска должна выполняться для каждой опасной ситуации путем определения элементов риска, перечисленных в таблице А.4.

Таблица А.4 — Оценка рисков в соответствии с ИСО 12100

Элементы риска (ссылки на ИСО 12100:2010, пункт 5.5.2)	Комментарии (например, источник информации, ссылка на документ)
Серьезность возможного повреждения	
Серьезность возможного повреждения или ущерба здоровью, например, легкий, серьезный, летальный исход	
Вероятность нанесения такого повреждения	
Подверженность людей опасности	
Возникновение опасного события	
Возможность избежать повреждения или ограничить его последствия	

В дополнение к таблице А.4 рассматривают аспекты, приведенные в таблице А.5.

Таблица А.5 — Дополнительно рассматриваемые аспекты при оценке рисков в соответствии с ИСО 12100

Аспекты, рассматриваемые при оценке рисков (ссылки на ИСО 12100:2010, пункт 5.5.3)	Комментарии (например, источник информации, ссылка на документ)
Лица, подвергающиеся опасности	
Все люди (операторы и другие лица)	
Тип, частота и продолжительность воздействия опасности	
Необходим доступ к машине во время погрузки/разгрузки, настройки, обучения, корректировки или смены технологического процесса, чистки, обнаружения неисправностей и технического обслуживания	
Работы, для выполнения которых требуется приостанавливать действие защитных мер	
Соотношение воздействия опасности и ее последствий	
Воздействие опасности и ее последствий для каждой опасной ситуации	
Человеческий фактор	
Взаимодействие лица (лиц) с оборудованием	
Взаимодействие между отдельными операторами	
Аспекты, связанные со стрессом	
Эргономические аспекты	
Способность лиц осознавать риски	
Пригодность защитных мер	
Обстоятельства, которые могут привести к нанесению вреда здоровью	
Возможность отключения защитных мер или действия в обход них	
Защитные меры замедляют производство, мешают какой-либо другой деятельности или противоречат предпочтениям пользователя	
Защитная мера трудна в применении	

Окончание таблицы А.5

Аспекты, рассматриваемые при оценке рисков (ссылки на ИСО 12100:2010, пункт 5.5.3)	Комментарии (например, источник информации, ссылка на документ)
В производственный процесс вовлекаются другие лица, помимо оператора	
Защитная мера не признается пользователем или не принимается как подходящая для своей функции	
Способность поддерживать защитные меры	
Условие, необходимое для обеспечения требуемого уровня защиты, если это невозможно — поощряют отмену защитной меры	
Информация для пользователя	
Соответствующая информация для обеспечения мер по снижению риска	

А.2.3.4 Оценка рисков

Необходимо провести оценку рисков, чтобы определить, требуется ли снижение риска. Если снижение риска требуется, то должны быть выбраны и применены соответствующие защитные меры. Применение трехэтапного метода в соответствии с ИСО 12100 позволяет достичь адекватного снижения риска.

В процессе оценки риска риски, связанные с машинами или частями машин, можно сравнить с рисками аналогичных машин или частей машин.

А.3 Снижение риска за счет защитных ограждений и дополнительных мер защиты

А.3.1 Общие сведения

Снижение риска должно осуществляться путем применения иерархического подхода, называемого трехэтапным методом:

1) шаг 1. Меры по разработке безопасной конструкции самой машины;
2) шаг 2. Защитные ограждения и/или другие дополнительные защитные меры;
3) шаг 3. Информация для пользователя.

Примечание — Шаг 2 применим к МЭК 62061 или ИСО 13849-1, см. раздел 4.

Меры по разработке безопасной конструкции самой машины являются первым и наиболее важным шагом в процессе снижения риска. Это должно быть достигнуто путем предотвращения опасностей или снижения рисков путем подходящего выбора конструктивных особенностей для самой машины и/или взаимодействия между незащищенными лицами и машиной.

Информация по классификации функций безопасности, реализуемых защитными ограждениями и дополнительными мерами защиты, описана в ИСО 12100:2010, пункт 6.3.

Там, где разработка безопасной конструкции самой машины невозможна, будут реализованы другие меры.

Поэтому снижение риска в соответствии с шагом 2 итеративного процесса снижения риска, описанного в ИСО 12100, может быть достигнуто путем разработки для каждой опасности адекватных защитных ограждений и дополнительных мер защиты, чтобы:

a) снизить вероятность опасного события; или
b) ограничить продолжительность или возникновение опасного события; или
c) уменьшить последствия опасного события.

Приоритетом в процессе снижения риска является устранение опасностей с помощью разработки безопасной конструкции самой машины.

Устранение опасностей на этапе проектирования является наиболее эффективным методом снижения риска, поскольку устраняется источник нанесения вреда.

Если опасности не могут быть устранены или риски не могут быть адекватно снижены с помощью разработки безопасной конструкции самой машины, то будут применяться дополнительные защитные меры, такие как:

a) снижение вероятности возникновения опасного события путем устранения вероятных причин; или
b) наложение ограничения на подверженность опасностям; или
c) повышение возможности избежать вреда или по крайней мере снизить его интенсивность.

А.3.2 Меры по разработке безопасной конструкции самой машины

Это защитные меры, которые либо устраняют опасности, либо снижают риски, связанные с опасностями, путем изменения конструктивных или эксплуатационных характеристик машины без использования защитных ограждений или защитных устройств.

А.3.3 Выбор защитных ограждений и дополнительных защитных мер

А.3.3.1 Общие положения

Защитные меры могут быть пассивными или активными.

А.3.3.2 Стационарные защитные ограждения в качестве «пассивных» защитных мер

Стационарная защита предотвращает доступ к опасности и работает непрерывно. Она не зависит от системы управления машиной (MCS) и не нуждается в активации для достижения снижения риска. Такая защита является «пассивной» защитной мерой.

Примерами «пассивных» защитных мер являются:

- ограждения;
- неподвижные средства защиты для предотвращения доступа в опасные зоны.

Они обеспечивают защиту, сокращая продолжительность воздействия опасности. Приведено лишь предельное снижение риска в зависимости от серьезности вреда.

Примечание — В МЭК 61508 используется термин «другие меры по снижению риска», которые не основаны на какой-либо системе, связанной с безопасностью, см. МЭК 61508-1:2010, пункт 7.6.2.1.

Пассивные защитные меры не входят в область применения МЭК 62061, ИСО 13849-1 или ИСО 13849-2.

А.3.3.3 Функции безопасности как «активные» защитные меры

А.3.3.3.1 Общие положения

Функция безопасности, выполняемая SCS, запускается в ответ на определенное изменение измеряемой входной характеристики (например, датчика или переключателя). Такая функция безопасности является «активной» защитной мерой.

Они предназначены для снижения риска, создаваемого, например, следующими событиями:

a) взаимодействие человека с машиной (операции) (см. А.3.3.3.2);

b) отказы системы автоматического управления машиной (см. А.3.3.3.3);

c) ненадлежащее использование машины (см. А.3.3.3.4).

Как правило, из всех дополнительных мер защиты они оказывают наибольшее влияние на снижение вероятности возникновения вреда.

Примечание — В МЭК 61508 используется термин «E/E/PE системы, связанные с безопасностью», которые не основаны ни на одной системе, связанной с безопасностью, см. МЭК 61508-1:2010, пункт 7.6.2.1.

А.3.3.3.2 Взаимодействие человека с машиной (операции)

Не исключено, что люди могут подвергнуть себя опасности при выполнении определенной задачи или работе машины.

Примеры устройств, используемых для активных защитных мер, подходящих для снижения рисков, возникающих в результате взаимодействия человека с машиной:

- чувствительные защитные устройства для обнаружения лиц, входящих в опасную зону или находящихся в ней (например, фотоэлектрические защитные барьеры, лазерные сканеры, чувствительные коврики);
- устройства, связанные с командами машины (например, разрешающее устройство, удерживающие устройства управления);
- блокировочные ограждения.

Они предназначены для работы сразу после конкретного инициирующего события. Их роль заключается в обеспечении того, чтобы опасные части машины не травмировали людей или части человеческого тела.

«Запрос» на защиту формируется лицом при его взаимодействии (операциях) с процессом машины.

А.3.3.3.3 Отказы системы автоматического управления машиной

Возможно, что отказ компонента системы управления машиной, который участвует в определенном процессе машины, может создать опасные ситуации, такие как горячие поверхности, пламя, чрезмерные вибрации, взрывы и т. д.

Примеры устройств, используемых для активных защитных мер, подходящих для снижения риска из-за отказов компонентов:

- ограничители крутящего момента;
- устройства для ограничения давления или температуры;
- ограничители превышения скорости;
- устройства контроля за излучением или газом;
- пожарные и дымовые детекторы.

Они используются в качестве средства предотвращения и предназначены для работы до того, как произойдет конкретное инициирующее событие. Их роль заключается в обеспечении того, чтобы авария не произошла, или, по крайней мере, в замедлении ее развития или ограничении до приемлемого уровня отклонения процесса.

Неисправность системы управления машины может вызвать функцию безопасности.

А.3.3.3.4 Разумно предсказуемое ненадлежащее использование машины

Возможно, что интенсивное использование машины из-за недостатка времени или предельного режима, из-за чрезмерных нагрузок или из-за обработки неподходящего материала может вывести работу машины за пределы возможностей ее конструкции, что, в свою очередь, может привести к механическим отказам самой машины или повреждению изделий, подлежащих обработке, и далее может создать риски для людей.

Примеры устройств, используемых для реализации активных защитных мер, подходящих для снижения риска из-за разумно предсказуемого неправильного использования:

- ограничители крутящего момента;
- ограничители давления;
- ограничители превышения скорости;
- тензодатчики;
- датчики перегрузки по току.

«Запрос» создается в результате перегрузки машины из-за ее разумно предсказуемого неправильного использования.

А.3.3.3.5 Снижение риска за счет дополнительных защитных мер

Для достижения дальнейшего снижения риска может потребоваться использование дополнительных защитных мер с учетом предполагаемого использования и разумно предсказуемого неправильного использования машины.

Дополнительными защитными мерами, основной эффект которых заключается в предотвращении или ограничении вреда, являются:

- аварийный останов;
- меры по обеспечению безопасного доступа к машинам и механизмам;
- меры по эвакуации и спасению людей, попавших в затруднительное положение.

Дополнительными защитными мерами, основным эффектом которых является сокращение продолжительности воздействия опасности, являются:

- устройства, подходящие для отключения энергии, такие как отсечные клапаны и отсечные выключатели;
- устройства, пригодные для рассеивания энергии, такие как клапаны сброса давления;
- затворы механического действия для предотвращения перемещений.

А.4 Другие защитные меры (основанные на процедурах)

А.4.1 Общие положения

Чтобы гарантировать, что пассивные, активные и дополнительные защитные меры остаются эффективными на протяжении всего жизненного цикла машины, необходимы дополнительные действия, основанные на процедурах и организации.

Примечание — Важно упомянуть эти аспекты, даже если они выходят за рамки настоящего стандарта, поскольку они играют важную роль в обеспечении безопасности на рабочем месте.

А.4.2 Процедуры технического обслуживания

Возможно, что отсутствие технического обслуживания может привести к механическим отказам или ошибкам некоторых частей машины, что может привести к рискам для людей.

Примерами отказов из-за отсутствия технического обслуживания являются:

- плохая смазка или
- потеря охлаждающих жидкостей.

Чтобы уменьшить эти типы опасностей, необходимо разработать и внедрить подробные инструкции по техническому обслуживанию.

А.4.3 Организационные рабочие процедуры

Как минимум должны действовать следующие организационные меры:

- четко определенные роли и обязанности работников, руководителей и менеджмента;
- план периодических тренировок рабочих;
- наличие подходящих инструментов для технического обслуживания и верификации;
- план периодических проверок полноты безопасности защит;
- план эвакуации и аварийных процедур;
- средство отслеживания периодической верификации.

А.5 Защитные ограждения и защитные устройства в соответствии с ИСО 12100

А.5.1 Общие положения

Защитные ограждения и устройства защиты будут использоваться для защиты людей во всех случаях, когда меры по разработке безопасной конструкции самой машины не позволяют в разумных пределах устранить опасности или в достаточной степени снизить риски. Возможно, придется принять дополнительные защитные меры, включающие дополнительное оборудование (например, оборудование аварийной остановки).

Защитные ограждения являются физическим барьером, спроектированы как часть машины для обеспечения защиты и могут быть классифицированы в соответствии с таблицей А.6.

А.5.2 Блокирующее ограждение с функцией пуска, с функцией ручного сброса

Восстановление функции безопасности путем сброса защиты отменяет команду остановки. Если указано в оценке риска, эта отмена команды остановки будет подтверждена ручным, отдельным и предполагаемым действием (ручной сброс).

Таблица А.6 — Защитные ограждения в соответствии с ИСО 12100

Защитные ограждения и дополнительные меры (ссылки на ИСО 12100:2010, пункт 6.3)	Комментарии (например, источник информации, ссылка на документ)
Перемещаемое ограждение (см. ИСО 12100:2010, пункт 3.27.2)	
Может быть открыто без использования инструментов	
Регулируемое ограждение (см. ИСО 12100:2010, пункт 3.27.3)	
Неподвижное или перемещаемое ограждение, регулируемое в целом	
Блокирующее защитное ограждение (см. ИСО 12100:2010, пункт 3.27.4)	
Ограждение, оснащенное блокировочным устройством, где	
опасные функции машины «прикрыты» ограждением	
открытие ограждения подает команду на остановку	
только при закрытом ограждении машина может выполнять опасные функции	
Блокирующее защитное ограждение с фиксацией закрытия (см. ИСО 12100:2010, пункт 3.27.5)	
Ограждение, оснащенное блокировочным устройством и устройством фиксации ограждения в закрытом положении, где	
опасные функции машины могут выполняться только в том случае, если ограждение закрыто и заблокировано	
ограждение остается закрытым и заблокированным до тех пор, пока не исчезнет риск из-за опасных функций машины	
только при закрытом и заблокированном ограждении машина может выполнять опасные функции	
Блокирующее ограждение с функцией пуска (см. ИСО 12100:2010, пункт 3.27.6)	
Специальное блокирующее ограждение, подающее после закрытия команду пуска опасной(ых) функции(й) машины без использования отдельного органа управления пуском	

Функция ручного сброса:

- обеспечивается через отдельное и управляемое вручную устройство, которое отделено от команды запуска внутри SCS или SRP/CS;
- достигается только в том случае, если все затронутые функции безопасности и ограждения работают;
- не инициирует опасную ситуацию самостоятельно;
- запускается преднамеренным действием;
- включает систему управления для приема отдельной команды запуска;
- принимает изменение сигнала.

Примечание — Оценка риска может определить, требуется ли функция безопасности ручного сброса и отличается ли ее значение SIL или PLr от соответствующей функции безопасности.

А.5.3 Защитное устройство в соответствии с ИСО 12100

Защитное устройство — это средство защиты, отличное от ограждения; примеры приведены в таблице А.7.

Таблица А.7 — Примеры защитных устройств согласно ИСО 12100

Защитные ограждения и дополнительные защитные меры (ссылки на ИСО 12100:2010, пункт 6.3)	Комментарии (например, источник информации, ссылка на документ)
Блокировочное устройство (см. ИСО 12100:2010, пункт 3.28.1)	
Устройство механического, электрического или другого типа, препятствующее включению опасных функций машины при определенных условиях (как правило, пока защитное ограждение не закрыто)	

Окончание таблицы А.7

Защитные ограждения и дополнительные защитные меры (ссылки на ИСО 12100:2010, пункт 6.3)	Комментарии (например, источник информации, ссылка на документ)
Устройство разблокировки (см. ИСО 12100:2010, 3.28.2)	
Управляемое вручную дополнительное устройство, которое в сочетании с органом управления пуском, может позволить машине выполнять ее функции только при постоянном воздействии вручную на это устройство	
Удерживающее управляющее устройство (см. ИСО 12100:2010, пункт 3.28.3)	
Управляющее устройство, которое инициирует и поддерживает функционирование машины, только пока активирован механизм ручного управления (исполнительный механизм)	
Двуручное управляющее устройство (см. ИСО 12100:2010, пункт 3.28.4)	
Управляющее устройство, которое для включения и поддержания опасных функций машины требует одновременного воздействия обеих рук оператора, что является защитной мерой только для человека, управляющего машиной с помощью этого устройства	
Сенсорное предохранительное оборудование (SPE) (см. ИСО 12100:2010, 3.28.5)	
Оборудование для обнаружения присутствия людей или частей тела человека в опасной зоне, генерирующее соответствующий сигнал в систему управления с целью снижения риска для лиц, попавших в эту зону	
Активное оптоэлектронное предохранительное устройство (см. ИСО 12100:2010, пункт 3.28.6)	
Устройство, считывающая функция которого выполняется оптоэлектронными излучающими и принимающими элементами, предназначенное для обнаружения присутствия непрозрачного объекта в установленной зоне (зоне обнаружения) за счет прерывания этим объектом оптического излучения, генерируемого устройством	
Механическое ограничительное устройство (см. ИСО 12100:2010, пункт 3.28.7)	
Устройство, представляющее собой прочную механическую преграду (например, клин, палец, упор, тормозной башмак), способную препятствовать любому опасному перемещению машины или ее частей	
Ограничивающее устройство (см. ИСО 12100:2010, пункт 3.28.8)	
Устройство, препятствующее машине или опасным режимам работы превысить предельные значения параметров, предусмотренные конструкцией машины (например, пространственные ограничения, предельные значения давления, нагрузки)	
Устройство управления ограниченным перемещением (см. ИСО 12100:2010, пункт 3.28.9)	
Управляющее устройство, однократное приведение которого в действие совместно с системой управления машиной допускает только ограниченное перемещение какого-либо элемента машины	

А.5.4 Ручное устройство (и процедура) местного управления

При местном управлении машиной, например с помощью переносного устройства управления, должны выполняться следующие требования:

- средства, выбранные для местного управления, должны быть расположены за пределами опасной зоны;
- во избежание опасных ситуаций запуск опасных условий эксплуатации в локальной зоне с оцененным риском должен быть возможен только от одного устройства местного управления;
- переключение управления между местным и главным не должно создавать опасную ситуацию;
- система управления должна быть спроектирована таким образом, чтобы подача команд с разных постов управления не приводила к опасной ситуации. Может быть необходимо исключить использование других элементов управления при работе местного устройства управления.

А.5.5 Устройство (и процедура) выбора параметров вручную

Когда параметры, связанные с безопасностью, например положение, скорость, температура, время, крутящий момент или давление, отклоняются от заранее установленных пределов, SCS или SRP/CS инициируют соответствующие меры (например, запуск остановки, предупреждающего сигнала, сигнализации).

Если ошибки при ручном вводе данных, связанных с безопасностью, в программируемые или конфигурируемые электронные системы могут привести к опасной ситуации, то в SCS или SRP/CS должна быть предусмотрена система проверки данных, например проверка пределов, формата и/или логических входных значений.

Стандарты типа С на изделие могут потребовать систему проверки данных для некоторых или всех параметров, введенных вручную.

А.5.6 Устройство (и процедура) выбора режима работы вручную

Рекомендуются следующие систематические аспекты:

- одновременно может быть активным только один режим работы; каждый выбранный режим работы будет четко идентифицирован или обозначен;
- выбор режима сам по себе не инициирует работу машины. Потребуется отдельное включение управления запуском;
- при переходе из одного режима работы в другой включаются функции безопасности и/или меры по снижению риска, необходимые для выбранного режима работы; без потери охвата защитой во время перехода.

А.5.7 Устройство (и процедура) управления питанием

Когда происходят отклонения уровней энергоснабжения за пределы расчетного рабочего диапазона, включая его потерю, SCS или SRP/CS продолжают обеспечивать или инициировать выходной(ые) сигнал(ы), который(е) позволит(ят) другим частям системы машины поддерживать безопасное состояние (см. также ИСО 14118).

А.6 Метод формирования матрицы рисков

А.6.1 Обзор

Оценка риска функций безопасности будет выполняться для каждой опасности путем определения параметров риска, как определено в ISO/TR 14121-2, следующим образом:

- степень тяжести вреда Se и
- вероятность возникновения этого вреда, которая является функцией:
  - частоты и продолжительности воздействия на людей опасности Fr,
  - вероятности возникновения опасного события Pr,
  - возможности избежать или ограничить вред Av.

Если расчетный риск будет снижен путем внедрения SCS или SRP/CS, то оценка риска позволяет определить требуемую полноту безопасности для таких SCS или SRP/CS. Требуемая полнота безопасности определяется требуемым значением SIL в соответствии с МЭК 62061 или значением PL_r в соответствии с ИСО 13849-1.

Подходы к определению требуемого значения SIL или PL_r более подробно описаны в МЭК 62061:2021, приложение А (формирование матрицы), и ИСО 13849-1:2015, рисунок А.1 (граф рисков).

Другие подходы можно найти в МЭК 61508. С точки зрения машинного оборудования подход LOPA неприменим или не подходит, поскольку среда машинного оборудования с точки зрения пользователя отличается от таковой в подходе для перерабатывающей промышленности, например, в МЭК 61511.

А.6.2 Общие положения

Методология формирования матрицы позволяет оценить параметры риска с использованием масштабирования и оцифровывания рассматриваемого параметра. Основное различие между ИСО 13849-1:2015, рисунок А.1, и матричным подходом МЭК 62061 заключается в параметре риска «существенность». МЭК 62061 имеет четыре уровня для оценки, в то время как ИСО 13849-1 предлагает только два уровня.

Кроме того, формирование матрицы позволяет оценить PL_r на основе целевых значений PFH в дополнение к оценке SIL. Поскольку PL_r c < 3,0 E-06 (или 30 % от 1,0 E-05), то SIL 1 может быть объединением соответственно PL_r c и PL_r b. PL_r a соответствует «другим мерам» (ОМ) и основан на базовых требованиях технического проектирования, таких как основные принципы безопасности. Систематические аспекты являются определяющими и нет необходимости в требуемом значении PFH.

Примечание — Уровень менее SIL 1 не определен и не добавляет какой-либо величины, поэтому других мер достаточно.

А.6.3 Методология МЭК 62061:2021, приложение А

Точкой входа является оценка параметра риска существенность Se. На основе выбранной строки для Se следующим шагом является оценка трех других параметров риска путем выбора соответствующего значения между 1 и 5.

Добавление этих значений позволяет определить класс Cl = Fr + Pr + Av.

Пересечение между строкой Se и столбцом Cl приводит к требуемым уровням SIL и PL_r

На рисунке А.1 показаны все параметры риска в виде объединения таблиц А.1 — А.6 МЭК 62061:2021.

А.7 Подход, основанный на графе рисков

А.7.1 Общие положения

Граф риска основан на параметрах риска, где вероятность возникновения не представлена и считается высокой.

А.7.2 Методология назначения SIL в ИСО 13849-1:2015, приложение А

Граф риска представлен на рисунке А.2.

Последствия	Существенность Се	Класс Cl = Fr + Pr + Av												
		3	4	5	6	7	8	9	10	11	12	13	14	15
Смерть, потеря глаза или руки	4	SIL 1		SIL 2			SIL 2			SIL 3			SIL 3	
		PL_r b	PL_r c	PL_r d			PL_r d			PL_r e			PL_r e	
Постоянная травма, потеря пальцев	3			OM			SIL 1			SIL 2			SIL 3	
				PL_r a			PL_r b	PL_r c		PL_r d			PL_r e	
Обратимая травма, медицинская помощь	2	SIL (или PL) не требуется					OM			SIL 1			SIL 2	
							PL_r a			PL_r b	PL_r c		PL_r d	
Обратимая травма, первая помощь	1	OM – другие методы (например, основные принципы безопасности, МЭК 62061:2021, таблица 7)								OM			SIL 1	
										PL_r a			PL_r b	PL_r c

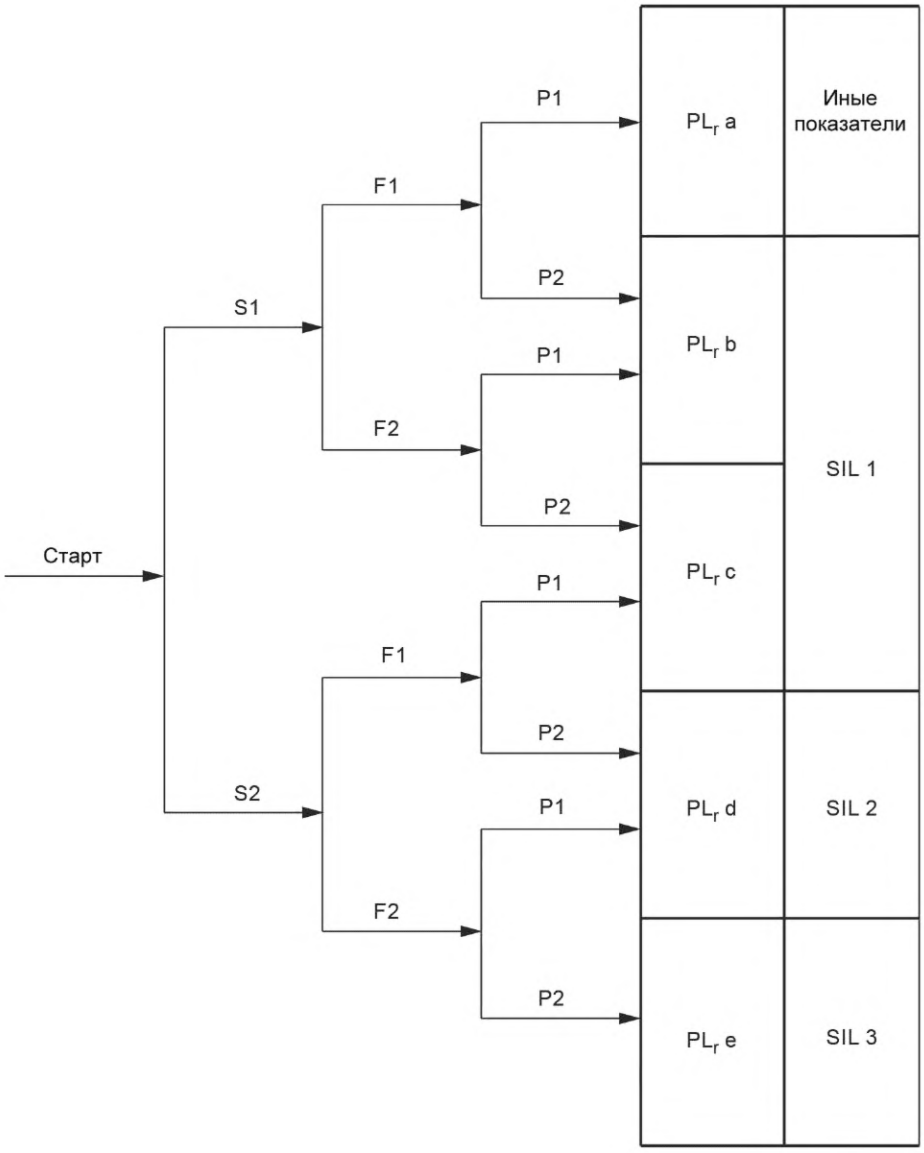
Частота и продолжительность воздействия (Fr)

Частота воздействия	Частота Fr	
	Продолжительность воздействия ≥ 10 мин	Продолжительность воздействия < 10 мин
≥ 1 в час	5	5
от < 1 в час до ≥ 1 в день	5	4
от < 1 в день до ≥ 1 за 2 недели	4	3
от < 1 за 2 недели до ≥ 1 в год	3	2
от < 1 в год	2	1

Вероятность возникновения	Вероятность (Pr)
Очень высокая	5
Вероятно	4
Возможно	3
Редко	2
Незначительная	1

Возможность избежать или ограничить вред (Av)	
Невозможно	5
Редко	3
Вероятно	1

Рисунок А.1 — Подход к назначению SIL



S — серьезность травмы	F — частота и/или подверженность опасности	P — возможность избежать опасности или ограничить вред
S1 легкая (нормально обратимая травма) S2 серьезная (как правило, необратимые травмы или летальный исход)	F1 От редкого к менее частому F2 частое и непрерывное и/или длительное время воздействия	P1 возможно при определенных условиях P2 едва ли возможно

Рисунок А.2 — Метод построения графа рисков по ИСО 13849-1:2015, рисунок А.1 с назначением SIL

Приложение В
(справочное)

Методология проектирования SCS или SRP/CS

В.1 Общие положения

Функции безопасности, выполняемые SCS или SRP/CS, реализуют:

- используя уже разработанную SCS или SRP/CS, отвечающую требованиям полноты безопасности, или
- проектируя новую SCS или SRP/CS с использованием предварительно спроектированных подсистем, или проектируя новые подсистемы, или сочетая и то и другое.

Примечание 1 — Методология проектирования SCS соответствует МЭК 62061, а методология проектирования SRP/CS соответствует ИСО 13849-1.

Примечание 2 — Проектирование сложных программируемых электронных подсистем или элементов подсистем не входит в область применения МЭК 62061.

В.2 План функциональной безопасности

В данном контексте план функциональной безопасности определяет общую управленческую и техническую деятельность, необходимую для проектирования, внедрения и интеграции одной или нескольких SCS или SRP/CS, используемых для безопасности машин.

В таблице В.1 представлен обзор основных требований плана функциональной безопасности.

Таблица В.1 — Обзор плана функциональной безопасности

Деятельность	Соответствующий раздел/подраздел МЭК 62061:2021	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Деятельность (т. е. проектирование SCS, программное обеспечение, валидация)	Раздел 4		
Политика и стратегия	Раздел 4		
Стратегия для прикладного программного обеспечения	Раздел 8		
Ответственные лица, подразделения (или иные подразделения)	Раздел 4		
Запись и ведение информации для каждой SCS	Раздел 10		
Управление конфигурацией (т.е. определение архитектуры SCS, контроль, регистрация/отчетность, проверка)	Подраздел 4.4, раздел 10		
Управление изменениями (и анализ влияния, если изменения внесены в SCS)	Подраздел 4.5, раздел 10		
План верификации (т. е. кто выполняет, методы, испытательное оборудование, критерии приемки)	Раздел 9, раздел 10		
План валидации (т. е. требования, подлежащие валидации, результаты верификации, режимы работы, критерии приемки)	Раздел 9, раздел 10		

Примечание — План функциональной безопасности может быть частью общей технической документации на машину и не обязательно представляет собой единый документ.

В.3 Требования безопасности

В.3.1 Общие положения

Настоящий раздел устанавливает процедуры для определения требований к функции(ям) безопасности, которые должны быть реализованы SCS или SRP/CS.

Каждая функция безопасности определяется:

- спецификацей функциональных требований;
- спецификацей требования к полноте безопасности.

B.3.2 Функциональные требования

Входная информация, полученная в результате применения общей оценки риска и процесса снижения риска для конкретной конструкции машины, необходима и описана в 4.1. Эта информация будет доступна как для разработки спецификации функциональных требований (см. таблицу B.2), так и для спецификации требований к полноте безопасности SCS или SRP/CS.

Таблица B.2 — Обзор основных функциональных требований

Функциональные требования	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Описание функции безопасности	- Ограничения машины согласно ИСО 12100. - Риск, связанный с конкретной опасной ситуацией в соответствии с ИСО 12100[a]		
Рабочая среда	- Ограничения машины согласно ИСО 12100 (например, электромагнитная помехоустойчивость, температура, влажность, пыль, химические вещества, механическая вибрация и удар)[a]		
Состояние(я) (например, режим работы) машины	- Спецификации для предполагаемого выполнения соответствующих мер по снижению риска/защитных мер в соответствии с ИСО 12100[a]		
Приоритет			
Сброс			
Частота работы			
Время отклика			
Реакция на сбой	Условия перезапуска, ограничения		
Интерфейсы с другими функциями машины			
Тесты	Испытательное оборудование		
Другие специальные требования			
[a] Входную информацию, полученную в процессе оценки рисков в соответствии с ИСО 12100, см. в 4.4.			

B.3.3 Требования к полноте безопасности

Требуемая полнота безопасности для каждой функции безопасности, выполняемой SCS или SRP/CS, будет определена в значениях SIL в соответствии с таблицей B.3 и документально оформлена.

Таблица B.3 — Значения SIL и предельные значения PFH

SIL	Предельные значения PFH (1/ч)
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

B.4 Защита от неожиданного запуска

Неожиданный запуск машины имеет значение во время всех проектных работ, и будут рассмотрены соответствующие требования ИСО 14118. Например, при проектировании функции останова, связанной с безопасностью, предотвращение неожиданного запуска будет рассматриваться в контексте этой функции безопасности: это не означает, что предотвращение неожиданного запуска является отдельной или дополнительной функцией безопасности, но оно будет рассмотрено в дополнение к проектируемой функции безопасности.

Дальнейшие примеры неожиданного запуска:

- существует опасность неожиданного перезапуска машины во время переналадки обрабатываемой детали или во время технического обслуживания;

- функция «ручной сброс» должна быть функцией безопасности;
- блокировочное устройство, связанное с блокировочным ограждением и с функцией запуска, выполнено таким образом, что его отказ не может привести к непреднамеренному/неожиданному запуску.

В.5 Декомпозиция функции безопасности

В.5.1 Общие положения

На основании спецификации требований безопасности при проектировании SCS или SRP/CS может выполняться:

- выбор подсистем,
- определение полноты безопасности,
- соблюдение требований систематической полноты безопасности SCS или SRP/CS, включая, где это применимо, электромагнитную помехоустойчивость, защиту информации, периодические испытания и программное обеспечение.

В.5.2 Архитектура подсистемы, основанная на декомпозиции сверху вниз

SCS может включать в себя:

- одну или несколько предварительно спроектированных подсистем и/или
- одну или несколько подсистем, разработанных в соответствии с настоящим стандартом на основе элемента(ов) подсистемы.

В.6 Проектирование SCS с использованием подсистем

Каждая функция безопасности будет декомпозирована и представлена структурой подфункций. Каждая подфункция будет выполняться подсистемой (распределенной подсистеме).

Типичная декомпозиция функции безопасности представлена на рисунке В.1.

Как показано на рисунке В.1, значения SIL, которые могут быть достигнуты с помощью SCS, будут рассматриваться отдельно для каждой функции безопасности и определяться на основе SIL и значения PFH для каждой подсистемы следующим образом:

- достигаемое значение SIL равно или меньше самого низкого значения SIL любой из подсистем и
- значение SIL ограничивается суммой значений PFH всех подсистем.

<table>
<tr><td colspan="4">Функция безопасности, выполняемая SCS или SRP/CS, с требуемой полнотой безопасности</td></tr>
<tr><td>1</td><td>Входная подфункция (инициирующее событие, причина)</td><td>Логическая подфункция</td><td>Выходная(ые) подфункция(и) (привод машины, полезный эффект)</td></tr>
<tr><td>2</td><td>Подсистема, выполняющая подфункцию (выделение подсистемы)</td><td>Подсистема, выполняющая подфункцию (выделение подсистемы)</td><td>Подсистема, выполняющая подфункцию (выделение подсистемы)</td></tr>
<tr><td>3.a</td><td>Выбор предварительно спроектированной подсистемы
в соответствии с МЭК 62061, или МЭК 61508, или МЭК 61496, или ИСО 13849-1:
- SIL или PL и
- PFH
ИЛИ</td><td>Предварительно спроектированная подсистема в соответствии с МЭК 61508 или МЭК 61496:</td><td>Выбор предварительно спроектированной подсистемы
в соответствии с МЭК 62061 или МЭК 61508, или МЭК 61496, или ИСО 13849-1:
- SIL или PL и
- PFH
ИЛИ</td></tr>
<tr><td>3.b</td><td>Проектирование подсистемы в соответствии с МЭК 62061 или ИСО 13849-1:
- ограничения архитектуры (SFF) или категория;
- SIL или PL
PFH</td><td>- SIL или PL
PFH</td><td>Проектирование подсистемы в соответствии с МЭК 62061 или ИСО 13849-1:
- ограничения архитектуры (SFF) или категория;
- SIL или PL
PFH</td></tr>
<tr><td>4</td><td colspan="3">SCS, выполняющая функцию безопасности, достигла требуемой полноты безопасности:
- достигнутое значение SIL или PL соответствует самому низкому значению SIL или PL из всех подсистем;
- достигнутое значение PFH SCS является суммой значений PFH всех подсистем</td></tr>
</table>

Рисунок В.1 — Пример декомпозиции функции безопасности

В.7 Требования к систематической полноте безопасности

В.7.1 Общие положения

Эти требования применяются к уровню SCS или SRP/CS и уровню подсистемы.

В.7.2 Уровень SCS

Меры по обеспечению уровня SCS или SRP/CS приведены в таблице В.4 и таблице В.5.

Таблица В.4 — Предотвращение систематических отказов (уровень SCS или SRP/CS)

Предотвращение систематических отказов (использование соответствующих компонентов)	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
План функциональной безопасности			
Правильный выбор, объединение, компоновка, сборка и установка	Монтажная схема подсистем	Проект подсистемы (7.3.3)	
Спецификации SCS изготовителя	Информация изготовителя (см. спецификацию и инструкцию по установке)		
Электробезопасность	Монтаж	МЭК 60204-1	
Разумно предсказуемое неправильное использование, изменения внешней среды или модификации	Вопросы аппаратных средств (и межсоединений). Вопросы программного обеспечения. Вопросы охвата диагностикой	Изготовитель	
Заключительные этапы проектирования			
Анализ проекта аппаратного обеспечения	Осмотр или обход. Анализ для выявления расхождений между спецификацией и реализацией	Валидация (верификация)	
Моделирование или анализ	Использование программных инструментов, если это полезно. Функциональные характеристики и правильное определение размеров компонентов. Взаимодействие подсистем	Валидация (верификация)	

Таблица В.5 — Управление систематическими отказами (уровень SCS или SRP/CS)

Управление систематическими отказами (прикладные меры)	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Управление влиянием временных отказов подсистемы	Колебание напряжения источника питания. Электромагнитные помехи	МЭК 60204-1	
Основные принципы безопасности (ИСО 12100, ИСО 13849-2)			
Применение обесточивания	Потеря питания приводит к безопасному состоянию	Изготовитель. Стандарты на изделия	
Управление процессом передачи данных	Обнаружение ошибок	Стандарты на изделия	
Проверенные принципы безопасности (ИСО 12100, ИСО 13849-2)			
Опасный сбой в интерфейсе (в кабельной разводке входов и выходов подсистем)	Диагностическая функция для оценки постоянного напряжения. Функция реакции на сбой, выполняемая до возникновения опасности		

В.7.3 Уровень подсистемы

Меры по обеспечению уровня подсистемы приведены в таблице В.6 и таблице В.7.

Таблица В.6 — Предотвращение систематических отказов (уровень подсистемы)

Предотвращение систематических отказов (использование соответствующих компонентов)	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Правильный выбор, объединение, компоновка, сборка и установка	Информация изготовителя (приложения, инструкции по установке, спецификации). Использование надлежащей инженерной практики (например, МЭК 60204-1)	Изготовитель, ИСО 13849-2	
Подсистема и элементы подсистемы в спецификации изготовителя	Информация изготовителя (см. спецификацию и инструкцию по установке)	Изготовитель	
Компоненты с совместимыми эксплуатационными характеристиками	Предыдущий опыт проектирования	Опыт проектирования	
Указанные условия внешней среды	Особенно температура, влажность, вибрация и электромагнитные поля	ИСО 12100	
Компоненты, используемые в соответствии со стандартом на изделие	Электромеханические. Гидравлические. Пневматические	Изготовитель, стандарты на изделие	
Использование подходящих материалов и надлежащее производство	Общие требования к конструкции машины, см. ИСО 12100	ИСО 12100	
Правильное определение размеров и формообразование			
Заключительные этапы проектирования			
Анализ проекта аппаратного обеспечения	Осмотр или обход. Анализ для выявления расхождений между спецификацией и реализацией	Валидация (верификация)	
Моделирование или анализ	Использование программных инструментов, если это полезно. Функциональные характеристики и правильное определение размеров компонентов	Валидация (верификация)	

Таблица В.7 — Управление систематическими отказами (уровень подсистемы)

Управление систематическими отказами (прикладные меры)	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Управление изменением напряжения	Влияние пробоя изоляции. Изменения и прерывания напряжения, перенапряжение и пониженное напряжение. Использование источника питания PELV/SELV	МЭК 60204-1	
Управление воздействием физической среды	Температура, влажность, вода, вибрация, пыль, коррозионные вещества. Электромагнитные помехи и их влияние	Изготовитель	
Управление изменением температуры	Требуется обнаружение перегрева там, где этого не удается избежать	ИСО 12100	

Окончание таблицы В.7

Управление систематическими отказами (прикладные меры)	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Управление изменением давления	Разрыв шланга. Изменения и прерывания давления	ИСО 4414 (пневматика) ИСО 4413 (гидравлика)	
Основные принципы безопасности (ИСО 12100, ИСО 13849-2)			
Применение обесточивания	Потеря питания приводит к безопасному состоянию	Изготовитель, стандарты на изделия	
Управление процессом передачи данных	Обнаружение ошибок	Стандарты на изделие	
Проверенные принципы безопасности (ИСО 12100, ИСО 13849-2)			
Обнаружение отказов автоматическими тестами	Диагностическая функция для оценки постоянного напряжения. Резервированное оборудование (двухканальное)		
Разнообразие аппаратных средств			
Работа в положительном режиме	Например, переключатель положения для блокировки защиты	Стандарты на изделие	
Механически связанные контакты	Например, зеркальные контакты контакторов	Стандарты на изделие	
Прямое действие открытия			
Завышение размеров	Например, 50 %		

В.8 Электромагнитная устойчивость

Функция электрических или электронных систем, связанных с безопасностью, не должна зависеть от внешних воздействий таким образом, чтобы это могло привести к неприемлемому риску.

Дополнительные указания даны в Е.2 (меры по снижению воздействия ЭМИ на основе МЭК 60204-1:2016, приложение Н, и МЭК 60204-1:2016/AMD1:2021, приложение Н).

В.9 Программная ручная параметризация

Цель этих требований состоит в том, чтобы гарантировать, что параметры, связанные с безопасностью, определенные для функции или для подфункции безопасности, были правильно переданы в аппаратные средства, выполняющие функцию или подфункцию безопасности. Настоящий раздел ограничен только ручной программной параметризацией, которая выполняется и управляется уполномоченным лицом.

Если подсистема способна обеспечить ручную параметризацию на основе программного обеспечения, выполняемую прикладным программным обеспечением уровня 1, то необходимо выполнение требований для предотвращения опасного отказа из-за перечисленных ниже воздействий (см. также МЭК 62061:2021, 6.7.2) или любого другого влияния, которое является разумно предсказуемым:

- ошибок ввода данных лицом, ответственным за параметризацию;
- сбоев программного обеспечения инструментального средства параметризации;
- сбоев последующего программного обеспечения и/или сервиса, предоставляемого вместе с инструментальным средством параметризации;
- сбоев аппаратных средств инструментального средства параметризации;
- сбоев при передаче параметров из инструментального средства параметризации в SCS или SRP/CS или подсистему;
- сбоев SCS или подсистемы при корректном хранении передаваемых параметров;
- систематических помех в процессе параметризации, например электромагнитных помех или потери мощности;
- помехи из-за внешних воздействий или факторов, таких как электромагнитные помехи или (случайные) потери мощности.

При использовании инструментального средства параметризации должны выполняться соответствующие требования к подсистеме в соответствии с МЭК 61508 для обеспечения правильной параметризации.

Примечание — Как правило, это происходит, когда изготовитель компонентов предоставляет это инструментальное средство вместе с подсистемой, например параметризация функций привода в соответствии с МЭК 61800-5-2.

В таблице В.8 представлен обзор основных элементов, которые необходимо учитывать при ручной параметризации на основе программного обеспечения.

Таблица В.8 — Программная ручная параметризация

Меры	Основные вопросы, требующие рассмотрения	Входная информация. Источник требования	Выходная информация. Где можно найти информацию
Спецификация требований безопасности	Спецификация требований безопасности программного обеспечения		
Проверка достоверности данных	Проверка предельных значений данных, формата и/или логических входных значений		
Целостность всех используемых данных	Контроль диапазона допустимых входных данных. Контроль искажения данных перед передачей. Контроль влияния ошибок процесса передачи параметров. Контроль влияния неполной передачи параметров. Контроль последствий сбоев и отказов аппаратных средств и программного обеспечения параметризации. Контроль влияния перебоев в электроснабжении		
Специальная процедура (если инструментальное средство не разработано в соответствии с МЭК 61508)	Повторная передача измененных параметров в инструментальное средство параметризации. Другие средства для подтверждения полноты безопасности параметров или последующего подтверждения. Новые значения параметров, связанных с безопасностью, не должны включаться до тех пор, пока изменения не будут признаны и подтверждены		

В.10 Защита информации

Когда применяются контрмеры защиты информации, они не должны отрицательно влиять на полноту безопасности (например, увеличение времени отклика и т. д.). Для этого может потребоваться итеративный междисциплинарный групповой анализ.

Риски защиты информации оцениваются с использованием оценки рисков защиты информации для определения целей защиты информации.

Оценка риска защиты информации основана на том, что изделие или система находятся в среде, в которой существуют угрозы и известные уязвимости. Целью этой деятельности является разработка соответствующих контрмер защиты информации, применяемых к машине для достижения общих целей защиты информации.

При декларировании мер противодействия защите информации, реализуемых в рамках SCS, информация предоставляется соответствующим образом.

В контексте безопасности машин контрмеры защиты информации предназначены для защиты способности поддерживать безопасную работу машины, и их реализация не должна отрицательно влиять на какую-либо функцию безопасности.

Рисунок 2 IEC TR 63074:2019 показывает в этом контексте возможные последствия риска(ов) защиты информации для SCS, как представлено на рисунке В.2.

В.11 Тестирование

В зависимости от режима работы существует два типа тестирования:

- для функций безопасности диагностические тесты проводятся автоматически (инициируются автоматически или вручную) и часто (связаны с безопасным временем процесса и частотой запросов);
- для редко активируемых функций безопасности проводятся тесты начальной и периодических верификаций в дополнение к диагностическим тестам (см. раздел 7).

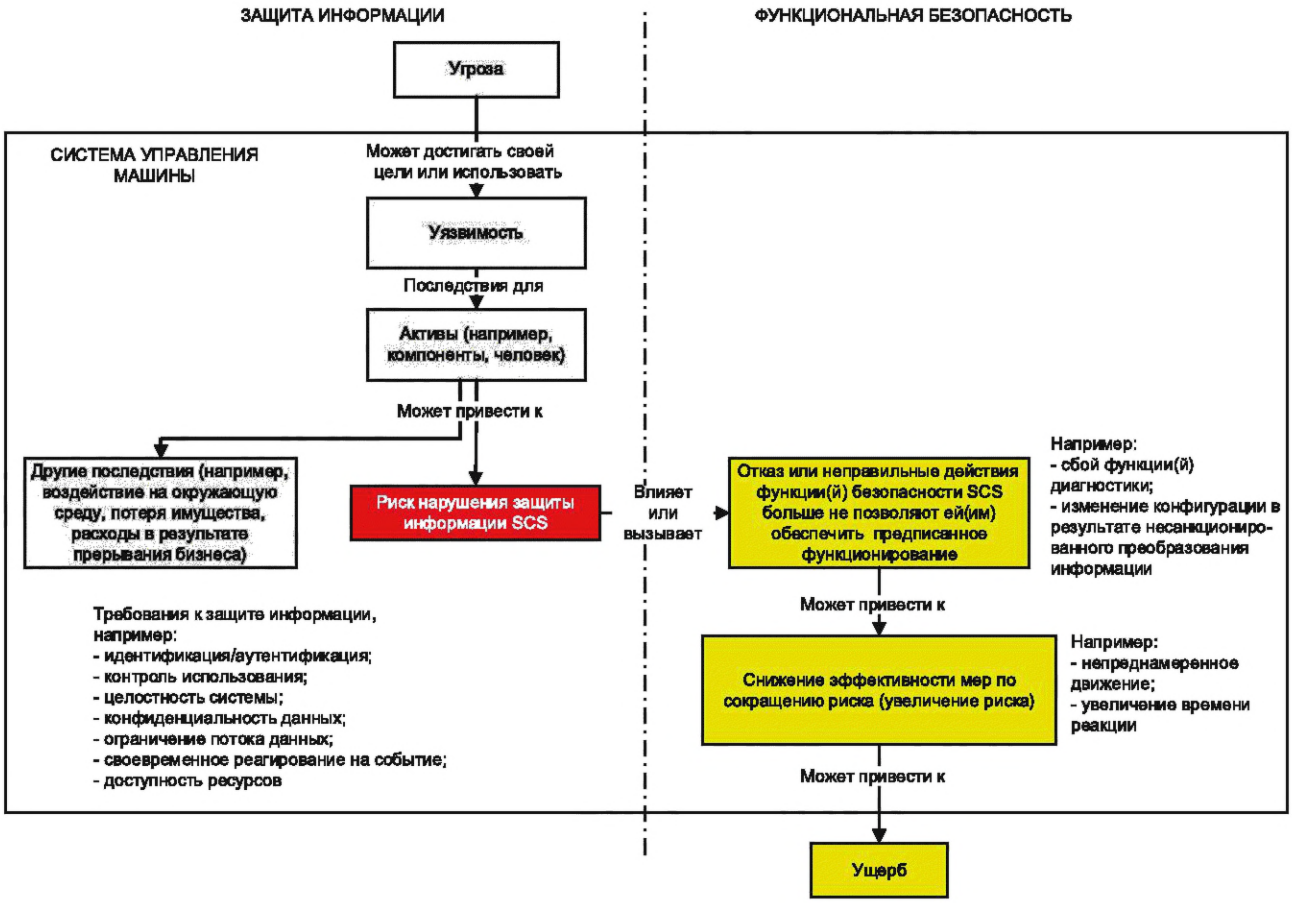


Рисунок В.2 — Возможные последствия для SCS рисков, связанных с нарушением защиты информации (IEC TR 63074:2019, рисунок 2)

В.12 Проектирование и разработка подсистемы

В.12.1 Общие положения

Существует два типа требований к подсистемам и элементам подсистем:

- качественные требования:
  - для предотвращения и управления систематическими отказами (см. раздел В.7);
  - для рассмотрения сбоев и исключения сбоев (см. В.12.3);
- количественные требования:
  - интенсивность отказов [λ, MTTF (среднее время до отказа) или B_{10}];
  - и другие соответствующие параметры (например, срок службы T_{10}).

Для неэлектронных компонентов, в частности, учитываются следующие требования:

a) срок службы ограничен T_{10}, и компоненты будут заменяться, если никакая другая информация не предоставляется стандартами изделия (см. также 6.5.3.2);

b) когда функциональное тестирование для неэлектронной технологии необходимо для обнаружения возможного накопления сбоев или необнаруженной сбоев до следующего запроса, оно будет проводиться в течение следующих интервалов тестирования:

- не реже одного раза в месяц для SIL 3;
- не реже одного раза в 12 месяцев для SIL 2.

Это требование основано на опыте подсистем с неэлектронной технологией, например мониторинг защитных дверей, в случае их нечастой эксплуатации, а функция мониторинга невозможна, если нет изменения состояния, а между тем возможно накопление сбоев.

В.12.2 Проектирование архитектуры подсистемы

В.12.2.1 Общие положения

Любая подсистема, используя один или нескольких элементов подсистемы, выполняет подфункцию функции безопасности, а отказ подсистемы приводит к потере функции безопасности.

Подсистема(ы), включающая(ие) сложные компоненты, будет(ут) соответствовать стандартам на продукцию или МЭК 61508-2 и МЭК 61508-3 в соответствии с требуемым значением SIL, и при проектировании будет использоваться способ 1_H (см. МЭК 61508-2: 2010, 7.4.4.2) для режима с высокой частотой запросов и/или непрерывного режима.

Если проект подсистемы включает в себя такой сложный компонент, как элемент подсистемы, то он может рассматриваться как компонент низкой сложности. Например, когда PDS используется для STO в соответствии с МЭК 61800-5 с полнотой безопасности SIL 2, то это может быть использовано в базовой архитектуре D подсистемы в качестве одного элемента подсистемы, и при использовании дополнительного элемента подсистемы, например контактора, эта подсистема может претендовать на значение SIL 3.

B.12.2.2 Мониторинг инициирующего события (причины)

Существуют два возможных случая обнаружения запроса к функции безопасности.

Вариант 1. Непрерывный режим работы.

Инициирующее событие реализуется в непрерывном режиме работы.

Пример — Возможны следующие случаи обнаружения опасных ситуаций в непрерывном режиме:

- мониторинг положения при управлении фактическим значением положения по сравнению с приемлемым порогом;

- мониторинг скорости при управлении фактическим значением скорости по сравнению с приемлемым порогом;

- мониторинг температуры при управлении фактическим значением температуры по сравнению с допустимым порогом;

- мониторинг давления при управлении фактическим значением давления по сравнению с допустимым порогом.

Случай 2. Режим, управляемый событиями.

Инициирующее событие обнаруживается только при запросе к функции безопасности.

Пример — Возможны следующие случаи обнаружения опасной ситуации, управляемые событиями:

- мониторинг защитной двери переключателем(ями) положения;

- управление положением с помощью датчика отключения при переходе за установленную позицию в случае достижения опасного положения;

- управление перегревом с помощью цифрового датчика отключения температуры при опасной температуре;

- управление избыточным давлением с помощью датчика отключения избыточного давления при опасном давлении.

B.12.2.3 Инициирование функции реакции (результата)

Существует два возможных вида реакции на запрос функции безопасности.

Вариант 1. Непрерывный режим работы.

Инициирование функции реакции выполняется в непрерывном режиме работы.

Пример — Возможен следующий мониторинг функции реакции в непрерывном режиме:

- прекращение опасных передвижений STO PDS;

- мониторинг температуры автоматическим блоком управления температуры — термостатом;

- мониторинг давления автоматическим блоком управления давления — реле давления и схема управления.

Вариант 2. Инициирование событием.

Инициирование функции реакции выполняется только по запросу функции безопасности.

Пример — Возможен следующий мониторинг функции реакции, инициированной событием:

- отключение контактора двигателя для остановки опасного движения;

- прекращение гидравлических или пневматических перемещений путем перевода клапана в определенное состояние;

- включение разрыва цепи для удержания гидравлического привода в нужном положении.

B.12.2.4 Возможности проектирования

Проект редко активируемых функций безопасности зависит либо от того, должны ли быть защищены люди, либо от того, должна ли быть гарантирована целостность машины, см. таблицу B.9.

Данные возможности проектирования будут рассмотрены для требований к испытаниям, см. раздел 6.

B.12.2.5 Архитектуры редко активируемых функций безопасности

Режим работы по запросу подсистем, выполняющих редко активируемые функции безопасности, может быть различным и приводит к возможным комбинациям, представленным на рисунке B.3.

Таблица В.9 — Причины и следствия редко активируемых функций безопасности

Непрерывный режим работы	Событие инициировано	Поведение	Запрос функции безопасности для защиты	
			Людей	Полноты безопасности машины
Вход (инициирующее событие как причина)				
Динамически изменяющееся значение сигнала датчика		Динамический мониторинг физических параметров		Сам процесс
	Двоичный сигнал изменения датчика (Вкл./Выкл., Выкл./Вкл.)	Статический мониторинг	Оператор (действие человека)	Сам процесс
Выход (инициирование функции реакции как результат)				
Динамическое управление приводом		PDS	Оператор (действие человека)	Сам процесс
	Бинарное отключение привода	Обесточивание силовых элементов, ответственных за движения, давление, температуру, вибрацию,...	Оператор (действие человека)	Сам процесс

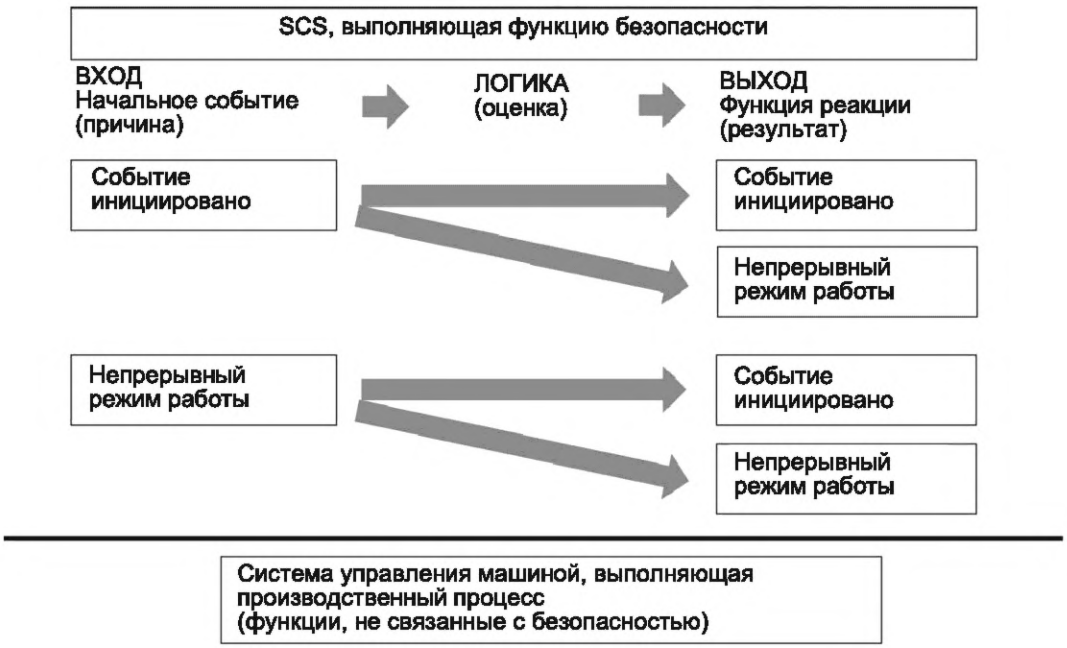


Рисунок В.3 — Редко срабатывающие функции безопасности и режим работы подсистем

В.12.3 Рассмотрение и исключение сбоев

Ограничения рассмотрения сбоев и исключения сбоев следующие: для некоторых приложений не ожидается, что все отказы могут быть исключены с достаточной уверенностью для SIL 3.

В.12.4 Архитектурные ограничения подсистемы

Архитектурные ограничения определяют предел для задаваемого значения SIL подсистемы независимо от значения PFH данной подсистемы (см. 6.3).

Поскольку охват диагностикой элемента(ов) подсистемы является основой для оценки SFF, эффективность диагностических функций становится важной. Эффективность диагностической функции может быть гарантирована только при наличии функции реакции на сбой, см. МЭК 62061:2021, 7.4.3.

Диагностические функции рассматриваются как отдельные функции, которые могут иметь другую структуру, чем функция безопасности, и могут выполняться:

- той же подсистемой, которая требует диагностики; или
- другими подсистемами SCS или SRP/CS; или
- подсистемами SCS или SRP/CS, не выполняющими функцию безопасности.

В таблице В.10 представлены требования к ограничениям архитектуры для наихудшего случая и базовые требования. Подсистемам, спроектированным в соответствии с МЭК 62061, могут быть назначены PL и категории ИСО 13849-1.

В таблице 7 показано это соответствие назначения максимального значения SIL и ограничений архитектуры согласно МЭК 62061 максимальному значению PL и категориям согласно ИСО 13849-1.

Таблица В.10 — Архитектурные ограничения и базовые требования к подсистеме

Доля безопасных отказов SFF = DC_{avg}	Отказоустойчивость аппаратных средств (HFT)[a]		Базовые требования (см. [c])	
	0	1		
	1 элемент подсистемы (как одноканальная подсистема)	2 элемента подсистемы (как двухканальная подсистема)		
< 60 %	SIL 1 хорошо отработанные компоненты не требовали никаких требований к CCF	SIL 1	Базовые принципы безопасности и хорошо отработанные принципы безопасности	CCF
От 60 % до 90 %	SIL 1	SIL 2		
От 90 % до 99 %	SIL 2	SIL 3		
≥ 99 %	SIL 3 (см. [b])	SIL 3		

[a] Отказоустойчивость аппаратных средств *N* означает, что отказы *N* + 1 могут привести к потере функции безопасности.

[b] Для HFT 0 и SFF ≥ 99 % могут быть применимы следующие ограничения:

- настоятельно рекомендуется ограничить максимум SIL 2, если исключения отказов были применены к отказам, которые могут привести к опасному отказу (см. 7.3.3.3);
- значение SIL 3 может быть назначено только при условии непрерывного мониторинга правильности функционирования элемента. Как правило, для этого потребуется электронная технология.

[c] Основные требования см. также в ИСО 13849-2:2012, приложение А — приложение D. Например, для базовых принципов безопасности это означает использование подходящих материалов; для хорошо отработанных принципов безопасности — применение обесточивания; а для испытанных компонентов — использование контакторов или переключателей положения.

Для одноканальной подсистемы (HFT = 0):

$$SFF \approx DC_{avg} = \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1 \cdot \lambda_{D1}}{\lambda_{D1}} = DC_1,$$

для двухканальной подсистемы (HFT = 1):

$$SFF \approx DC_{avg} = \frac{\lambda_{DD1} + \lambda_{DD2}}{\lambda_{D1} + \lambda_{D2}} = \frac{DC_1 \cdot \lambda_{D1} + DC_2 \cdot \lambda_{D2}}{\lambda_{D1} + \lambda_{D2}} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}},$$

где λ_{DD1}, λ_{DD2} — интенсивности опасных отказов элементов 1 и 2 подсистемы, определяемые функциями диагностики;

λ_{D1}, λ_{D2} — интенсивности опасных отказов элементов 1 и 2 подсистемы;

DC_1, DC_2 — охваты диагностикой элементов 1 и 2 подсистемы.

В.12.5 Проектирование архитектур подсистем

Исходя из отказоустойчивости аппаратных средств и ограничений архитектуры, в МЭК 62061:2021, пункт 7.5.2, предложены типовые базовые архитектуры подсистем, которые широко используются в контексте безопасности машин:

- базовая архитектура А подсистемы как одноканальная подсистема без функции диагностики, или описанная как 1oo1

(особый случай базовой архитектуры С подсистемы с DC = 0);

- базовая архитектура B подсистемы как двухканальная подсистема без функции диагностики, или описанная как 1oo2

(особый случай базовой архитектуры D подсистемы с DC = 0 для обоих каналов);

- базовая архитектура C подсистемы как одноканальная подсистема с функцией диагностики, или описанная как 1oo1D;

- базовая архитектура D подсистемы как двухканальная подсистема с функцией диагностики, или описанная как 1oo2D.

Могут использоваться другие архитектуры вместо оценки значения PFH и заявленного SIL, но настоящий стандарт не предлагает дополнительную информацию для оценки, поскольку эти архитектуры, как правило, не используются на практике.

B.12.6 Значение PFH подсистем

Для оценки значения PFH подсистемы в приложении H приводится дополнительная информация.

Параметры, которые следует учитывать:

выбранная базовая архитектура подсистемы;

оцененные значения охвата диагностикой (0 %, 60 %, 90 % или 99 %, см. также приложение D) и интервалы испытаний для каждого элемента подсистемы;

оцененный фактор β CCF (10 %, 5 %, 2 % или 1 %, см. также приложение E);

оцененное или вычисленное значение λ_D (или $MTTF_D$) каждого элемента подсистемы;

срок службы T_1, который может быть ограничен T_{10}.

В настоящем стандарте в разделах H.5 — H.12 представлена дополнительная информация о выводе формул PFH для обеспечения лучшего понимания оценки значения PFH и предотвращения неправильного использования оцененных значений PFH.

B.13 Валидация

Начальная верификация соответствует процессу валидации (см. раздел 7). В таблице B.11 представлен обзор процесса валидации.

Таблица B.11 — Обзор процесса валидации с необходимой информацией

	Процесс валидации	Входная информация. Источник требований	Выходная информация. Где можно найти информацию
Входная информация для процесса валидации	План валидации с основными требованиями		
	- Определены ли технические условия? - Указаны ли условия эксплуатации и условия внешней среды во время испытаний? - Выполняемые анализы и испытания. - Ссылка на применяемые стандарты испытаний. - Лица или стороны, ответственные за каждый этап процесса валидации. - Необходимое оборудование		
	Списки сбоев		
	- Сбои, взятые из общего(их) списка(ов), которые должны быть включены. - Любые другие соответствующие сбои, которые должны быть включены. - Сбои, взятые из общего(их) списка(ов), которые могут быть исключены. - В исключительных случаях любые другие сбои		
	Информация, необходимая для валидации		
	- Спецификация требуемых характеристик каждой функции безопасности. - Блок-схем(ы). - Принципиальная(ые) схема(ы). - Функциональное описание. - Временная(ые) диаграмма(ы) переключения компонентов. - Соответствующие характеристики компонентов, ранее прошедших валидацию. - Соответствующие характеристики компонентов, которые еще не прошли валидацию. - Анализ всех соответствующих сбоев. - Информация для пользователя, например, руководство/инструкция по установке и эксплуатации. - Характеристики проектируемой(ых) подсистемы (подсистем), связанной(ых) с безопасностью		

Окончание таблицы В.11

	Процесс валидации	Входная информация. Источник требований	Выходная информация. Где можно найти информацию
Действия в процессе валидации	a) Анализ в рамках валидации		
	Входная информация: - Функция(ии) безопасности и их характеристики. - Структура SCS или SRP/CS и архитектуры подсистем. - Количественные и качественные аспекты (систематика, программное обеспечение). Верификация спецификации требований безопасности (SRS) с целью согласованности, полноты и правильности: - Рассмотрены ли аспекты предполагаемого применения и безопасности? - Учтены ли все условия и поведение человека?		
	b) Тестирование в рамках валидации		
	Процедура испытания: - План испытаний (спецификации испытаний, требуемый результат теста, хронология). - Протоколы испытаний (люди, внешние условия, испытательное оборудование и т. д.). - Сравнение протоколов испытаний с планом испытаний		
	c) Валидация функции безопасности		
	- Демонстрация того, что SCS или SRP/CS выполняет функцию(и) безопасности в соответствии с их заданными характеристиками. - Выполнение анализа и тестирования (с внесением сбоя)		
	d) Валидация полноты безопасности SCS или SRP/CS		
	- Верификация всех связанных с безопасностью характеристик, а также валидация подсистем и объединения подсистем. - Валидация всех мер против систематических сбоев. - Валидация программного обеспечения, связанного с безопасностью		

В.14 Документация

В таблице В.12 представлен обзор работ по проектированию SCS или SRP/CS.

Таблица В.12 — Техническая документация, необходимая для процесса проектирования (таблица 9 МЭК 62061:2021, изменена)

Темы	Основные разделы
План функциональной безопасности	
Спецификация требований к безопасности (SRS)	Спецификация функциональных требований (для SCS или SRP/CS) Технические требования к полноте безопасности (для SCS или SRP/CS)
Проектирование SCS	Структурированный процесс проектирования Структура подфункций Архитектура SCS Требования безопасности к подфункциям и подсистемам
Проектирование и реализация подсистемы	Архитектура подсистемы Исключение сбоев, заявленное при оценке отказоустойчивости/SFF Сборка подсистемы
Программное обеспечение	Требования к безопасности программного обеспечения. Программная параметризация. Элементы управления конфигурацией программного обеспечения. Пригодность инструментальных средств разработки программного обеспечения.

Окончание таблицы В.12

Темы	Основные разделы
	Документация на прикладную программу. Результаты тестирования модуля прикладного программного обеспечения. Результаты тестирования интеграции прикладного программного обеспечения
Валидация	План валидации Принципы валидации
Документация	Документация по интеграции (тестированию) SCS или SRP/CS. Документация на хорошо отработанные компоненты. Документация по установке, использованию и техническому обслуживанию. Документация на выполнение валидации SCS. Документация по управлению конфигурацией SCS

В таблице В.13 представлен обзор всей соответствующей информации, особенно в контексте информации для использования, предоставленной:

- либо изготовителем подсистем;
- либо интегратором SCS или SRP/CS.

Изготовителем подсистемы может быть изготовитель оборудования, интегратор оборудования или изготовитель компонентов.

Примечание — Интегратором может быть, например, изготовитель, сборщик, инженерная компания или организация, несущая общую ответственность за машину.

Документация с точки зрения информации для использования будет доступна пользователям подсистемы (подсистем) или SCS, разработанных в соответствии с МЭК 62061, или SRP/CS, разработанных в соответствии с ИСО 13849-1.

Таблица В.13 — Обзор документации

Обзор документации	Входная информация. Источник требований	Выходная информация. Где можно найти информацию
Спецификация полноты безопасности		
SIL1, SIL2 или SIL3. Архитектурные ограничения подсистемы (подсистем), если применимо		
Техническая документация, относящаяся ко всем частям, связанным с безопасностью		
Документация в соответствии с МЭК 62061:2021, таблица 9. Функция(ии) безопасности, реализуемая SCS в соответствии с разделом 5, или подфункция безопасности, реализуемая подсистемой SCS. Подсистема при проектировании (согласно разделу 7) (включая испытания или анализ поведения при наличии сбоев). Характеристики каждой функции безопасности. Условия внешней среды. Меры против систематических сбоев. Хорошо отработанные компоненты в случае использования	МЭК 62061:2021, таблица 9	
Информация для использования, предоставляемая изготовителем подсистем (для безопасной установки, использования и обслуживания подсистемы)		
Описание подсистемы (общие сведения, функции, установка, интерфейс(ы), конфигурация/настройки/программирование). Информация о предельных значениях рабочих параметров (предельные значения внешней среды, граничные значения, другие предельные значения, например, рабочая частота и т. д.). Исключение сбоев. Необходимые меры в подсистеме для предотвращения ухудшения характеристик предполагаемой функции SCS.		

Окончание таблицы В.13

Обзор документации	Входная информация. Источник требований	Выходная информация. Где можно найти информацию
Обеспечение ремонтопригодности. Время отклика подсистемы. Срок службы подсистемы. Функции диагностики. Процедуры проверки. Параметры, связанные с безопасностью		
Информация для использования, предоставленная интегратором SCS (для того, чтобы пользователь машины разработал процедуры для обеспечения требуемой функциональной безопасности SCS во время использования и технического обслуживания машины)		
Эксплуатационные ограничения SCS (включая условия внешней среды). Понятные описания и соответствующие инструкции для интерфейсов пользователя SCS (например, панель оператора, индикаторы и аварийные сигналы). Описание (включая принципиальные схемы). Маркировка, если требуется, в соответствии с ИСО 12100:2010, 6.4.4. Срок службы и требования к компонентам SCS. Любой режим работы, относящийся к функции(ям) безопасности. Инструменты, необходимые для технического обслуживания и повторного ввода в эксплуатацию, а также процедуры технического обслуживания инструментов и оборудования. Средства технического обслуживания и вся информация для технического обслуживания (процедуры диагностики и ремонта неисправностей, процедуры подтверждения правильной работы после ремонта и профилактического технического обслуживания и корректирующего технического обслуживания		

Приложение С
(справочное)

Примеры значений $MTTF_D$ для отдельных компонентов

В настоящем приложении описаны различные методы расчета или оценки значений $MTTF_D$ для отдельных компонентов. Таблица С.1 и таблица С.2 объединяют соответствующую информацию (для получения дополнительной информации к таблице С.1 см. МЭК 62061 или ИСО 13849-1).

Таблица С.1 — Значения $MTTF_D$ или B_{10D} для компонентов (на основе ИСО 13849-1:2015)

Компонент	Типичные значения $MTTF_D$ (годы) или B_{10D} (циклы)
Механические компоненты	$MTTF_D$ = 150
Гидравлические компоненты с $n_{op} \geq 1\,000\,000$	$MTTF_D$ = 150
Гидравлические компоненты с $1\,000\,000 > n_{op} \geq 500\,000$	$MTTF_D$ = 300
Гидравлические компоненты с $500\,000 > n_{op} \geq 250\,000$	$MTTF_D$ = 600
Гидравлические компоненты с $250\,000 > n_{op}$	$MTTF_D$ = 1200
Пневматические компоненты	B_{10D} = 20 000 000
Реле и контакторные реле с малой нагрузкой (механическая нагрузка)	B_{10D} = 20 000 000
Реле и контакторные реле с максимальной нагрузкой	B_{10D} = 400 000
Бесконтактные выключатели с небольшой нагрузкой (механическая нагрузка)	B_{10D} = 20 000 000
Бесконтактные выключатели с номинальной нагрузкой	B_{10D} = 400 000
Контакторы с малой нагрузкой (механическая нагрузка)	B_{10D} = 20 000 000
Контакторы с номинальной нагрузкой	B_{10D} = 1 300 000 (см. [a])
Переключатели положения	B_{10D} = 20 000 000
Позиционные переключатели (с отдельным приводом, защита-блокировка)	B_{10D} = 2 000 000
Устройства аварийного останова	B_{10D} = 100 000
Кнопки (например, разрешающие переключатели)	B_{10D} = 100 000

[a] B_{10D} оценивается как удвоенное значение B_{10} (50 % опасных отказов), если нет другой информации (например, стандарта на изделие).

[b] «Номинальная нагрузка» или «малая нагрузка» должны учитывать принципы безопасности, описанные в ИСО 13849-2, такие как чрезмерная величина номинального значения тока. «Малая нагрузка» означает, например, 20 %.

Таблица С.2 — Взаимосвязь λ_D, $MTTF_D$ и B_{10D}

Формулы	Единицы	Параметры
$\lambda_D \sim 0{,}1\frac{C}{B_{10D}} = \frac{C}{10}\frac{RDF}{B_{10}}$	[1/ч]	$C = \frac{\text{циклы}}{\text{час}[\text{ч}]}$,
$MTTF_D = \frac{1}{\lambda_D 8760} \sim \frac{10}{n_{op}}\frac{B_{10}}{RDF}$	[*a*]	$n_{op} = \frac{\text{циклы}}{\text{час}[a]}$,
$T_{10D} = \frac{B_{10D}}{n_{op}} \sim \frac{MTTF_D}{10}$	[*a*]	$B_{10D} = \frac{B_{10}[\text{циклов}]}{RDF}$. Доля опасных отказов (RDF)

Приложение D
(справочное)

Примеры охвата диагностикой (DC)

D.1 Общие положения

Функция диагностики представляет собой функцию периодического тестирования (см. МЭК 62061:2021, 6.9), выполняемую подсистемой SCS или SRP/CS.

Диагностические функции выполняются:

- автоматически (запускаются автоматически или вручную);
- регулярно (связано с временем безопасности процесса и интенсивностью запросов).

Таким образом, охват диагностикой (DC) может быть определен (см. МЭК 62061:2021, пункты 7.4.3 и 7.4.4) только для функции диагностики, когда:

- реализуется реакция на сбой, которая:
  - переводит соответствующую часть машины в безопасное состояние вследствие обнаруженного сбоя;
  - выполняется до возникновения опасности из-за этого сбоя;
- интервал диагностических проверок достаточен для выявления отказов по крайней мере по запросу функции безопасности (интервал диагностических проверок больше или равен интенсивности запросов).

Следовательно, для определения всех сбоев подсистемы и их соответствующих видов отказа выполняется анализ каждого элемента подсистемы (см. МЭК 62061:2021, пункт 7.3.3).

DC каждого элемента подсистемы оказывает существенное влияние на оценку SFF (см. МЭК 62061:2021, пункт 7.4.2). Используя подход, основанный на наихудшем случае, $\lambda_S \approx 0$ и в зависимости от HFT, SFF может быть оценена со следующими уравнениями:

для HFT = 0:
$$SFF \approx DC_{avg} = \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1 \cdot \lambda_{D1}}{\lambda_{D1}} = DC_1, \quad (D.1)$$

для HFT = 1:
$$SFF \approx DC_{avg} = \frac{\lambda_{DD1} + \lambda_{DD2}}{\lambda_{D1} + \lambda_{D2}} = \frac{DC_1 \cdot \lambda_{D1} + DC_2 \cdot \lambda_{D2}}{\lambda_{D1} + \lambda_{D2}} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}}, \quad (D.2)$$

где λ_{DD1}, λ_{DD2} — интенсивности опасных отказов элементов подсистемы 1 и 2, определяемые функциями диагностики;

λ_{D1}, λ_{D2} — интенсивности опасных отказов элементов подсистемы 1 и 2;

DC_1, DC_2 — охваты диагностикой элементов подсистемы 1 и 2.

D.2 Влияние кабельной системы, разводки и межкомпонентных соединений

D.2.1 Общие положения

Для обеспечения систематической полноты безопасности SCS или SRP/CS на уровне подсистемы и SCS или SRP/CS реализуются меры по предотвращению систематических отказов аппаратных средств. Кабельные системы, разводки и межкомпонентные соединения могут влиять на способность функции диагностики и, следовательно, могут ограничивать возможное значение охвата диагностикой элемента подсистемы: рассмотрение специфических сбоев и предотвращение подозреваемых сбоев приводят к возможному влиянию на оценку охвата диагностикой.

В принципе, могут существовать меры, указанные в таблице D.1, для предотвращения короткого замыкания и воздействия максимально допустимого постоянного тока.

D.2.2 «Последовательное соединение сигналов»

Необнаруженные или скрытые сбои возможны при использовании последовательного соединения сигналов. Меры по предотвращению накопления сбоев будут применяться в зависимости от применения и вероятности возникновения накопления. Там, где невозможно исключить накопление сбоев, следует принять DC менее 90 %.

Таблица D.1 — Меры по предотвращению короткого замыкания

Сбой	Мера	Примеры
Короткое замыкание. Предотвращение короткого замыкания путем применения: - отработанных принципов безопасности и предотвращения сбоев или - перекрестного мониторинга, прямого или косвенного мониторинга	Основные принципы безопасности (см. также МЭК 60204-1, ИСО 13849-1):	
	- Использование обесточивания	Для сигналов, активных при высоком уровне напряжения (потеря питания, обрыв электропроводки или короткое замыкание)
	Проверенные принципы безопасности (см. также МЭК 60204-1, ИСО 13849-1):	
	- Предотвращение сбоев в кабелях	Вне шкафа: кабель с экранированием, подключенный к цепи защитного заземления для каждого отдельного проводника
	- Разделительное расстояние	Достаточное расстояние между клеммами, компонентами и проводниками во избежание непреднамеренных соединений
	Сбои и их предотвращение (см. также МЭК 60204-1, ИСО 13849-1)	
	Между любыми двумя проводниками	- Постоянно подключенные (стационарные) и защищенные от внешних повреждений, например, кабельными каналами, армированием; - в электрическом шкафу; - вне шкафа: - индивидуально экранированные с заземлением или - отдельные многожильные кабели
	Между соседними клеммами	Клеммы и соединения в соответствии с МЭК 60947-7-1 или МЭК 60947-7-2 и требованиями МЭК 60204-1
Короткое замыкание. Предотвращение короткого замыкания путем применения: - отработанных принципов безопасности и предотвращения сбоев или - перекрестного мониторинга, прямого или косвенного мониторинга	Достоверно испытанный компонент (см. также МЭК 60204-1, ИСО 13849-1)	
	Кабель	Кабели вне шкафа защищены от механических повреждений (включая, например, вибрацию или изгиб)
	Функция диагностики	
	Перекрестный мониторинг. Прямой или косвенный мониторинг	Оценка достоверности состояния сигнала(лов)

Примечание 1 — Меры по предотвращению короткого замыкания применяются к одноканальным и двухканальным подсистемам.

Примечание 2 — Для двухканальной подсистемы DC = 99 % для каждого элемента подсистемы достижим там, где можно предотвратить неисправность(и) из-за короткого замыкания.

Пример 1 — Мониторинг трех защит с блокировкой, когда для каждой блокировки защиты используются два позиционных выключателя, и оценка этих позиционных выключателей осуществляется с помощью «последовательного соединения». Когда один оператор одновременно открывает и закрывает только одну защиту из-за производственного процесса, то вероятность возникновения скрытых сбоев в одной из остальных защит может быть исключена. Когда один оператор использует любую из мер безопасности для входа в одну и ту же опасную зону, то может возникнуть вероятность возникновения скрытых сбоев для одной из других мер безопасности и возможное предсказуемое неправильное использование не может быть исключено. Можно разумно предположить, что DC составляет 60 %, и каждая подсистема (защита) ограничивается максимально достижимым уровнем SIL 2. Для получения дополнительной информации см. также ИСО 14119:2013, пункт 8.6, и ISO/TR 24119.

Пример 2 — Устройства аварийного останова подключаются последовательно с использованием двух электрических контактных элементов, которые открываются прямым открывающим действием с механической фиксацией. Электрические контактные элементы соединены последовательно. Можно исключить, что оператор нажмет одно устройство аварийной остановки, а затем второе. Вероятность возникновения скрытых сбоев может рассматриваться как очень низкая, и поэтому исключается. Можно предположить, что DC составляет 99 %, и каждая подсистема (устройство аварийного останова) может претендовать на SIL 3.

D.3 Использование информации о производственном процессе

D.3.1 Общие положения

Не связанная с безопасностью часть системы управления машиной выполняет производственный процесс и может предоставлять на основе ожидаемого поведения производственного процесса информацию, которая может использоваться для оценки диагностики элемента(ов) подсистемы.

В зависимости от интенсивности диагностики (испытания) производственного процесса величины DC для SCS или SRP/CS могут привести к более высоким значениям DC для элемента(ов) подсистемы, чем без учета этой информации.

Оценка информации о производственном процессе реализуется логикой, связанной с безопасностью.

Типичные причины выполнения этой процедуры:

- прямой мониторинг элемента подсистемы невозможен;
- ухудшение процесса или проблемы с качеством процесса позволяют прогнозировать предстоящие возможные опасные ситуации, прежде чем потребуется функция безопасности.

Оцениваемое значение DC для каждого элемента подсистемы в зависимости от частоты диагностического тестирования (rt) и частоты запросов (rd) функции безопасности ограничено:

- DC ≤ 60% при rt/rd > 1;
- DC ≤ 90% при rt/rd ≥ 10;
- DC ≤ 99% при rt/rd ≥ 100.

D.3.2 Использование ожидаемых сроков или ожидание статуса сигнала

Синхронизация сигналов, обусловленная производственным процессом, может использоваться для диагностики, особенно там, где ожидается, что физически одноканальный сигнал будет иметь определенное поведение.

Пример 1 — Индуктивное или аналоговое устройство мониторинга используется с хорошо известным динамическим сигналом оценки. Когда поведение этого динамического сигнала отклоняется от ожидаемого значения или порога, диагностическая функция может обнаружить это отклонение и инициировать функцию реакции отказа, что можно рассматривать как одноканальную подсистему со значением DC от 60 % до 90 % и максимально достижимым значением SIL 2.

Пример 2 — Прямой мониторинг достоверно испытанных компонентов (например, контакторов) с использованием сигналов обратной связи (зеркальных контактов), подключенных к аппаратным средствам, не связанным с безопасностью, но оцененным подсистемой, связанной с безопасностью (логика с перекрестным мониторингом с динамическим изменением сигнала для обнаружения статических сбоев и короткого замыкания).

D.4 Типовые меры DC

В таблице D.2 представлен обзор значений DC и примеры рекомендуемых мер. При применении конкретной меры следует учитывать эффективность диагностики.

Таблица D.2 — Значения DC и рекомендуемые меры

DC	Меры	Примеры
99 %	Перекрестный мониторинг двух каналов с динамическим изменением сигнала для обнаружения статических сбоев и короткого замыкания	
	Проверка достоверности двух каналов	Нормально разомкнутые и нормально замкнутые механически связанные контакты
	Прямой мониторинг (для одноканальной или двухканальной подсистемы)	Электрический мониторинг положения регулирующих клапанов. Мониторинг электромеханических устройств с помощью механически связанных контактных элементов
90 %	Перекрестный мониторинг входов без динамического испытания	Использование производственного процесса (ожидание поведения сигнала). Без предотвращения короткого замыкания
	Циклические тесты, сформированные путем динамического изменения входных сигналов	Автоматическое изменение выхода, чтобы проверить, изменит ли состояние вход, подключенный к этому выходу

Окончание таблицы D.2

DC	Меры	Примеры
	Перекрестный мониторинг выходных сигналов с динамическим тестированием без обнаружения коротких замыканий (для нескольких входов/выходов)	Проверяют, отключились ли два выпускных клапана 3/2, пользуясь манометрическим выключателем, и включают клапаны один за другим, чтобы увидеть, возникает ли разница в давлении
	Косвенный мониторинг	Мониторинг с помощью реле давления, электрический мониторинг положения исполнительных механизмов, мониторинг того, находится ли цилиндр в его конечном положении и остается ли цилиндр в этом конечном положении
60 %	Перекрестный мониторинг входов без динамического испытания	Использование производственного процесса (ожидание поведения сигнала)
	Контроль некоторых характеристик датчика	Время отклика. Диапазон аналоговых сигналов, электрическое сопротивление, емкость

Приложение Е
(справочное)

Меры достижения функциональной безопасности в отношении электромагнитных явлений

Е.1 Общие положения

Электромагнитные помехи могут нарушить или повредить системы мониторинга, управления и автоматизации технологического процесса. Токи, вызванные молнией, операциями переключения, короткими замыканиями и другими электромагнитными явлениями, могут вызывать перенапряжение и электромагнитные помехи.

Эти эффекты могут возникнуть, например:

- при наличии мощных проводящих контуров,
- если различные системы электропроводов установлены на общих трассах, например кабели питания, связи, управления или сигнальные кабели.

Другие электрические помехи могут быть вызваны электростатическими разрядами из-за людей, вступающих в контакт с оборудованием, от использования поблизости мобильных телефонов и работы преобразователей частоты.

Для целей электромагнитной совместимости (EMC) электрическое оборудование для машинного оборудования реализуется либо отдельным, либо стационарным аппаратом. Если для электробезопасности и электромагнитной совместимости сформированы различные требования, то электробезопасность (особенно поражение электрическим током) всегда имеет более высокий приоритет, см. также, например, МЭК 60204-1.

Е.2 Меры

Е.2.1 Общие положения

Рекомендации в Е.2.2 — Е.2.3 содержат указания по обеспечению устойчивости к электромагнитным помехам (EMI) для элементов оборудования (устройств и/или аппаратуры) и их интеграции в электрооборудование машины.

Е.2.2 Рекомендации по электрическим/электронным элементам оборудования (устройствам или аппаратам)

Для электрических/электронных элементов оборудования (устройств или аппаратуры):

- при наличии должны использоваться только электрические и/или электронные устройства или аппараты, отвечающие требованиям соответствующего стандарта на изделие (связанного с устойчивостью к электромагнитным явлениям); поскольку стандарт на семейство изделий/изделие, как правило, предъявляет более конкретные требования, обычно считается, что он имеет приоритет над соответствующим общим стандартом;
- примерами стандартов на изделия являются МЭК 61326-3-1, МЭК 61800-5-2, МЭК 61496-1, МЭК 60947-5-3. Для их интеграции/установки в электрооборудование машины будет применяться информация для применения от изготовителя;
- если не существует соответствующего специального стандарта на семейство изделий или на изделие, касающегося учета влияния электромагнитных воздействий на функциональную безопасность, то применяется общий стандарт МЭК 61000-6-7:2014;
- для подсистем, спроектированных в соответствии с МЭК 62061 или ИСО 13849-1, электромагнитная среда и ее явления должны учитываться в SRS, как того требует МЭК 61508. Требования к помехоустойчивости должны основываться на прогнозируемых электромагнитных угрозах в реальной среде в течение всего срока службы оборудования.

И с к л ю ч е н и е — Для SCS или SRP/CS, спроектированных в соответствии с PL a или PL b с использованием категории B по ИСО 13849-1, необходимо следовать требованиям EMI МЭК 61000-6-2: 2014.

Е.2.3 Рекомендации по интеграции SCS или SRP/CS в электрооборудование машины

Для интеграции SCS или SRP/CS в электрооборудование машины могут применяться меры EMI в соответствии с МЭК 60204-1: 2016, приложение H, и МЭК 60204-1:2021.

В таблице Е.1 приведен перечень рекомендаций по повышению электромагнитной устойчивости SCS или SRP/CS и снижению эмиссии электромагнитных помех.

Таблица Е.1 — Неисчерпывающий список рекомендаций относительно мер EMI для интеграции устройств или оборудования в электрооборудование машины

Примеры мер EMI	Использование
Устанавливается в экранированном и заземленном шкафу или компоненты в экранированном и заземленном корпусе	Рекомендуется устанавливать по возможности
Экранированные и заземленные или витые кабели для датчиков и связанных с безопасностью входных/выходных сигналов (экраны кабелей плоские, заземлены с низким импедансом рядом с компонентами)	
RF-фильтр, защита от перенапряжения и переходных процессов (например, фильтр, диод подавления переходных напряжений, оптопара, ферриты) для входных/выходных сигналов, связанных с безопасностью	
Если применимо: экранированные и заземленные кабели для двигателей или синус-фильтр между двигателем и инвертором или эквивалентные меры	
RC-фильтр, обратный диод или эквивалентные меры для достижения гашения искр при переключении индуктивных нагрузок	
…	
Опыт эксплуатации системы с высокой надежностью	Настоятельно рекомендуется
Жгут низковольтного постоянного напряжения к компонентам в витой паре	
Подходящие электромагнитные фильтры для силовой сети (защита от перенапряжения и переходных процессов)	
Разделение источников ЭМС и чувствительных компонентов, например: - раздельная трассировка и расположение линий питания и сигнальных линий; - отдельные металлические шкафы для силовой электроники и маломощной электроники; - расстояние > 20 см между силовыми компонентами и чувствительными компонентами	
…	

Приложение F
(справочное)

Руководство по программному обеспечению

F.1 Общие положения

Таблицы F.1 — F.6 дают обзор необходимых документов и основных видов деятельности.

Примечание — Программное обеспечение (SW) может быть разработано в соответствии с МЭК 62061 или ИСО 13849-1.

Прикладное программное обеспечение, связанное с безопасностью, работает на предварительно разработанной платформе (сочетание аппаратных средств и программного обеспечения) в соответствии с МЭК 61508 или другими стандартами по функциональной безопасности, связанными с МЭК 61508, например МЭК 61131-6, где:

SW уровня 1 использует язык с ограниченной изменчивостью (LVL),

SW уровня 2 использует язык, отличный от языка с ограниченной изменчивостью (LVL).

F.2 Документация

В таблицах F.1 — F.6 обобщены соответствующие документы и информация для проектирования, внедрения и интеграции SW уровня 1 и SW уровня 2.

Таблица F.1 — Документы для SW уровня 1 и SW уровня 2

Документ	Комментарии
Руководящие принципы кодирования	См. таблицу F.2
Спецификация функций безопасности	См. раздел 5, B.3 и таблицу B.2
Спецификация проекта аппаратного обеспечения (см. [a]): - эскиз(ы) установки; - проект системы управления; - монтажная(ые) схема(ы); - перечень вводов/выводов	См. 4.4
Спецификация проекта программного обеспечения (см. [b]): - спецификация и план валидации программного обеспечения, связанного с безопасностью; - спецификация проекта системы программного обеспечения и модулей; - архитектура программы, связанной с безопасностью; - архитектура программы, не связанной с безопасностью; - модульная архитектура программы, связанной с безопасностью; - эскиз программы (логическое представление)	См. обзор основных работ для SW уровня 1, таблицу F.3 и SW уровня 2, таблицу F.4. SW уровня 1 и SW уровня 2. SW уровня 2
Протоколы: - верификации программного обеспечения; - обзор кода; - валидации программного обеспечения	См. таблицу F.3
[a] Можно использовать распечатку аппаратных средств, созданную средствами САПР. [b] Может использоваться распечатка программного обеспечения, сгенерированная предварительно разработанной программной платформой.	

Таблица F.2 — Рекомендации по кодированию

A Переменные
Префиксы булевых переменных: «b». Префиксы двоичных входов: «I_b» (вход, не связанный с безопасностью), «IS_b» (вход, связанный с безопасностью). Префиксы двоичных выходов: «Q_b» (выход, не связанный с безопасностью) или «QS_b» (вход, связанный с безопасностью). Префиксы экземпляров: таймеры: «T_», обнаружения положительных ребер: «R_», триггеры: «FF _».

Окончание таблицы F.2

Префиксы экземпляров: экземпляры SF_GUARD: GUARD_<guard name >, SF_ESTOP: ESTOP_<number>, SF_ FDBACK: CONTACTORS_<contactors > Префиксы глобальных переменных: «G_» (не связаны с безопасностью), «GS_» (связаны с безопасностью). Префиксы временных переменных: «#». Имена переменных: имя переменной после префикса должно быть понятным, например, должно содержать рассматриваемое имя устройства. Например, GD1 для защитной двери 1. Объявление переменной: инициализировать с самым безопасным условием. Следует включить комментарий в каждое объявление
В Обработка сигналов
Архитектура программного обеспечения: разделение потока данных программного обеспечения на слой предварительной обработки (входы), логику выключения (логика) и слой постобработки (выходы). Реализация уровня предварительной обработки в последовательных сетях. Выход каждой сети должен каким-то образом способствовать логике выключения. Для каждого двоичного выхода: реализовать соответствующую логику выключения и уровень постобработки в одной сети (если возможно). Назначение: используйте выходные данные и переменные только в одном операторе программы. Комментарии: у каждой сети есть комментарий. Циклическая обработка: запускают каждую часть программного обеспечения, связанного с безопасностью, без условий, как часть каждого цикла. Мониторинг двух канальных входов: мониторинг на двух канальных входах (например, кнопки) с помощью карт ввода с временем расхождения, например, 100 мс. Мониторинг контакторов: мониторинг зеркальных контактов контакторов со временем обратной связи, например, 1 сек. Мониторинг защитной двери: мониторинг блокирующих устройств с временем расхождения, например, от 100 мс до 500 мс. Автоматический перезапуск: допускается только для защитных дверей, где оператор не может оставаться в опасной зоне. Ошибки в периферийных устройствах: необходим ручной сброс. Срабатывание функций безопасности: срабатывание по ложному сигналу. Концепция подтверждения обнаруженных отказов: селективность «сброса/подтверждения» в зависимости от концепции доступности; требования к действиям персонала. Время отклика (типичное): рассчитывают или тестируют и документируют время отклика программы, связанной с безопасностью
Использование: везде, где это применимо, используют предварительно разработанную библиотеку FBs/FCs. Защитная дверь: SF_GUARD. Устройство аварийной остановки: SF_ESTOP. Контактор: SF_FDBACK. Разрешающее устройство: SF_EV2DI. Автоматический сброс: в зависимости от функций библиотеки (цитируется здесь). Активация: в зависимости от функций библиотеки (цитируется здесь). Самостоятельно разработанные FB/FC: если применимо, то комбинации логических сигналов капсул, которые имеют несколько назначений в рамках проекта в FB/FC. Жизненный цикл соответствует V-модели. Эти FB/FC будут защищены паролем. Необходимо управление библиотекой.

Таблица F.3 — Обзор протоколов

Действия	Ссылка	Корректность (да/нет)
Верификация спецификации проекта системы программного обеспечения		
1 Соответствует ли архитектура модуля спецификации функций безопасности? 2 Соответствует ли спецификация проекта программного обеспечения спецификации функций безопасности?		
Обзор программного кода		
1 Соответствует ли программное обеспечение рекомендациям по кодированию? 2 Соответствует ли проект системы управления спецификации? 3 Корректны ли соединения сигналов ввода/вывода в программном обеспечении? Корректна ли параметризация соответствующих FB? 4 Соответствует ли иерархия программы безопасности PLC спецификации? 5 Соответствует ли архитектура программы безопасности PLC спецификации? 6 Соответствует ли программа безопасности PLC спецификации таблицы? 7 Соответствует ли спецификация программного обеспечения, связанного с безопасностью, спецификации функций безопасности?		

Окончание таблицы F.3

Действия	Ссылка	Корректность (да/нет)
Валидация программного обеспечения — необходимо проверить		
1 Был ли проведен тест ввода-вывода с положительным результатом? 2 Было ли испытание функций безопасности и других требований испытаний выполнено с положительным результатом? 3 Все ли специальные испытания изготовителя по параметризации внешних устройств безопасности (например, лазерных сканеров, преобразователей и т. д.) были проведены с положительным результатом и документально оформлены? 4 Документы по V-модели. 5 Окончательный документ по безопасности соответствующего программного обеспечения, включая подписи. 6 Окончательный документ по конфигурации аппаратных средств системы управления с контрольными суммами и всеми корректировками. 7 Архивирование руководств для всех компонент системы, важных для безопасности. 8 Окончательный документ по конфигурации всех периферийных устройств, важных для безопасности. 9 Соответствующие стандарты по С		
Дата: Имя: Подпись ответственного за программное обеспечение: Подпись ответственного за аппаратные средства:		

F.3 Действия

Основным отличием SW уровня 2 от SW уровня 1 является более высокая степень гибкости в программировании за счет большей свободы и сложности используемого языка программирования.

Поэтому необходимы следующие дополнительные мероприятия:

- проектирование системы программного обеспечения;
- проектирование модуля.

Таблица F.4 — SW уровня 1. Обзор основных видов действий

Требования (входные данные)	Результат (выходные данные)
Разработка требований к безопасности программного обеспечения	
Спецификация функции(й) безопасности	Входные данные
Архитектура SCS или SRP/CS	
Время отклика	
Интерфейсы и средства управления оператора	**Спецификация проекта программного обеспечения**
Соответствующие режимы работы машины	
Диагностика (например, характеристики датчиков, исполнительных механизмов)	
Руководящие принципы кодирования	
Разработка спецификации к проекту программного обеспечения	
Спецификация проекта программного обеспечения	Входные данные
Для каждой подсистемы	
SIL и тестовые случаи	**Кодирование**

Окончание таблицы F.4

Требования (входные данные)	Результат (выходные данные)
Для проектирования модулей применяются те же требования, основанные (см. 8.3.3) на описании модуля, интерфейсе, используемых библиотеках и конкретных правилах кодирования	Логика
	Вставка или включение(я) сбоев в тестовых случаях
	Диагностические функции с реакцией на сбой
	Достижение или поддержание безопасного состояния
	Периодические испытания или функциональные испытания
	Предотвращение несанкционированных изменений
	Время отклика
	Архитектура ПО; глобальные данные; библиотеки; ранее существовавшие программные модули; тестовые случаи и процедуры
Кодирование	
Спецификация проекта программного обеспечения	Подлежит испытанию **Программный код**
Правила кодирования	
Руководящие принципы кодирования	
Для кодирования модулей применяются те же требования	Листинг исходного кода (например, лестничная структура, функциональные блоки, модели)
	Структура как логический поток
	Отчет об анализе кода
	Достаточные комментарии
	Одинаковые имена параметров
	Имена представляют функцию
	Предопределенное состояние
	Ограниченное использование установка/сброс
	Выходы назначаются только один раз
Тестирование программного обеспечения	
Спецификация проекта программного обеспечения	Проверен **Программный код** (верификация тестированием)
Проверка функциональности	
Правила и рекомендации по кодированию	
Для тестирования модуля применяются те же требования (см. 8.3.3)	Руководство по испытаниям:
	Виды испытаний; испытательное оборудование; контроль версий программного обеспечения; корректирующие действия по неудачному тесту
	Спецификация изготовителя
	Функциональное тестирование
	Моделирование отказов
	Документация

Таблица F.5 — SW уровня 2 — Обзор основных видов действий (1/2)

Требования (входные данные)	Результат (выходные данные)
Разработка требований к безопасности программного обеспечения	
Спецификация функции(й) безопасности. Архитектура SCS или SRP/CS. Время отклика. Интерфейсы и средства управления оператора. Соответствующие режимы работы машины. Диагностика (например, характеристики датчиков, исполнительных механизмов). Руководящие принципы кодирования	Входные данные **Спецификация проекта программного обеспечения**
Разработка спецификации к проектированию программного обеспечения	
Структурированный, проверяемый, тестируемый, понятный, ремонтопригодный и работоспособный. Для каждой подсистемы. SIL и тестовые случаи	Входные данные **Проект системы программного обеспечения**
	Логика. Вставка или включение(я) сбоев в тестовых случаях. Диагностические функции с реакцией на сбой. Достижение или поддержание безопасного состояния. Периодические испытания или функциональные испытания. Предотвращение несанкционированных изменений. Время отклика. Архитектура ПО; глобальные данные; библиотеки; ранее существовавшие программные модули; тестовые случаи и процедуры
Разработка спецификации к проектированию модулей	
Спецификация к проектированию программного обеспечения. Для каждой подсистемы. SIL и тестовые случаи	Входные данные **Спецификация к проектированию модулей**
	Описание логики (т. е. функциональности) каждого модуля. Полностью определенные входные и выходные интерфейсы каждого модуля. Диапазоны формата и значений входных и выходных данных и их связь с модулями. Тестовые случаи, которые будут включать нормальную и внешнюю нормальную работу. Документирование прерываний
Проектирование модуля	
Спецификация к проектированию модуля. Описание модуля. Интерфейс модуля. Используемые библиотеки модулей. Специальные правила кодирования	Входные данные **Проект модуля**
Разработка модуля(ей)	Описание логики (т. е. функциональности) каждого модуля. Полностью определенные входные и выходные интерфейсы каждого модуля. Диапазоны формата и значений входных и выходных данных и их связь с модулями
	Тестовые случаи, которые будут включать нормальную и внешнюю нормальную работу Документирование прерываний

Таблица F.6 — SW уровня 2. Обзор основных видов действий (2/2)

Требования (входные данные)	Результат (выходные данные)
Кодирование	
Спецификация проекта программного обеспечения Правила кодирования Руководящие принципы кодирования	Подлежит испытанию **Программный код**
Для проектирования модулей применяются те же требования	Листинг исходного кода (например, лестничная структура, функциональные блоки, модели)
	Структура как логический поток
	Отчет об анализе кода
	Достаточные комментарии
	Одинаковые имена параметров
	Имена представляют функцию
	Предопределенное состояние
	Ограниченное использование установка/сброс
	Выходы назначаются только один раз
Тестирование модуля	
Спецификация проекта модуля Тестовые примеры Рекомендации по кодированию	Проверен **Программный код (верификация тестированием)**
	Документирование тестовых примеров: - функциональные испытания, - тестирование Black-Box, Grey-Box или White-Box. Документирование корректирующих действий — тестовые примеры интеграции: модули программного обеспечения и элементы/подсистемы программного обеспечения взаимодействуют корректно. Анализ программ
Тестирование программного обеспечения	
Спецификация проекта программного обеспечения. Тестовые примеры. Рекомендации по кодированию	Проверен **Программный код (верификация тестированием)**
	Руководство по испытаниям: - виды испытаний; испытательное оборудование; - контроль версий программного обеспечения; - корректирующие действия по неудачному тесту; - спецификация изготовителя; - функциональное тестирование; - моделирование отказов; - документация

Приложение G
(справочное)

Примеры функций безопасности

G.1 Общие положения

В МЭК 62061:2021, приложение G, приведены общие примеры типичных функций безопасности.

Определение функции безопасности отличается от определения ИСО 12100, поскольку в настоящем стандарте рассматривается снижение риска, выполняемое SCS или SRP/CS.

Примечание — Функции безопасности разработаны в соответствии с МЭК 62061 или ИСО 13849-1.

На основании дополнительной информации в разделах 4 и 5 конкретные функции безопасности перечислены в настоящем приложении.

G.2 Функции безопасности

G.2.1 Основная информация

В таблице G.1 приведен неисчерпывающий список примеров функций безопасности согласно ИСО 12100. Необходима некоторая базовая информация для описания реализованной функции безопасности.

Таблица G.1 — Примеры функций безопасности и связанных с ними устройств, связанных с безопасностью

Функции безопасности для защиты людей
Блокировочная защита
Блокировочное ограждение с блокировкой ограждения
Блокировочная защита с функцией запуска (с функцией ручного сброса)
Чувствительные средства защиты (SPE), шумоподавление
Чувствительные к давлению защитные устройства
Устройство со сбросом (кнопка)
Удерживающее устройство управления
Двуручное устройство управления
Разрешающее устройство
Другие функции безопасности
Выбор локального управления
Устройство ручного выбора параметров (и процедура)
Устройство (и процедура) ручного выбора режима работы
Устройство аварийного останова
Устройство управления энергией (и процедура)
Функции безопасности для обеспечения полноты безопасности машины
Ограниченная эксплуатация — другие защитные устройства
Эксплуатация в заданных ограничениях — другие защитные устройства

G.2.2 Подробное описание требований безопасности

Выполнение отдельной оценки риска не требуется, если требования к функции безопасности уже описаны в соответствующем стандарте типа С.

Если нет определенных требований, функция безопасности будет определяться в соответствии со спецификациями, требуемыми МЭК 62061 или ИСО 13849-1.

Спецификация требований безопасности определяет все требования к функции безопасности в отношении безопасности людей и окружающей среды. Она определяется на основе оценки рисков.

В таблице G.2 представлен обзор базовой информации, связанной с техническими требованиями по безопасности.

Таблица G.2 — Основная информация, связанная со спецификацией требований безопасности

Основная информация о функциях безопасности
Название функции безопасности (SF)
Краткое описание функций
Инициирующее событие
Реакция, связанная с безопасностью
Режим работы
Требуемая безопасность, PL_r/SIL
Частота запросов (интенсивность запросов)
Движение с превышением скорости
Поведение в случае сбоя питания
Приоритеты при комбинировании отдельных запросов
Дополнительная функция безопасности
Дополнительные параметры
Меры по обнаружению сбоя
Меры реагирования на сбой (функция)
Надлежащее использование
Безопасное состояние
Критерии достижения безопасного состояния машины
Предельные значения и критерии срабатывания функции безопасности
Подтверждение и перезапуск после обнаружения сбоев
Возможности обхода функции безопасности
Требования к датчикам
Требования к приводам
Требования к логике
Время реакции (с)
Вмешательство оператора
Интерфейсы с функциями, не связанными с безопасностью

Следующие вопросы могут быть важными:

- изучение следующих стандартов:
  МЭК 60204-1 — электробезопасность;
  ИСО 14119 — блокирующие ограждения;
  МЭК 61496 — электрочувствительное защитное оборудование;
  ИСО 13850 — функции аварийной остановки;
  ИСО 13851 — устройства управления двумя руками — функциональные аспекты и принципы проектирования;
  ИСО 13857 — безопасные расстояния для предотвращения попадания в опасные зоны верхних и нижних конечностей;
  ИСО 14118 — предотвращение неожиданного запуска;
  другие;
  …
- функциональное описание функции безопасности:
  «Когда защитная дверь открыта, двигатель немедленно останавливается»;
  …;

- меры по обеспечению систематической полноты безопасности с применением принципов безопасности:
  основные принципы безопасности ✓:...
  хорошо отработанные принципы безопасности ✓:...
  хорошо отработанные компоненты ✓:....
  …;
- систематическая полнота безопасности привлекает другие дополнительные меры:
  Предотвращение ✓ : Выбор компонентов
  ✓ : …
  Управление ✓ : Напряжение
  ✓ : EMC, EMI
  ✓ : ...
  …;
- другие дополнительные требования:
  Перезапуск — когда опасная зона доступна, автоматический перезапуск не разрешен;
  Неожиданный перезапуск — до тех пор, пока блокировочная защита открыта;
  другие;
  … .

G.2.3 Пример блокировки ограждения

Параметры, связанные с безопасностью, для функции безопасности с требуемым значением SIL 1, приведены для примера в таблице G.3.

Таблица G.3 — Пример параметров, связанных с безопасностью, для функции безопасности с требуемым уровнем SIL 1

Вход	Логика	Выход
Ограничения по архитектуре, макс. SIL 1 HFT = 0 Категория = 1 DC = 0 Частота отказов Позиционный переключатель 1 B_{10D} [циклов] = 20 000 000 C [1/ч] = 1 λ_D [1/ч] = 5,0 E-09 высокий $MTTF_D$ [a] = 22 831 T_{10D} [a] = 2283 SFF = 0 PFH (< SIL 3) Базовая архитектура подсистемы A PFH = 5,0 E-09 Достигнут SIL 1		Ограничения по архитектуре, макс. SIL 1 HFT = 0 Категория = 1 DC = 0 Частота отказов Контактор 1 B_{10D} [циклов] = 1 300 000 C [1/ч] = 1 λ_D [1/ч] = 7,7 E-08 высокий $MTTF_D$ [a] = 1484 T_{10D} [a] = 148 SFF = 0 PFH (< SIL 3) Базовая архитектура подсистемы A PFH = 7,7 E-08 Достигнут SIL 1

Параметры, связанные с безопасностью для функции безопасности с требуемым уровнем SIL 3, приведены, например, в таблице G.4.

Таблица G.4 — Пример параметров, связанных с безопасностью, для функции безопасности с требуемым уровнем SIL 3

Вход	Логика	Выход
Ограничения по архитектуре, макс. SIL 3 HFT = 1 Категория = 3 DC = 0,90 Частота отказов Позиционный переключатель 1 (с отдельным приводом) B_{10D} [циклов] = 20 000 000 Позиционный переключатель 2 (с отдельным приводом) B_{10D} [циклов] = 20 000 000 C [1/ч] = 1 λ_{D1} [1/ч] = 5,0 E-08 λ_{D2} [1/ч] = 5,0 E-08 высокий $MTTF_{D1}$ [a] = 2283 высокий $MTTF_{D2}$ [a] = 2283 T_{10D1} [a] = 228 T_{10D2} [a] = 228 SFF = 90 % PFH (< SIL 3) Базовая архитектура подсистемы D PFH = 1,0 E-09 Достигнут SIL 3		Ограничения по архитектуре, макс. SIL 3 HFT = 1 Категория = 4 DC = 0,99 Частота отказов Контактор 1 B_{10D} [циклов] = 1 300 000 Контактор 2 B_{10D} [циклов] = 1 300 000 C [1/ч] = 1 λ_{D1} [1/ч] = 7,7 E-08 λ_{D2} [1/ч] = 7,7 E-08 $MTTF_{D1}$ [a] = 1484 $MTTF_{D2}$ [a] = 1484 T_{10D1} [a] = 148 T_{10D2} [a] = 148 SFF = 99 % PFH (< SIL 3) Базовая архитектура подсистемы D PFH = 1,6 E-09 Достигнут SIL 3

Приложение Н
(справочное)

Оценка значения PFH подсистемы

Н.1 Общие положения

В настоящем приложении представлены подходы к оценке значения PFH подсистемы.

Примечание — Оценка значения PFH подсистемы основана на МЭК 62061 или ИСО 13849-1.

Н.2 Подход к распределению таблиц (МЭК 62061)

Следующее упрощение может быть применено для подсистем, основанных на распределении Вейбулла:

- $\lambda_D \approx C / B_{10D}$ [1/ч] или $MTTF_D = 1/8760\ \lambda_D$ [лет] ;
- $T_1 = T_{10D} \approx 0{,}1/\lambda_D$ [ч] или $T_1 = 0{,}1/8760\ \lambda_D = 0{,}1\ MTTF_D$ [лет].

Значения PFH могут быть оценены с использованием таблиц Н.1 и Н.2 МЭК 62061:2021 со следующим ограничением:

- T_1 равно 20 годам;
- для двухканальных подсистем (HFT = 1) $MTTF_D$ каждого канала равно;
- если $MTTF_D$ на канал отличается, в качестве наихудшего варианта может использоваться для обоих каналов либо наименьшее значение $MTTF_D$ из двух каналов, либо среднее геометрическое значение $MTTF_D$ обоих каналов $MTTF_D = (MTTF_{D1} \cdot MTTF_{D2})^{1/2}$.

Н.3 Упрощенные формулы для оценки значения PFH (МЭК 62061)

В МЭК 62061:2021, раздел Н.2, описан упрощенный подход к оценке PFH для ряда основных архитектур подсистем и даны формулы, которые могут быть использованы для подсистем.

Дальнейшие подходы описаны в настоящем стандарте в разделе Н.4.

Н.4 Подходы МЭК 61508, МЭК 62061 и ИСО 13849-1

Н.4.1 Общие положения

Оценка формул для вычисления PFH может выполняться различными способами с соответствующими граничными условиями. В настоящем разделе будут описаны различные способы.

Ряд методов оценки надежности, в той или иной степени, непосредственно используются для анализа ненадежности подсистем, связанных с безопасностью, среди которых — блок-схемы надежности и цепи Маркова. В МЭК 62061 традиционно используются блок-схемы надежности и предполагается, что подсистемы не подлежат ремонту (за исключением формул в МЭК 62061:2021, раздел Н.4), в то время как в ИСО 13849-1 всегда использовалось моделирование Маркова и предполагалось, что подсистемы подлежат ремонту.

В контексте МЭК 62061 основной подход и важность T_{10} будут подробно описаны в разделе Н.6. В разделе Н.7 дается обзор формул PFH, полученных в настоящем приложении.

Н.4.2 Подход МЭК 61508

Н.4.2.1 Общие положения

Методы обеспечения надежности отсортированы в соответствии с двумя следующими точками зрения:

- статические (булевы) и динамические (состояния/переходы) модели;
- аналитические расчеты по сравнению с расчетами моделирования методом Монте-Карло.

Логические модели охватывают все модели, описывающие статические логические связи между элементарными отказами и полным отказом системы. Блок-схемы надежности (RBD) и деревья отказов (FT) относятся к булевым моделям.

Модели состояний/переходов охватывают все модели, описывающие поведение системы (переходы из состояния в состояние) в соответствии с возникающими событиями (отказы, ремонты, тесты и т. д.). Марковские процессы, сети Петри и модели на основе формальных языков, относятся к моделям состояний/переходов.

Примечание — Для получения дополнительной информации см. МЭК 61508-6:2010, приложение В.

Упрощенный подход основан на графических представлениях RBD.

Когда E/E/PE система, связанная с безопасностью, используется в непрерывном режиме работы или режиме работы с высокой частотой запросов, МЭК 61508-6:2010 требует расчета ее PFH. Это среднее значение так называемой безусловной интенсивности отказа (также называемой частотой отказа) $w(t)$ за интересующий период:

$$\mathrm{PFH}(T) = \frac{1}{T}\int_0^T w(t)\,dt.$$

Н.4.2.2 Ограничения МЭК 61508

Использование подхода на основе блок-схемы надежности (RBD) предполагает, что частота отказов постоянна. Расчеты основаны на следующих предположениях:

- результирующая средняя вероятность отказа по запросу для системы менее 10^{-1} или результирующая средняя частота опасного отказа для системы менее 10^{-5} $ч^{-1}$;
- частота отказов элементов постоянна в течение срока службы системы;
- общая частота отказов аппаратных средств канала подсистемы — сумма частоты опасных отказов и частоты безопасных отказов для этого канала, которые принимаются равными;
- интервал контрольных проверок на порядок больше, чем MRT;
- для каждой подсистемы установлен отдельный интервал проведения контрольных проверок и MRT;
- ожидаемый интервал между запросами на порядок больше интервала контрольных проверок;
- для всех подсистем, работающих в режиме с высокой частотой запросов или в непрерывном режиме, доля отказов, определяемая охватом диагностикой, обнаруживается и устраняется в пределах величины MTTR (среднее время восстановления, как правило, принимаемое равным 8 ч), используемой для определения требований к полноте безопасности аппаратных средств;
- для групп с голосованием 1oo1 и 2oo2, работающих в режиме с высокой частотой запросов или в непрерывном режиме, E/E/PE система, связанная с безопасностью, всегда достигает безопасного состояния после обнаружения опасного сбоя; для достижения этого ожидаемый интервал между запросами на порядок больше, чем интервалы контрольных проверок, или сумма интервалов контрольных проверок и время достижения безопасного состояния меньше, чем время безопасности процесса;
- в тех случаях, когда используется термин «канал», он ограничивается только той частью рассматриваемой системы, которая, как правило, является подсистемой из датчика, логики или исполнительного элемента.

Н.4.3 Подход МЭК 62061

Н.4.3.1 Общие положения

Упрощенный подход основан на графических представлениях RBD, где используются четыре основные архитектуры.

Значение PFH функции безопасности задается суммой значений PFH всех подсистем, участвующих в выполнении функции безопасности.

Н.4.3.2 Ограничения МЭК 62061

Упрощенные формулы, используемые для оценки значения PFH, основаны на следующих предположениях:

- методика моделирования основана на блок-схемах надежности (RBD);
- экспоненциальная модель отказа (частота отказов компонентов постоянна в течение срока службы компонента);
- системы неремонтопригодны;
- неготовность $P(t) = 1 - e^{-\lambda t}$;
- плотность распределения отказов $P'(t)$;
- предполагается, что величина $(\lambda t) \leq 0{,}1$, это позволяет считать, что $P'(t) \approx \lambda$;
- для отказов по общей причине величина β фактора поддерживается в диапазоне от 1 % до 10 %;
- в отношении срока службы компонентов, которые подвержены старению и износу, механизм отказа ограничен T_{10D};
- общая частота отказов аппаратных средств канала подсистемы — сумма частоты опасных отказов и частоты безопасных отказов для этого канала;
- для голосующих групп 1oo1 и 2oo2, работающих в режиме с высокой частотой запросов или в непрерывном режиме, SCS всегда достигает безопасного состояния после обнаружения опасного сбоя; для достижения этого ожидаемый интервал между запросами на порядок больше, чем интервалы контрольных проверок, или сумма интервалов контрольных проверок и время достижения безопасного состояния меньше, чем время безопасности процесса;
- в тех случаях, когда используется термин «канал», он ограничивается только той частью рассматриваемой системы, которая, как правило, является подсистемой датчиков, логики и исполнительных элементов.

Н.4.4 Подход ИСО 13849-1:2015, приложение К

Н.4.4.1 Общие положения

По сравнению с SIL, ИСО 13849-1 использует уровень эффективности защиты (PL) для выражения связанной с безопасностью способности функций безопасности. «PL a» — «PL e» обозначают уровень эффективности защиты в порядке возрастания. Как и в случае SIL, каждый PL требует, чтобы PFH (в ИСО 13849-1 PFH называется PFH_D) не превышал количественный предел, специфичный для PL.

ИСО 13849-1 допускает любой метод расчета для PFH, который адекватно учитывает функции, перечисленные в ИСО 13849-1:2015, пункт 4.5.1, то есть частоту отказов, диагностику, восприимчивость к отказам по общей причине и архитектуру системы.

Тем не менее, ИСО 13849-1:2015, пункт 4.5.4, предоставляет упрощенную процедуру для оценки количественных аспектов PL, то есть для оценки PFH. ИСО 13849-1:2015, приложение К, состоит только из таблицы К.1. В рамках упрощенной процедуры и в связи с другими приложениями ИСО 13849-1:2015, таблица К.1, используется для получения PFH подсистемы, выполняющей функцию безопасности, или ее части.

Для реализации функций безопасности или подсистем, реализующих часть функции безопасности, ИСО 13849-1 определяет пять категорий (B и от 1 до 4), прежде всего путем определения поведения (под)системы при наличии сбоев. Поскольку это поведение в основном зависит от архитектуры системы, ИСО 13849-1 предлагает специально определенную архитектуру для каждой категории. Хотя указанные архитектуры не являются обязательными для конкретной категории, они служат основой для определения PFH.

Пять специально определенных архитектур можно отнести к трем основным архитектурам:

- категория B и категория 1: одноканальная, не диагностируемая (1oo1);
- категория 2: одноканальная с отдельным устройством для диагностики (1oo1D);
- категория 3 и категория 4: двухканальная, каналы взаимно диагностируемые (1oo2D).

Примечание 1 — Несмотря на то, что категория 4, требует значение отказоустойчивости не менее двух, консервативная оценка PFH выполняется на основе двухканальной архитектуры в сочетании с высоким охватом диагностикой 99 %.

ИСО 13849-1 допускает только высокую частоту запросов к функции безопасности, т. е. запрос происходит один раз в год.

По этой причине PFH может быть отождествлен с интенсивностью отказов.

Методика определения PFH по упрощенной процедуре (фактически: по интенсивности отказов) для специально определенных архитектур предполагает наличие высокой частоты запросов вплоть до непрерывного запроса для категорий B, 1, 3 и 4.

Причина этого заключается в том, что в пределах этого диапазона частоты запросов соответствующие специально определенные архитектуры не демонстрируют значительной зависимости PFH от фактической частоты запросов. Однако специально определенная архитектура для категории 2 обладает такой зависимостью.

Чтобы устранить эту зависимость, упрощенная процедура предполагает подходящий и практически значимый случай, когда любой обнаруживаемый отказ единственного функционального канала всегда будет обнаружен в надлежащее время до возникновения запроса или что скорость тестирования намного выше, чем частота запросов.

Кроме того, упрощенная процедура предполагает восстановление дефектных систем и новый запуск в течение незначительного периода времени, как только отказ был обнаружен диагностикой или был выявлен в результате аварии, в последнем случае внеся вклад в PFH.

Типичная работа подсистем, применяющих специально определенные архитектуры в области машин, приводит к очень низкому влиянию времени восстановления на PFH, а если пренебречь временем восстановления, то это подразумевает оценку с безопасной стороны в отношении PFH.

В ИСО 13849-1:2015, таблица K.1, приведены предварительно рассчитанные значения PFH для пяти категорий, определенных в ИСО 13849-1. Эти значения были получены путем применения марковского моделирования к специально определенным архитектурам. Теперь возможные комбинации отказов функциональных блоков или отказов каналов составляют различные состояния системы. Отказы, испытания, запросы функции безопасности и ремонт приводят к переходам между состояниями системы, формируя таким образом модель перехода состояний.

Поскольку восстановление после аварии также рассматривается, нет никаких поглощающих состояний, то есть состояний без выхода. Некоторые состояния системы являются опасными, что означает невозможность выполнения функции безопасности. Предполагается, что все скорости перехода состояния являются постоянными во времени или аппроксимируются как постоянные во времени. Поэтому модели перехода состояний становятся марковскими моделями, которые позволяют легко численно оценить развитие во времени вероятности состояний и потоков между состояниями. Все потоки, выходящие из опасных состояний системы и вследствие запросов к функции безопасности, принимаются в качестве вклада в PFH. Среднее по времени значение их суммы дает PFH.

Одним из входных параметров, используемых для численной оценки, является частота отказов канала в опасную сторону.

Из-за предположения, что частота отказов постоянна во времени, среднее время до опасного отказа $MTTF_D$ задается обратной величиной λ_D частоты опасных отказов. Чтобы иметь дело с удобной мерой, в ИСО 13849-1 было принято решение использовать $MTTF_D$ в годах вместо опасной частоты отказов. Таким образом, $MTTF_D$ просто следует интерпретировать как синоним $1/\lambda_D$ и не путать с гарантированным сроком службы.

Вторым существенным входным параметром является среднее значение охвата диагностикой функционального канала DC_{avg}, выраженное в процентах.

ИСО 13849-1 требует архитектуры, подразумевающие резервирование для ограничения отказов по общей причине. Используется простая процедура оценки β фактора для предоставления доказательств того, что были предприняты достаточные усилия для ограничения отказов по общей причине максимальным значением 2 % (ИСО 13849-1:2015, приложение F). Упрощенная процедура ИСО 13849-1 предполагает, что это требование выполнено. Упрощенная процедура ИСО 13849-1 разработана таким образом, чтобы обеспечить результаты с небольшими затратами на моделирование, в оптимальном случае без сложных расчетов. Таким образом, знание категории, $MTTF_D$ функционального канала(ов) и DC_{avg} достаточно для получения величины PFH для (под)системы из ИСО 13849-1:2015, таблица K.1. Гистограмма из ИСО 13849-1:2015, рисунок 5, представляет собой краткий обзор числового содержания таблицы K.1.

Примечание 2 — ИСО 13849-1:2015, рисунок 5, не охватывает значения PFH для категории 4 с $MTTF_D >$ > 100 лет, в то время как ИСО 13849-1:2015, таблица K.1, включает значения $MTTF_D$ до 2500 лет для категории 4.

Если функциональный канал содержит несколько функциональных блоков или компонентов, его $MTTF_D$ будет рассчитываться по значениям $MTTF_D$ блока или компонента до использования таблицы К.1. Для этого в приложении D приводится простое уравнение (D.1).

В случае категории 3 или 4, использующей каналы с неравным $MTTF_D$, должно использоваться среднее значение $MTTF_D$ для ИСО 13849-1:2015, таблица К.1. Оно рассчитывается по уравнению (D.2) приложения D.

Соответственно, до применения ИСО 13849-1:2015, таблица К.1, ряду функциональных блоков или компонентов с различными значениями DC будет присвоено среднее значение DC, DC_{avg}. Это значение получено из уравнения (Е.1) приложения Е ИСО 13849-1:2015. То же самое уравнение может использоваться для категории 3 или 4, если значения DC двух каналов различны.

Н.4.4.2 Ограничения ИСО 13849-1:2015, приложение К

Упрощенная процедура ИСО 13849-1 поддерживает только специально определенные архитектуры.

Если отличающиеся архитектуры могут быть декомпозированы на последовательность подсистем, каждая из которых представляет специально определенную архитектуру, то упрощенная процедура может применяться к каждой подсистеме отдельно. Затем значение PFH функции безопасности задается суммой значений PFH всех подсистем, участвующих в выполнении функции безопасности.

Упрощенную процедуру ИСО 13849-1 также допускается использовать, если другая архитектура может быть сопоставлена с одной из специально определенных архитектур с помощью упрощений с безопасной стороны, то есть пренебрегая резервированием.

Как и большинство методов количественной оценки, упрощенная процедура предполагает постоянную во времени частоту отказов. Поэтому использование деталей, подверженных износу, требует ограничения рабочего времени до значения T_{10D}, заданного уравнением (С.3).

Использование упрощенной процедуры из ИСО 13849-1 подразумевает, что значение PFH всегда должно быть получено из ИСО 13849-1:2015, таблица К.1, то есть единственной таблицы ограниченного размера. Поэтому в отношении входных параметров вводятся некоторые ограничения.

Время миссии системы безопасности установлено в 20 лет.

Значение β фактора для учета отказов по общей причине определено в 2 %, что означает, что β более 2 % не поддерживается. В случае, если β составляет менее 2 %, процедура дает оценку с безопасной стороны.

В случае одноканальной архитектуры с диагностикой категории 2 (1oo1D) поддерживается только оптимальное по времени тестирование. Это означает, что любой обнаруживаемый отказ одного функционального канала всегда должен быть обнаружен вовремя или по крайней мере что частота тестирования должна быть намного выше, чем частота запросов.

Кроме того, существуют некоторые численные ограничения упрощенной процедуры в ИСО 13849-1:2015, таблица К.1. Эти ограничения обусловлены спецификациями категорий ИСО 13849-1:2015, 6.2, и они касаются диапазона $MTTF_D$ и значений DC_{avg}, которые охватываются или не охватываются ИСО 13849-1:2015, таблица К.1.

В случае категории В, ИСО 13849-1:2015, таблица К.1, охватывает значения $MTTF_D$ от 3 до 30 лет. Для категории 1 $MTTF_D$ составляет от 30 до 100 лет, тогда как для категории 2 или 3 охватывается диапазон от 3 до 100 лет. В случае категории 4, ИСО 13849-1:2015, таблица К.1, перечислены значения PFH для $MTTF_D$ в диапазоне от 30 до 2500 лет.

Что касается $MTTF_D$, все записи таблицы расположены в шахматном порядке в соответствии с логарифмическим рядом Е24, что приводит к 24 значениям на декаду. Зачастую исходное значение $MTTF_D$ не полностью вписывается в запись таблицы, поэтому необходимо выбрать следующую нижнюю запись.

Примечание 1 — Ограничения диапазона $MTTF_D$ по категориям в ИСО 13849-1:2015, таблица К.1, отражают один из подходов в ИСО 13849-1:2015, чтобы предотвратить достижение системами без резервирования или без *звуковой диагностики* высоких уровней производительности исключительно из-за их низкой частоты отказов или, соответственно, из-за их высокого значения $MTTF_D$. Это достигается путем ограничения $MTTF_D$, если оно превышает определенные пределы, тем самым ухудшая определяемое значение PFH.

Более сильное ограничение в ИСО 13849-1:2015, таблица К.1, заключается в предоставлении значений PFH только для одного или двух значений среднего охвата диагностикой, в зависимости от категории.

Для категории 2 или 3 ИСО 13849-1:2015, таблица К.1, поддерживает DC_{avg} 60 % и 90 %. Только для категории 4 поддерживается DC_{avg} 99 %, поскольку ИСО 13849-1 не допускает более низкого охвата диагностикой в этой категории. На практике (без дополнительных ресурсов под рукой) в случае категории 2 или 3 DC_{avg} между 60 % и 90 % должен быть ограничен значением 60%, а DC_{avg} выше 90% должен быть ограничен значением 90 %. Существенное ограничение несомненно приведет к значительному увеличению значения PFH, то есть к консервативной оценке.

Примечание 2 — Необходимо подчеркнуть, что ограничение DC_{avg} до 90 % в категории 2 или 3 является частью подхода ИСО 13849-1 для ограничения достижимого уровня производительности. В качестве побочного эффекта это приводит к более консервативному значению PFH. Свободно доступная программная реализация упрощенной процедуры ИСО 13849-1 использует интерполяцию, чтобы избежать ограничения DC_{avg} между значениями 60 % и 90 %, что позволяет определять более точные значения PFH.

Н.5 Основные соображения относительно экспоненциального распределения и распределения Вейбулла

Н.5.1 Экспоненциальное распределение

Неготовность (ненадежность) элемента с постоянной частотой отказов λ может быть выражена в виде интегральной функции распределения (CDF), основанной на экспоненциальном распределении, следующим образом:

$$P(t) = 1 - e^{-\lambda t}, \quad (Н.1)$$

где t — время.

Если $(\lambda t) << 1$, то упрощенный подход к оценке $P(t)$ может иметь вид:

$$P(t) \approx \lambda t. \quad (Н.2)$$

Предположение $e^{-\lambda t} \approx 1 - \lambda t$ основано на реальной экспоненциальной функции, как правило, определяемой следующими степенными рядами:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} \ldots .$$

Примечание — $P(t)$ может быть записано как $P(t) \approx -x - \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} - \ldots$, где $x = -\lambda t$.

С точностью до 1 % $\frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} - \ldots \le \frac{-x}{100}$, что приводит к $-x \le \frac{1}{50}$; $-x \le \frac{1}{10}$ применяется соответственно с точностью ≤ 5 % и $-x \le \frac{1}{5}$ с точностью ≤ 10 %.

В надлежащей инженерной практике допустима точность 5 % и $(\lambda t) << 1$ можно записать как $\lambda t \le \frac{1}{10}$.

На основании формулы (Н.1) функцию плотности вероятности $P'(t)$ можно записать как

$$P'(t) = \frac{d}{dt} P(t) = \lambda e^{-\lambda t}, \quad (Н.3)$$

где t — время;

λ — постоянная частота отказов.

Н.5.2 Распределение Вейбулла

Неэлектронные компоненты, как правило, характеризуются распределением Вейбулла.

В соответствии с МЭК 61649 интегральная функция распределения Вейбулла $F(t)$ (как неготовность элемента) определяется как

$$F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}}, \quad (Н.4)$$

где t — время;

η — характерное время жизни или параметр масштаба (распределения);

β — параметр формы (распределения).

Три диапазона значений параметров формы β являются очевидными:

- для $\beta = 1$ распределение Вейбулла идентично экспоненциальному распределению;
- $\beta > 1$ — случай увеличения относительной частоты отказов;
- $\beta < 1$ — случай снижения относительной частоты отказов.

$F(t) = P(t)$ при $\eta = 1/\lambda$ и $\beta = 1$.

Если $\left(\frac{t}{\eta}\right)^{\beta} << 1$, тогда может быть принят упрощенный подход для оценки $F(t)$:

$$F(t) = \left(\frac{t}{\eta}\right)^{\beta}. \quad (Н.5)$$

Предполагая $\eta = 1/\lambda$, формулу (Н.5) можно записать как

$$F(t) \approx (\lambda t)^{\beta}. \quad (Н.6)$$

В соответствии с МЭК 61649 функция плотности вероятности Вейбулла определяется как

$$F(t) = \frac{d}{dt} F(t) \approx \beta \frac{t^{\beta-1}}{\eta^{\beta}} e^{-\left(\frac{t}{\eta}\right)^{\beta}}, \quad (Н.7)$$

где t — время;

η — характерное время жизни или параметр масштаба;

β — параметр формы.

Относительная частота отказов $\lambda(t)$ определяется как

$$\lambda(t) = \beta \frac{t^{\beta-1}}{\eta^{\beta}}. \quad (H.8)$$

H.6 T_{10} и B_{10}

H.6.1 Общие положения

Для электромеханических аппаратов управления и для пневматических клапанов, которые характеризуются двумя состояниями (открыт или закрыт), отказы в основном связаны с продолжительностью их использования (которая зависит от количества циклов). Для этих компонентов номинальный срок службы, как правило, измеряется в циклах B_{10} (количество циклов до тех пор, пока 10 % компонентов откажут при испытании на долговечность).

Значение B_{10D} — это количество циклов до тех пор, пока с 10 % компонентов произойдут опасные отказы, которое можно оценить с помощью $B_{10D} = B_{10}$/RDF, где RDF — доля опасных отказов (сравнимо с $MTTF_D = MTTF/RDF$).

Если RDF неизвестен или недоступен, то B_{10D} можно определить как $B_{10D} = 2B_{10}$. Информация о B_{10D} преобразуется как функция времени по следующему соотношению: $T_{10D} = T_{10}/n_{op}$.

Коэффициент пересчета — среднее количество срабатываний за год (n_{op}).

T_{10D} означает прошедшее время, в течение которого с 10 % протестированных компонентов произойдут опасные отказы.

Благодаря практической процедуре испытаний (например, изготовителем компонентов) RDF может быть оценен только как T_{10}. Для рассматриваемого времени T_{10} не существует практических значений RDF, потому что процедуры испытаний заканчиваются на T_{10}. Ограничением должно быть T_{10}, а не T_{10D}. Благодаря положениям ИСО 13849-1 была установлена T_{10D}, и формула (H.12) представляет собой компромисс, ограничивая T_{10D}, когда различие между T_{10} и T_{10D} становится слишком большим (то есть RDF ≤ 50 %).

Предполагая в качестве первого приближения, что отказы следуют экспоненциальному распределению вместо распределения Вейбулла, оценка надежности (MTTF) на основе полного срока службы T_{10D} таких компонентов может быть вычислена на основе полного срока службы T_{10}.

H.6.2 T_{10} при экспоненциальном распределении

Неготовность T_{10} при экспоненциальном распределении записывается как

$$P(T_{10}) = 1 - e^{-\lambda T_{10}} = 0,1 \quad (H.9)$$

и на основе общих формул $y = e^x$ и $x = \ln y$ приводит к

$$T_{10} \frac{\ln(0,9)}{\lambda} \approx 0,1 \frac{1}{\lambda} = 0,1\ MTTF. \quad (H.10)$$

С B_{10}, B_{10D} и n_{op}, средним количеством срабатываний за год, можно записать следующее соотношение:

$$T_{10} = \frac{B_{10}}{n_{op}} \approx 0,1\ MTTF \text{ или } T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{B_{10}}{RDF n_{op}} \approx 0,1\ MTTF_D. \quad (H.11)$$

На основе формулы (H.16) MTTF и $MTTF_D$ для компонентов могут быть рассчитаны как

$$MTTF \approx \frac{B_{10}}{0,1 n_{op}} \text{ или } MTTF_D \approx \frac{B_{10D}}{0,1 n_{op}} = \frac{B_{10}}{RDF 0,1 n_{op}}.$$

Если RDF ≤ 50 %, то T_{10D} будет ограничен:

$$T_{10D} = \frac{B_{10}}{RDF n_{op}} = \frac{B_{10}}{0,5 n_{op}} \approx 0,1\ MTTF_D. \quad (H.12)$$

По достижении T_{10} интегральная функция распределения Вейбулла резко возрастает, и доля опасных отказов (RDF) компонента изменяется. Таким образом, T_{10} представляет собой максимальное значение времени контрольных проверок или срока службы. После T_{10} неэлектронные компоненты будут заменены.

H.6.3 T_{10} при распределении Вейбулла

Неготовность за время T_{10} с помощью распределения Вейбулла, например с параметром формы распределения 2, можно записать как

$$F(T_{10}) = 1 - e^{-(\lambda_W T_{10})^2}, \quad (H.13)$$

что приводит к

$$T_{10} = \frac{\sqrt{-\ln(0,9)}}{\lambda_W} \approx 0,325\frac{1}{\lambda}. \quad \text{(Н.14)}$$

Зависимость между интенсивностью отказов данного распределения Вейбулла и экспоненциальным распределением на основе формулы (Н.10) и формулы (Н.14) при T_{10} имеет вид:

$$T_{10} = \frac{\sqrt{-\ln(0,9)}}{\lambda} = \frac{\sqrt{-\ln(0,9)}}{\lambda_W} \quad \text{(Н.15)}$$

или

$$\lambda_W = \frac{\lambda}{\sqrt{-\ln(0,9)}} = \frac{\lambda}{\sqrt{\ln\left(\frac{1}{0,9}\right)}} = \ln\left(\frac{1}{0,9}\right)^{-\frac{1}{2}}\lambda = 3,08\lambda. \quad \text{(Н.16)}$$

В следующем примере показана релевантность T_{10}:
- при B_{10} = 1 000 000 циклов;
- рабочем цикле C = 1/ч или n_{op} = 8760 циклов в год;
- MTTF становится MTTF ≈ 1141 года и T_{10} ≈ 114 лет.

В рассматриваемое время T_1 = 20 лет число циклов составляет 8760 циклов в год · 20 [a] или 175 200 [циклов], что соответствует только 17,52 % значения B_{10}.

На рисунке Н.1 показаны функции распределения и значение, различающее готовность функций распределения, равное примерно 6.

Экспоненциальное распределение будет иметь наихудшее значение неготовности по сравнению с распределением Вейбулла.

Когда T_{10} > 20 лет или T_{10} < T_1, распределение Вейбулла и экспоненциальное распределение будут значительно различаться. Поэтому T_{10} является важным ограничением для оценки значений PFH.

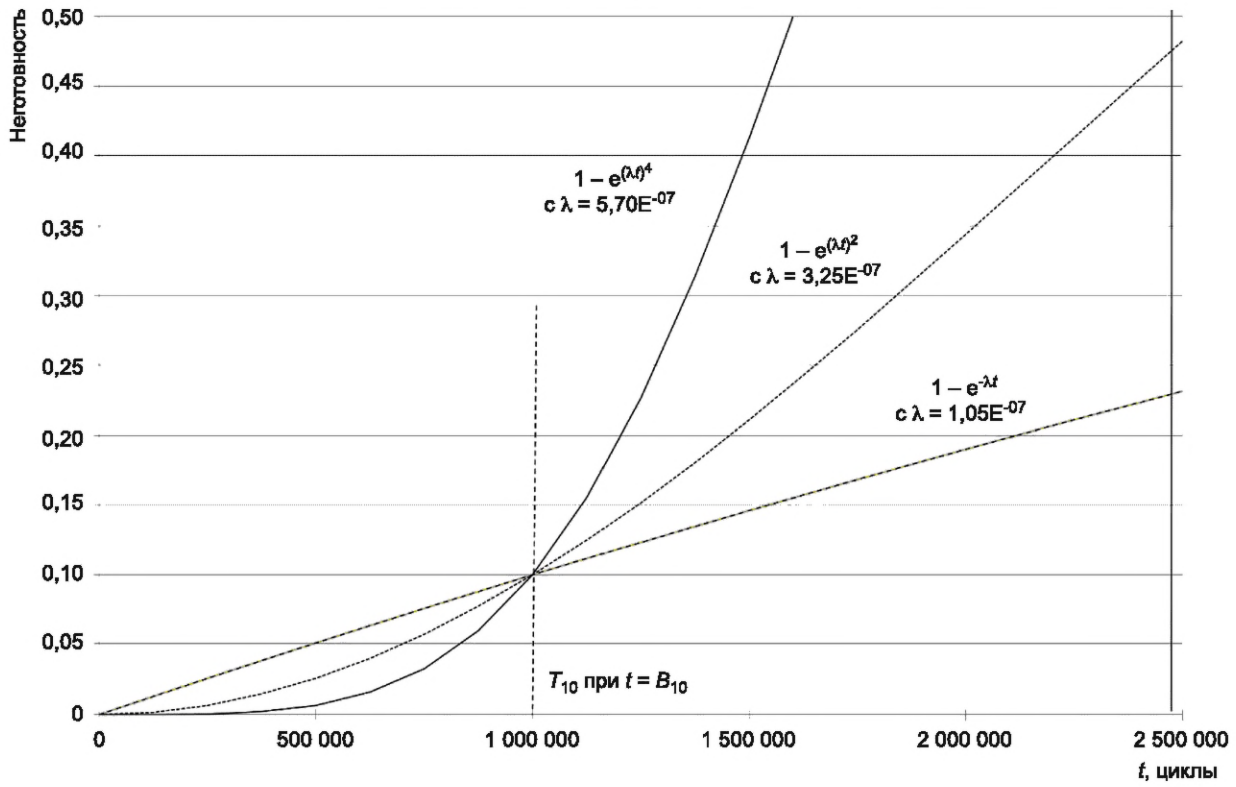


Рисунок Н.1 — Интегральные функции распределения (CDF)

Значение λ можно считать постоянным при допущении, что значение t для рассматриваемого периода времени:
- равно полезному сроку службы электронных компонентов и
- равно наименьшему из полезного срока службы или T_{10D} для неэлектронных компонентов.

Н.7 Обзор формул PFH

Н.7.1 Определения

Основным определением PFH (средняя частота отказов) за период [0, T] является

$$\mathrm{PFH} = \frac{1}{T}\int_{T}^{1}\left(\frac{\mathrm{d}}{\mathrm{dt}}P(t)\right)\mathrm{dt} = \frac{1}{T}\int_{0}^{T}P'(t)\,\mathrm{dt}, \qquad (\text{Н.17})$$

где t — время;

$P'(t)$ — функция плотности вероятности (PDF) для невосстанавливаемых подсистем;

T — время миссии, меньше или равное полезному сроку службы подсистемы. Приведенные примеры основаны на времени миссии, равной 20 годам.

Н.7.2 Формулы

Допускается использовать формулы для PFH, перечисленные в таблицах Н.1 — Н.6. Подробное описание этих формул приведено в разделах Н.8 — Н.12.

Примечание — Формулы, приведенные в таблицах Н.1 — Н.6, основаны на блок-схеме надежности и аналогичны при использовании моделирования Маркова согласно ИСО 13849-1 и при упрощенном подходе, где (λ t) << 1, см. Н.5.1.

Таблица Н.1 — Формулы для базовой архитектуры A (1oo1) подсистемы

Формула PFH	Экспоненциальное распределение	Комментарии
λ_D	$\frac{1}{T}\left(1-e^{-\lambda_D T}\right)$	Общая формула
Примечание — Для неэлектронных компонентов можно предположить наихудший случай $\lambda_D = \lambda_{DU}$ = = 1000 FIT с 1 FIT = 1E-09/ч, если ожидаемая скорость запроса составляет менее одного раза в год.		
Обозначения: - λ_D — интенсивность опасных отказов канала, 1/ч; - T — срок службы или время миссии, ч.		

Таблица Н.2 — Формулы для базовой архитектуры C (1oo1D) подсистемы

Формулы PFH	Комментарии
$(1 - \mathrm{DC})\,\lambda_D$	Общая формула (реакция на отказ, выполняемая другой подсистемой)
$(1-\mathrm{DC})\lambda_D^{CC} + \mathrm{DC}\lambda_D^{CC}\lambda_{react}^{CC}(T_1+T_2)/2 + \lambda_{CC}$	Общая формула
$(1 - \beta)(1 - \mathrm{DC}) + (1 - \beta)^2\mathrm{DC}\lambda_D^2\,(T_1 + T_2)/2 + \beta\lambda_D$	Рассмотрение наихудшего случая в контексте машинного оборудования, где $\lambda_{react} \le \lambda_D$ и β мин. (λ_D, λ_{react}) = $\beta\,\lambda_D$
Примечание 1 — Для неэлектронных компонентов может быть принято наихудшее значение $\lambda_D = \lambda_{DU}$ = = 1000 FIT с 1 FIT = 1E-09/ч, если ожидаемая частота запросов составляет менее одного раза в год.	
Обозначения: - β-фактор (0,01; 0,02; 0,05 или 0,1) между основным каналом и каналом, реагирующим на сбой, %; - λ_D — интенсивность опасных отказов основного канала, 1/ч; - λ_{react} — интенсивность отказов канала при реакции на сбой, 1/ч; - DC — охват диагностикой (0; 0,6; 0,9 или 0,99) основного канала, %; - $\lambda_{CC} = \beta$ мин. (λ_D, λ_{react}) — интенсивность отказов по общей причине, 1/ч; - $\lambda_D^{CC} = \lambda_D - \lambda_{CC}$, 1/ч; - $\lambda_{react}^{CC} = \lambda_{react} - \lambda_{CC}$, 1/ч; - T_1 — срок службы, ч; - T_2 — интервал диагностических проверок, ч. Примечание 2 — Другие стандарты по функциональной безопасности используют для T_1 значение времени выполнения миссии T_M.	

Таблица Н.3 — Формулы для базовой архитектуры B (1oo2) подсистемы

Формулы PFH	Комментарии
$\lambda_{D1}^{CC}\lambda_{D2}^{CC}T_1 + \lambda_{CC}$	Общая формула
$(1-\beta)^2\lambda_D^2\,T_1 + \beta\lambda_D$	Общая формула, где $\lambda_D = \lambda_{D1} = \lambda_{D2}$
Примечание 1 — Для неэлектронных компонентов может быть принято наихудшее значение $\lambda_D = \lambda_{DU}$ = = 1000 FIT с 1 FIT = 1E-09/ч, если ожидаемая частота запросов составляет менее одного раза в год.	
Обозначения: - β-фактор (0,01; 0,02; 0,05 или 0,1) между каналом 1 и каналом 2, %; - λ_{D1} — интенсивность опасных отказов канала 1, 1/ч; - λ_{D2} — интенсивность опасных отказов канала 2, 1/ч; - DC_1 — охват диагностикой (0; 0,6; 0,9 или 0,99) канала 1, %; - DC_2 — охват диагностикой (0; 0,6; 0,9 или 0,99) канала 2, %; - λ_{CC} = β мин., (λ_{D1}, λ_{D2}) — интенсивность отказов по общей причине, 1/ч; - $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$, 1/ч; - $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$, 1/ч; - T_1 — срок службы, ч. Примечание 2 — Другие стандарты по функциональной безопасности используют для T_1 значение времени выполнения миссии T_M.	

Таблица Н.4 — Формулы для базовой архитектуры D (1oo2D) подсистемы

Формулы PFH	Комментарии
$\lambda_{D1}^{CC}\lambda_{D2}^{CC}\left((1-DC_1)\frac{T_{1o1}}{2}+(1-DC_2)\frac{T_{1o2}}{2}\right)+\lambda_{D1}^{CC}\lambda_{D2}^{CC}(DC_1+DC_2)\frac{T_2}{2}+\lambda_{CC}$	Общая формула
$\lambda_{D1}^{CC}\lambda_{D2}^{CC}(2-DC_1-DC_2)\frac{T_1}{2}+\lambda_{D1}^{CC}\lambda_{D2}^{CC}(DC_1+DC_2)\frac{T_2}{2}+\lambda_{CC}$	Общая формула, где $T_1 = T_{1o1} = T_{1o2}$
$(1-\beta)^2\lambda_D{}^2((1-DC)T_1 + DCT_2) + \beta\lambda_D$	Общая формула, где $\lambda_D = \lambda_{D1} = \lambda_{D2}$, $DC = DC_1 = DC_2$
Примечание 1 — Для неэлектронных компонентов может быть принято наихудшее значение $\lambda_D = \lambda_{DU}$ = = 1000 FIT с 1 FIT = 1E-09/ч, если ожидаемая частота запросов составляет менее одного раза в год.	
Обозначения: β-фактор (0,01; 0,02; 0,05 или 0,1) между каналом 1 и каналом 2, %; λ_{D1} — интенсивность опасных отказов канала 1, 1/ч; λ_{D2} — интенсивность опасных отказов канала 2, 1/ч; DC_1 — охват диагностикой (0; 0,6; 0,9 или 0,99) канала 1, %; DC_2 — охват диагностикой (0; 0,6; 0,9 или 0,99) канала 2, %; λ_{CC} = β мин., (λ_{D1}, λ_{D2t}) — интенсивность отказов по общей причине, 1/ч; $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$, 1/ч; $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$, 1/ч; T_1 — срок службы, ч; T_{1o1} — срок службы канала 1, ч; T_{1o2} — срок службы канала 2, ч; T_2 — интервал диагностических проверок, ч. Примечание 2 — Другие стандарты по функциональной безопасности используют для T_1 значение времени выполнения миссии T_M.	

Н.7.3 Примеры

На практике значение PFH, основанное на B_{10D} и рабочих циклах, не ограничивает достижимый SIL:

- при частоте цикла один раз в час или один раз в сутки значение PFH (максимальное значение PFH требуемого SIL);
- ограничения архитектуры являются ограничивающим фактором достижимого уровня SIL.

Если рабочий цикл выше, чем один раз в час, то T_{10D} становится важным.

В таблице Н.5 показаны типичные значения с использованием наихудшего случая B_{10D} = 1 000 000 (например, контактор или позиционный переключатель).

Таблица Н.5 — Примеры значений PFH на основе B_{10D}

Одноканальная подсистема (HFT = 0)				DC = 0 %	DC = 60 %	DC = 90 %	
B_{10D}	Циклы	λ_D	$MTTF_D$	PFH = λ_D	PFH < λ_D 0,5	PFH < λ_D 0,2	
1 000 000	1 раз в минуту	6,00 E-06	19	6,00 E-06	2,65 E-06	9,69 E-07	SIL 1 < 1,00 E-05
	1 раз в час	1,00 E-07	1142	1,00 E-07	4,17 E-08	1,26 E-08	SIL 3 < 1,00 E-07
	1 раз в день	4,17 E-09	27 397	<< 1,00 E-08			
	1 раз в неделю	5,96 E-10	191 781				
	1 раз в месяц	1,49 E-10	767 123				
				SIL 1	SIL 1	SIL 2	
				Ограничения архитектуры			

Одноканальная подсистема (HFT = 1)				DC = 60 %	DC = 90 %	DC = 99 %	
B_{10D}	Циклы	λ_D	$MTTF_D$	PFH < λ_D0,06	PFH < λ_D 0,03	PFH < λ_D 0,021	
1 000 000	1 раз в минуту	6,00 E-06	19	3,51 E-07	1,78 E-07	1,26 E-07	SIL 2 < 1,00 E-06
	1 раз в час	1,00 E-07	1142	<< 1,00 E-08			SIL 3 < 1,00 E-07
	1 раз в день	4,17 E-09	27 397				
	1 раз в неделю	5,96 E-10	191 781				
	1 раз в месяц	1,49 E-10	767 123				
				SIL 2	SIL 3	SIL 3	
				Ограничения архитектуры			

Предполагая, что SCS имеет четыре подсистемы, можно рассчитать предельные значения PFH и, следовательно, предельные значения $MTTF_D$ и T_{10D} на основе B_{10D} = 1 000 000 для каждой подсистемы, как показано в таблице Н.6.

Таблица Н.6 — Примеры значений PFH на основе T_{10D} и B_{10D}

Предельные значения SIL с 4 подсистемами		DC = 0 % PFH = λ_D	DC = 60 % PFH < λ_D 0,5	DC = 90 % PFH < λ_D 0,2
HFT = 0	SIL 1, мин. $MTTF_D$ [a] $T_1 = T_{10D}$ [a] Максимальное количество циклов в час	$MTTF_D$ > 48 4,8 24	$MTTF_D$ > 24 2,4 48	
	SIL 2, мин. $MTTF_D$ [a] $T_1 = T_{10D}$ [a] Максимальное количество циклов в час			$MTTF_D$ > 92 9,2 12,5

Окончание таблицы Н.6

Предельные значения SIL с 4 подсистемами		DC = 60 % PFH = λ_D 0,06	DC = 90 % PFH < λ_D 0,03	DC = 99 % PFH < λ_D 0,0212
HFT = 1	SIL 2, мин. $MTTF_D$ [a] $T_1 = T_{10D}$ [a] Максимальное количество циклов в час	$MTTF_D$ > 48 2,8 41	$MTTF_D$ > 24 1,2 95	
	SIL 3, мин. $MTTF_D$ [a] $T_1 = T_{10D}$ [a] Максимальное количество циклов в час		$MTTF_D$ > 136 13,6 8,5	$MTTF_D$ > 92 9,2 12,5

Н.8 Методология оценки CCF

В случае структур с резервированием (архитектуры 1oo1D, 1oo2, 1oo2D) предполагается, что два канала совмещаются, не образуя обратные связи. Следовательно, индивидуальные частоты отказов каналов не будут увеличиваться при их объединении. Частота опасных отказов первого канала $\lambda_{D1} = \lambda_{DD1} + \lambda_{DU1}$, а второго канала — $\lambda_{D2} = \lambda_{DD2} + \lambda_{DU2}$.

Однако каналы не являются полностью независимыми, поскольку одно событие или состояние может вызвать критическую неисправность одновременно на обоих каналах.

По определению отказ по общей причине характеризуется отказом каждого канала по одной и той же («общей») причине: если отказывает только один канал, то это не может быть отказом по общей причине.

Поэтому отказ по общей причине всегда зависит от канала с более низкой частотой отказов:

- максимальная частота отказов по общей причине λ_{CC} возникает при $\beta = 1$ (100 %);
- если частота отказов второго канала выше частоты отказов первого канала, то второй канал имеет дополнительные отказы даже при $\beta = 1$. Эти дополнительные отказы не могут быть отказами по общей причине и λ_{CC} будет ниже, чем более высокая частота отказов двух каналов;
- максимальное количество отказов по общей причине возникает, если каждый отказ канала с меньшей частотой отказов является отказом по общей причине. Следовательно, самая низкая частота отказов двух каналов будет ограничивать λ_{CC}.

Такой подход выражается $\lambda_{CC} \approx \beta$ мин. (λ_{D1}, λ_{D2}), см. рисунок Н.2.

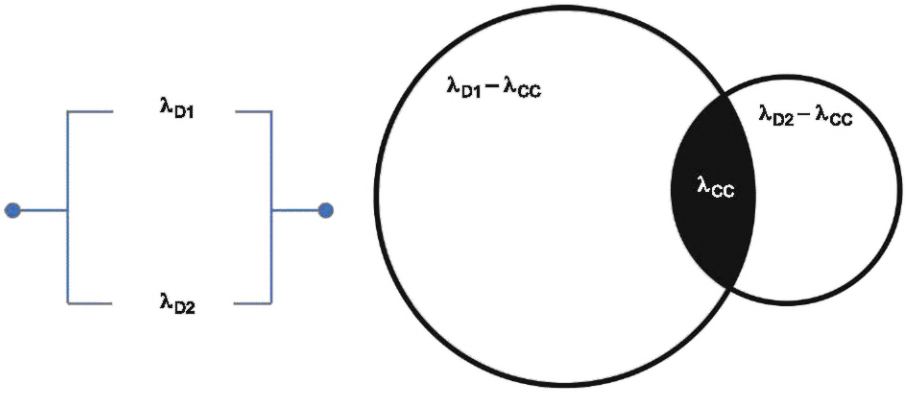


Рисунок Н.2 — Отказ по общей причине

Это уравнение гарантирует, что даже при сильной асимметрии интенсивности отказов интенсивность отказов по общей причине не может превышать нижнюю интенсивность отказов.

Если диагностика (с дополнительным оборудованием) для обнаружения отказов по общей причине не реализована, λ_{CC} дает прямой вклад в PFH, который может быть выражен как β мин. (λ_{D1}, λ_{D2}).

Н.9 Базовая архитектура А (1oo1) подсистемы

Н.9.1 Общие положения

Эта архитектура состоит из одного канала, где любой опасный отказ приводит к отказу функции безопасности при возникновении запроса. На рисунке Н.3 показана блок-схема надежности в момент *t*.

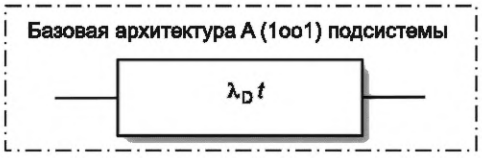


Рисунок Н.3 — Блок-схема надежности базовой архитектуры А (1оо1) подсистемы

Интенсивность опасных отказов канала определяется величиной λ_D. Неготовность $P_D(t)$ представлена на рисунке Н.4.

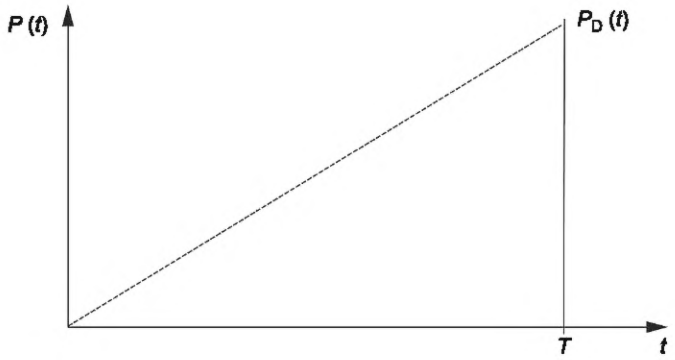


Рисунок Н.4 — Функция неготовности базовой архитектуры А (1оо1) подсистемы

Н.9.2 PFH

Предполагая, что (λt) << 1 в течение периода [0, T], можно использовать следующую упрощенную формулу: $P(t) = \lambda_D t$ (см. Н.5.1).

Для упрощенного подхода $\mathrm{PFH} = \frac{1}{T}\int P_D'(t)\,\mathrm{dt}$ с $P'_D(t) = \lambda_D$ получают:

$$\mathrm{PFH} = \frac{1}{T}\int \lambda_D \mathrm{dt} = \frac{1}{T}\lambda_D [t]_0^T = \lambda_D. \qquad (Н.18)$$

Для подхода $\mathrm{PFH} = \frac{1}{T}\int_0^T P'(t)\,\mathrm{dt}$ с $P'(t) = \lambda_D e^{-\lambda_D t}$ получают:

$$\mathrm{PFH} = \frac{1}{T}\int_0^T \lambda_D e^{-\lambda_D t}\mathrm{dt} = \frac{1}{T}\left[e^{-\lambda_D t}\right]_0^T = \frac{1}{T}\left(1 - e^{-\lambda_D T}\right). \qquad (Н.19)$$

Формула (Н.19) показывает, что значение PFH (средняя частота отказов) может математически уменьшаться по мере увеличения рассматриваемого периода времени T, но для любого компонента аппаратных средств (электронного или неэлектронного) используемое значение PFH не может измениться, т. е. не может уменьшаться только потому, что рассматриваемый период времени меняется, т. е. увеличивается.

Н.9.3 Упрощенный подход Вейбулла

Эта архитектура состоит из одного канала, где любой опасный отказ приводит к отказу функции безопасности при возникновении запроса. На рисунке Н.5 показана блок-схема надежности в момент t, если предположить, например, что коэффициент формы равен 2.

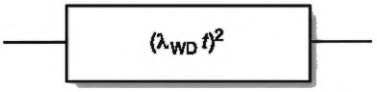


Рисунок Н.5 — Блок-схема надежности 1оо1, упрощенный подход Вейбулла

λ_{WD} представляет интенсивность отказов при распределении Вейбулла [см. также формулу (Н.16)] и может быть записан как

$$\lambda_{WD} \approx 3{,}08\ \lambda_D. \qquad (Н.20)$$

Предполагая, что (λt) << 1, можно использовать следующую упрощенную формулу в течение периода [0, T]: $P_{WD}(t) \approx (\lambda_D t)^2$, и для $\mathrm{PFH} = \frac{1}{T}\int_0^T P'_{WD}(t)\,\mathrm{d}t$ с $P'_{WD}(t) = \lambda_{WD}^2 t$ получают:

$$\mathrm{PFH} = \frac{1}{T}\int_0^T 2\lambda_D{}^2 t\,\mathrm{d}t = \frac{1}{T}\lambda_{WD}{}^2\left[t^2\right]_0^T = \lambda_{WD}{}^2 T \approx 9{,}49\lambda_D^2 T. \quad \text{(H.21)}$$

H.10 Базовая архитектура C (1oo1D) подсистемы

H.10.1 Общие положения

Различают два варианта реализации функции, реагирующей на сбой:

1) вариант 1: другая подсистема выполняет функцию реакции на сбой;

2) вариант 2: отдельный канал подсистемы выполняет функцию реакции на сбой.

H.10.2 Реакция на сбой, выполняемая другой подсистемой

Эта архитектура состоит из одного канала, где любой необнаруженный опасный отказ приводит к отказу функции безопасности при возникновении запроса. Обнаружение любого опасного отказа приведет к безопасному состоянию функции безопасности.

Пример — Фотоэлемент типа 2 подключен к логическому решающему устройству, связанному с безопасностью. Опасные отказы фотоэлемента λ_D циклически контролируются логическим решающим устройством. При срабатывании чувствительного поля фотоэлемента или при обнаружении опасного отказа логический вычислитель останавливает все опасные движения с помощью своего выходного сигнала, связанного с безопасностью.

Логическое представление показано на рисунке H.6.

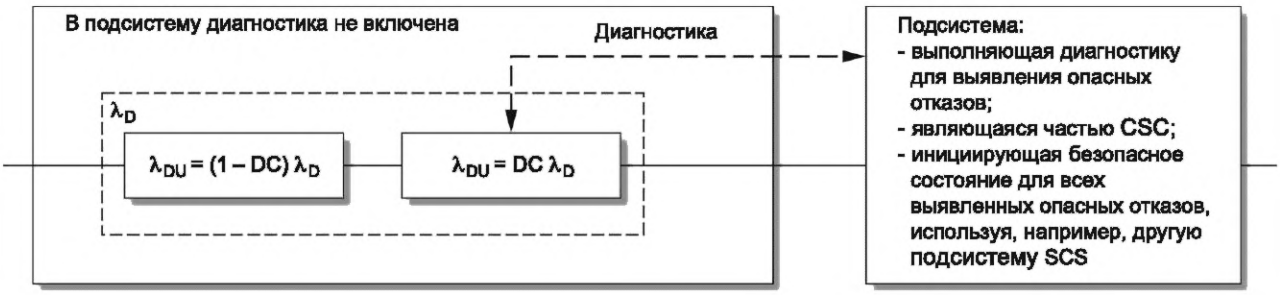


Рисунок H.6 — Логическое представление базовой архитектуры C (1oo1D) подсистемы с инициированием безопасного состояния, используя другую подсистему

На рисунке H.7 показана блок-схема надежности в момент t.

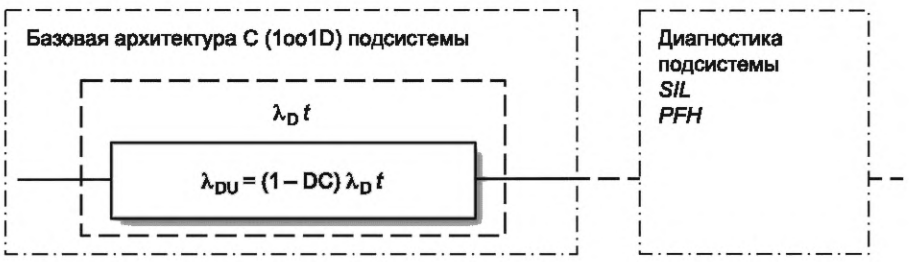


Рисунок H.7 — Блок-схема надежности базовой архитектуры C (1oo1D) подсистемы с инициированием безопасного состояния с использованием другой подсистемы

Интенсивность опасных отказов для канала определяется выражением $\lambda_D = \lambda_{DU}$, поскольку обнаружение любого опасного отказа функции безопасности приведет к безопасному состоянию.

Неготовность равна $P_D(t) = P_{DU}(t)$. $P_{DU}(t)$ представлена на рисунке H.8.

На основании формулы (H.2) для PFH получают:

$$\mathrm{PFH} = \frac{1}{T}\int_0^T \lambda_{DU}\,\mathrm{d}t = \frac{1}{T}\lambda_{DU}\left[t\right]\Big|_0^T = \lambda_{DU} = (1-\mathrm{DC})\lambda_D. \quad \text{(H.22)}$$

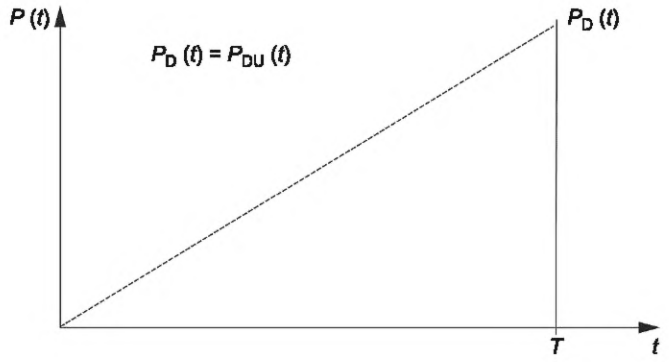


Рисунок Н.8 — Функции неготовности базовой архитектуры С (1oo1D) подсистемы

Н.10.3 Реакция на сбой, который следует учитывать в подсистеме

Эта архитектура состоит из одного канала, где любой необнаруженный опасный отказ приводит к отказу функции безопасности при возникновении запроса, а обнаруженные опасные отказы приводят к реакции на сбой, при котором функция безопасности инициирует безопасное состояние.

Таким образом, инициирование безопасного состояния функцией безопасности зависит от обнаруженных диагностикой опасных отказов λ_{DD} и отказов канала при его реакции на сбой λ_{react}.

Пример — Контактор с λ_D отключается, чтобы остановить опасное движение. Контролируя зеркальные контакты этого контактора, можно отключить другой исполнительный механизм (λ_{react}) (например, автоматический выключатель) в случае обнаружения опасного отказа контактора.

Логическое представление показано на рисунке Н.9.

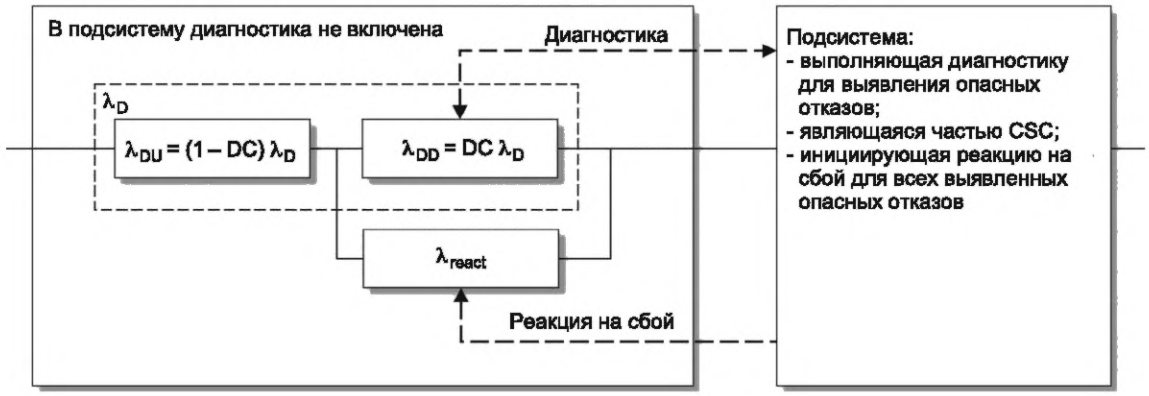


Рисунок Н.9 — Логическое представление базовой архитектуры С (1oo1D) подсистемы с реакцией на сбой

На рисунке Н.10 показана блок-схема надежности в момент *t*.

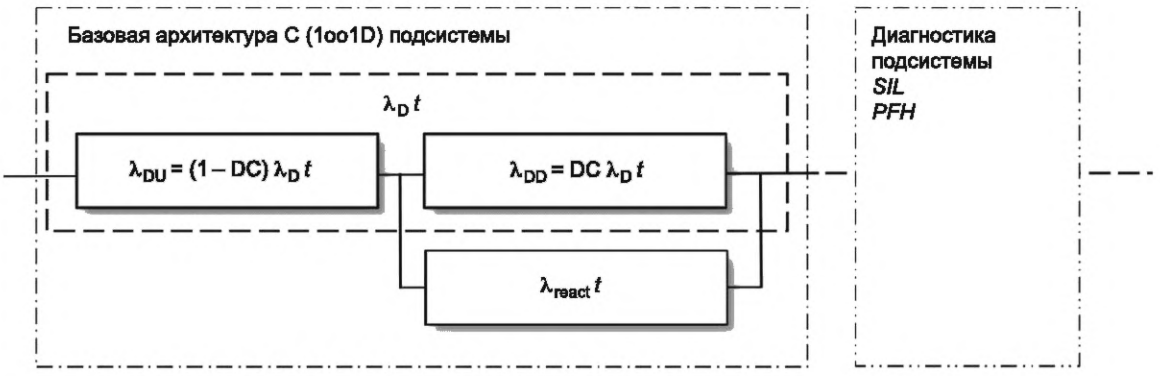


Рисунок Н.10 — Блок-схема надежности базовой архитектуры С (1oo1D) подсистемы с реакцией на сбой

Значение неготовности можно определить как $P_D(t) = P_{DU}(t) + P_{Diag}(t) = P_{DU}(t) + P_{DD}(t)\ P_{react}(t)$, где неготовность P_{Diag} представлена двумя параллельно соединенными каналами, частью функционального канала λ_{DD} и канала реакции на сбой λ_{react}.

$P_{DU}(t)$, $P_{DD}(t)$ и $P_{react}(t)$ представлены на рисунке Н.11.

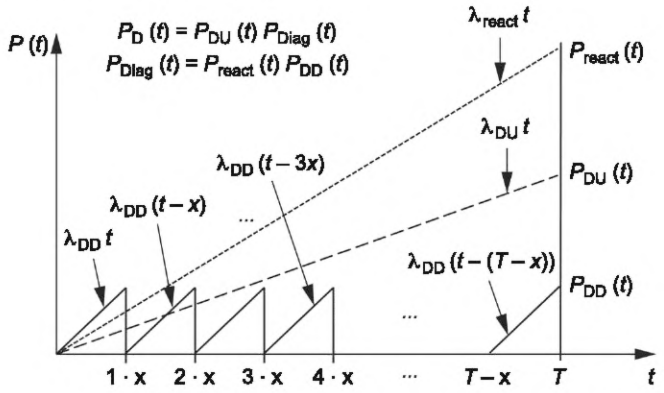


Рисунок Н.11 — Функции неготовности базовой архитектуры С (1oo1D) подсистемы

Величина «x» представляет интервал испытаний (или интервал диагностических проверок T_2) и $x << T$ (или срока службы T_1) и принимается, что $T = n\ x$.

Значение PFH_{DU} вычисляется по формуле (Н.22): $PFH_{DU} = \lambda_{DU} = (1 - DC)\ \lambda_D$.

Возможна следующая декомпозиция PFH_{Diag}:

$$PFH_{Diag} = \frac{1}{T}\int_0^T P'_{Diag}(t)\,dt$$

$$PFH_{Diag} = \frac{1}{T}\left(\int_0^x P'_{Diag}(t)\,dt + \int_x^{2x} P'_{Diag}(t)\,dt + \int_{2x}^{3x} P'_{Diag}(t)\,dt + \ldots + \int_{T-x}^{T} P'_{Diag}(t)\,dt\right). \quad (Н.23)$$

$$PFH_{Diag} = \frac{1}{T}\sum_{K=1(K-1)x}^{n}\int^{Kx} P'_{Diag}(t)\,dt,$$

где $P_{Diag}(t) = P_{DD}(t)\ P_{react}(t)$ и $P'_{Diag}(t)$ в течение общего периода $\Delta t = K - 1$, K становится равной $P'_{Diag}(t) = \lambda_{DD}\ \lambda_{react}\ [2t - (K - 1)\ x]$.

Если предположить, что $(\lambda t) << 1$, то можно использовать следующие упрощенные формулы:

- $P_{react}(t) \approx (\lambda_{react}\ t)$ в течение периода $[0,\ T]$;
- $P_{DD}(t) \approx (\lambda_{DD}\ t)$ за период $\Delta t = x$ ($[0,x]$, $[x,2x]$, $[2x,3x]$, …$[T\text{-}x,\ T]$).

Примечание — Для периодов Δt, приближающихся к T, предположение λt обеспечит более высокие результаты, чем $(1 - e^{-\lambda t})$.

Пример — Для Δt = 10 ч [10 000, 10 010] и λ = 3,81 E-06 (30 лет), λt = 3,81 E-05, но $(1 - e^{-\lambda 10\ 010}) - (1 - e^{-\lambda 10\ 000}) = 3{,}66$ E-05. В этом случае λt имеет результаты на 4 % выше, чем при детальном подходе $(1 - e^{-\lambda t})$, при λ = 1,14 E-05 (10 лет) λt на 12 % выше.

Формула (Н.23) принимает вид:

$$PFH_{Diag} = \lambda_{DD}\lambda_{react}\frac{(T_1 + T_2)}{2}. \quad (Н.24)$$

Н.10.4 PFH

Сложив слагаемые в формулах (Н.22) и (Н.24), получают:

$$PFH = (1 - DC)\lambda_D + \lambda_{DD}\lambda_{react}\frac{(T_1 + T_2)}{2}. \quad (Н.25)$$

Н.10.5 Влияние CCF

Формула (Н.25) в этом случае принимает вид:

$$PFH = (1 - DC)\lambda_D^{CC} + DC\lambda_D^{CC}\lambda_{react}^{CC}\frac{(T_1 + T_2)}{2} + \lambda_{CC}, \quad (Н.26)$$

где $\lambda_{CC} = \beta$ мин. (λ_D, λ_{react}), $\lambda_D^{CC} = \lambda_D - \lambda_{CC}$, $\lambda_{react}^{CC} = \lambda_{react} - \lambda_{CC}$, T_1 представляет собой срок службы, λ_D — интенсивность отказов канала, λ_{react} — интенсивность отказов функции, реагирующей на сбой, DC — охват диагностикой канала, а T_2 — интервал диагностических проверок с $T_2 << T_1$.

Наихудший случай следует рассматривать при β мин. (λ_D, λ_{react}) = $\beta\,\lambda_D$, поскольку значение λ_{react} на практике будет ниже, чем λ_D.

$$PFH = (1-\beta)(1-DC)\lambda_D + (1-\beta)DC\lambda_D(\lambda_{react} - \beta\lambda_D)\frac{(T_1+T_2)}{2} + \beta\lambda_D. \quad (H.27)$$

Когда значение λ_{react} на практике будет ниже или равно λ_D, формула (H.27) с $\lambda_{react} = \lambda_D$ будет иметь вид:

$$PFH = (1-\beta)(1-DC)\lambda_D + (1-\beta)^2 DC\lambda_D^2\frac{(T_1+T_2)}{2} + \beta\lambda_D. \quad (H.28)$$

H.11 Базовая архитектура B (1oo2) подсистемы

H.11.1 Общие положения

Данная архитектура состоит из двух каналов, соединенных параллельно, так что каждый канал может выполнять функцию безопасности. Одиночный отказ канала не приведет к потере функции безопасности. Диагностики, позволяющей обнаружить какой-либо опасный сбой в обоих каналах, не существует. При возникновении опасного отказа в обоих каналах функция безопасности не сработает при возникновении запроса.

На рисунке H.12 показана блок-схема надежности в момент *t*.



Рисунок H.12 — Блок-схема надежности базовой архитектуры B (1oo2) подсистемы

Интенсивность опасных отказов определяется значениями λ_{D1} и λ_{D2}.

Неготовность равна $P_D(t) = P_{D1}(t)\,P_{D2}(t)$.

$P_{D1}(t)$ и $P_{D2}(t)$ представлены на рисунке H.13.

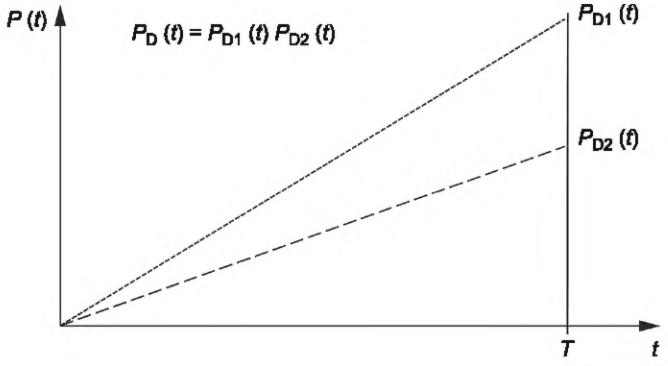


Рисунок H.13 — Функции неготовности базовой архитектуры B (1oo2) подсистемы

H.11.2 PFH

Если предположить, что (λt) << 1 в течение периода [0, *T*], то можно использовать следующие упрощенные формулы: $P_{D1}(t) \approx \lambda_{D1} t$ и $P_{D2}(t) \approx \lambda_{D2} t$ и $P_D(t) \approx \lambda_{D1}\,\lambda_{D2}\,t^2$.

$PFH = \frac{1}{T}\int_0^T P'_D(t)\,dt$ с $P'_D(t) \approx 2\,\lambda_{D1}\,\lambda_{D2}$ будет иметь вид:

$$PFH = \frac{1}{T}\ \lambda_{D1}\lambda_{D2}T^2 = \lambda_{D1}\ \lambda_{D2}T. \quad (H.29)$$

Кроме того, формулу (H.29) можно записать как

$$PFH = PFH_{D1}\ PFH_{D2}\ T, \quad (H.30)$$

где $PFH_{D1} = \lambda_{D1}$ и $PFH_{D2} = \lambda_{D2}$.

H.11.3 Влияние CCF

Формула (H.29) в этом случае принимает вид:

$$PFH = \lambda_{D1}^{CC}\lambda_{D2}^{CC}T_1 + \beta\lambda_{CC}, \quad (H.31)$$

где $\lambda_{CC} = \beta$ мин. (λ_{D1}, λ_{D2}), $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$, $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$, T_1 — представляет собой срок службы, λ_{D1} и λ_{D2} — интенсивность отказов каналов 1 и 2.

Если $\lambda_D = \lambda_{D1} = \lambda_{D2}$, то формула (H.31) принимает вид:

$$PFH = (1-\beta)^2\ \lambda_D\ T_1 + \beta\ \lambda_D. \quad (H.32)$$

H.12 Базовая архитектура D (1oo2D) подсистемы

H.12.1 Общие положения

Эта архитектура состоит из двух каналов, соединенных параллельно, так что каждый канал может выполнять функцию безопасности. Одиночный отказ канала не приведет к отказу функции безопасности. Для выявления опасного отказа в обоих каналах имеется диагностика. При обнаружении опасного отказа в любом канале функция безопасности инициирует безопасное состояние. На рисунке H.14 показана блок-схема надежности в момент *t*.

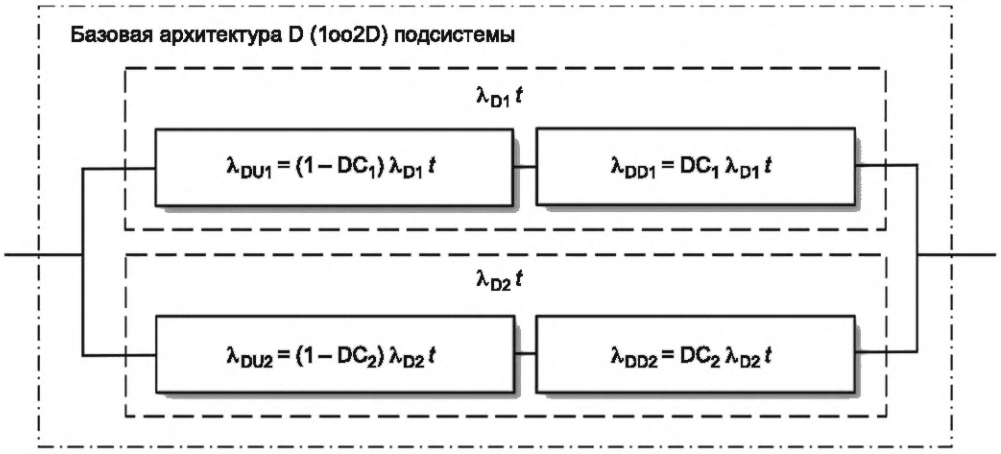


Рисунок H.14 — Блок-схема надежности базовой архитектуры D (1oo2D) подсистемы

Интенсивность опасных отказов определяется формулами $\lambda_{D1} = \lambda_{DU1} + \lambda_{DD1}$ и $\lambda_{D2} = \lambda_{DU2} + \lambda_{DD2}$.
Неготовность равна $P_D(t) = P_{D1}(t)\ P_{D2}(t) = (P_{DU1}(t) + P_{DD1}(t))\ (P_{DU2}(t) + P_{DD2}(t))$.
$P_{DU1}(t)$, $P_{DD1}(t)$, $P_{DU2}(t)$ и $P_{DD2}(t)$ представлены на рисунке H.15.

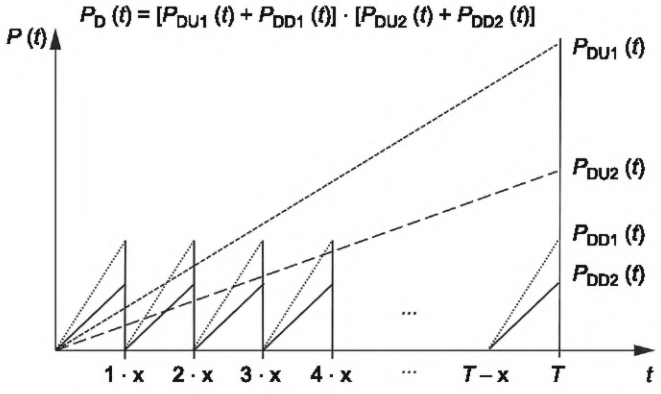


Рисунок H.15 — Функции неготовности базовой архитектуры подсистемы D (1oo2D)

Величина «x» представляет интервал испытаний (или интервал диагностических проверок T_2) и $x << T$ (или срока службы T_1), принимается, что $T = n\,x$. В результате получают:

$$\text{PFH} = \frac{1}{T}\int_0^T P'_D(t)\,\text{dt} = \frac{1}{T}\left(\int_0^x P'_D(t)\,\text{dt} + \int_x^{2x} P'_D(t)\,dt + \int_{2x}^{3x} P'_D(t)\,\text{dt} + \ldots + \int_{T-x}^{T} P'_D(t)\,\text{dt}\right).$$

Если предположить, что $(\lambda t) << 1$, то можно использовать следующие упрощенные формулы:

- $P_{DU1}(t) \approx \lambda_{DU1}\,t$, $P_{DU2}(t) \approx \lambda_{DU2}\,t$ в течение периода $[0,\ T]$;
- $P_{DD1}(t) \approx \lambda_{DD1}\,t$, $P_{DD2}(t) \approx \lambda_{DD2}\,t$ за период $\Delta t = x$ ($[0,x]$, $[x,2x]$, $[2x,3x]$, …$[T\text{-}x,\ T]$).

$$P_D(t) = P_{DD1}(t)\,P_{DD2}(t) + P_{DU1}(t)\,P_{DU2}(t) + P_{DU1}(t)\,P_{DD2}(t) + P_{DD1}(t)\,P_{DU2}(t).$$

Слагаемое A Слагаемое B Слагаемое C Слагаемое D

H.12.2 Оценка PFH слагаемого A

В целом PFH определяется как

$$\text{PFH} = \frac{1}{T}\int_0^T P'_D(t)\,\text{dt} = \frac{1}{T}\left(\int_0^x P'_D(t)\,\text{dt} + \int_x^{2x} P'_D(t)\,\text{dt} + \int_{2x}^{3x} P'_D(t)\,\text{dt} + \ldots + \int_{T-x}^{T} P'_D(t)\,\text{dt}\right).$$

Число периодов Δt равно T/x.

Для каждого периода $\Delta t = x$ ($[0,\ x]$, $[x,\ 2x]$, $[2x,\ 3x]$, …$[T - x,\ T]$) произведение $P_{DD1}(t)\,P_{DD2}(t)$ будет одинаковым и, следовательно, PFH можно записать следующим образом:

$$\text{PFH} = \frac{1}{T}\int_0^T P'(t)\,\text{dt} = \frac{1}{x}\int_0^x P'(t)\,\text{dt} = \frac{1}{x}\lambda_{DD1}\lambda_{DD2}x^2 = \lambda_{DD1}\lambda_{DD2}x \qquad \text{(H.33)}$$

или

$$\text{PFH} = \lambda_{DD1}\,\lambda_{DD2}\,T_2, \qquad \text{(H.34)}$$

где $P(t) = P_{DD1}(t)\,P_{DD2}(t) = \lambda_{DD1}\,\lambda_{DD2}\,t^2$ и $P'(t) = 2\,\lambda_{DD1}\,\lambda_{DD2}\,t$.

H.12.3 Оценка PFH слагаемого B

В течение периода $[0,\ T]$ $P_{DU1}(t) \approx \lambda_{DU1}\,t$, $P_{DU2}(t) \approx \lambda_{DU2}\,t$, $P'_{DU1}(t)\,P'_{DU2}(t) \approx 2\,\lambda_{DU1}\,\lambda_{DU2}\,t$ и формулу для PFH можно записать в виде:

$$\text{PFH} = \frac{1}{T}\int_0^T 2\lambda_{DU1}\lambda_{DU2}t\,\text{dt} \approx \lambda_{DU1}\lambda_{DU2}T \qquad \text{(H.35)}$$

или

$$\text{PFH} \approx (1 - \text{DC}_1)\,\lambda_{D1}\,(1 - \text{DC}_2)\,\lambda_{D2}\,T_1. \qquad \text{(H.36)}$$

H.12.4 Оценка PFH слагаемого C и слагаемого D

Формулу для PFH можно записать следующим образом [на основе формулы (H.24)]:

$$\text{PFH} = \lambda_{DU1}\lambda_{DD2}\frac{(T+x)}{2} + \lambda_{DU2}\lambda_{DD1}\frac{(T+x)}{2} \qquad \text{(H.37)}$$

или

$$\text{PFH} = \left[(1-\text{DC}_1)\lambda_{D1}\text{DC}_2\lambda_{D2} + (1-\text{DC}_2)\lambda_{D2}\text{DC}_1\lambda_{D1}\right]\left(\frac{T_1+T_2}{2}\right). \qquad \text{(H.38)}$$

H.12.5 PFH

Просуммировав члены в формулах (H.34), (H.36) и (H.38), получают:

$$\text{PFH} = \frac{\lambda_{D1}\lambda_{D2}}{2}\left[T_1\left(2-\text{DC}_1-\text{DC}_2\right) + T_2\left(\text{DC}_1+\text{DC}_2\right)\right]. \qquad \text{(H.39)}$$

H.12.6 Влияние CCF

Формула (H.39) в этом случае принимает вид:

$$\text{PFH} = \lambda_{D1}^{CC}\lambda_{D2}^{CC}\left(2-\text{DC}_1-\text{DC}_2\right)\frac{T_1}{2} + \lambda_{D1}^{CC}\lambda_{D2}^{CC}\left(\text{DC}_1+\text{DC}_2\right)\frac{T_2}{2} + \lambda_{CC}, \qquad \text{(H.40)}$$

где $\lambda_{CC} = \beta$ мин. $(\lambda_{D1},\ \lambda_{D2})$, $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$, $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$, T_1 — представляет собой срок службы, λ_{D1} и λ_{D2} — интенсивность отказов каналов 1 и 2, DC_1 и DC_2 — охват диагностикой каналов 1 и 2, T_2 — интервал диагностических проверок с $T_2 << T_1$.

Если $\lambda = \lambda_{D1} = \lambda_{D2}$ и $\text{DC} = \text{DC}_1 = \text{DC}_2$, то формула (H.40) принимает вид:

$$\text{PFH} = (1-\beta)^2\,\lambda_D^2\,(1-\text{DC})T_1 + (1-\beta)^2\,\lambda_D^2\,\text{DC}T_2 + \beta\,\lambda_D. \qquad \text{(H.41)}$$

Н.13 Базовая архитектура D (1oo2D) подсистемы с учетом двух периодов времени

Н.13.1 Общие положения

Для неэлектронных компонентов срок службы определяется как T_{10D} — среднее время, в течение которого 10 % компонентов выходят из строя. В зависимости от среднего количества операций компонента в год расчетное значение T_{10D} может оказаться меньше полезного времени (срока годности) T_1, указанного для подсистемы, поэтому срок службы будет ограничен T_{10D}. Может случиться так, что в архитектуре 1oo2D, в зависимости от конкретного приложения, компоненты в двух каналах имеют разные значения T_{10D} и, следовательно, два канала будут иметь два разных значения срока службы (названные ниже T_{1o1} и T_{1o2}) .

Пример — Один канал состоит из главного контактора, который отключается при нормальной работе машины и когда происходит запрос к функции безопасности. Второй канал состоит из главного контактора, который отключается только тогда, когда происходит запрос к функции безопасности.

Блок-схема надежности такая же, как в Н.12.1.

Неготовность равна $P_D(t) = P_{D1}(t)\,P_{D2}(t) = (P_{DU1}(t) + P_{DD1}(t))\,(P_{DU2}(t) + P_{DD2}(t))$ и

$$\mathrm{PFH} = \frac{1}{T}\int_0^T P'_D(t)\,\mathrm{d}t + \frac{1}{T}\left(\int_0^x P'_D(t)\,\mathrm{d}t + \int_x^{2x} P'_D(t)\,\mathrm{d}t + \int_{2x}^{3x} P'_D(t)\,\mathrm{d}t + \ldots + \int_{T-x}^{T} P'_D(t)\,\mathrm{d}t\right).$$

Если предположить, что $(\lambda t) << 1$, то можно использовать следующие упрощенные формулы:

- $P_{DU1}(t) \approx \lambda_{DU1}\,t$ в течение периода $[0,\ T_{1o1}]$; $P_{DU2}(t) \approx \lambda_{DU2}\,t$ в течение периода $[0,\ T_{1o2}]$;
- $P_{DD1}(t) \approx \lambda_{DD1}\,t$, $P_{DD2}(t) \approx \lambda_{DD2}\,t$ за период $\Delta t = x$ ($[0,\ x]$, $[x,\ 2x]$, $[2x,\ 3x]$, …$[T - x,\ T]$).

$$P_D(t) = \underbrace{P_{DD1}(t)\,P_{DD2}(t)}_{\text{Слагаемое A}} + \underbrace{P_{DU1}(t)\,P_{DU2}(t)}_{\text{Слагаемое B}} + \underbrace{P_{DU1}(t)\,P_{DD2}(t)}_{\text{Слагаемое C}} + \underbrace{P_{DD1}(t)\,P_{DU2}(t)}_{\text{Слагаемое D}}. \qquad (\text{Н.42})$$

Периоды времени рассмотрения: T_{1o1} для канала 1 и T_{1o2} для канала 2.

Н.13.2 Оценка PFH слагаемого A

В целом, PFH определяется как

$$\mathrm{PFH} = \frac{1}{T}\int_0^T P'_D(t)\,\mathrm{d}t = \frac{1}{T}\left(\int_0^x P'_D(t)\,\mathrm{d}t + \int_x^{2x} P'_D(t)\,\mathrm{d}t + \int_{2x}^{3x} P'_D(t)\,\mathrm{d}t + \ldots + \int_{T-x}^{T} P'_D(t)\,\mathrm{d}t\right).$$

Количество периодов Δt соответственно равно $\left(\frac{T_{1o1}}{x}\right)$ и $\left(\frac{T_{1o2}}{x}\right)$ и PFH становится:

$$\mathrm{PFH} = \frac{1}{x}\lambda_{DD1}\lambda_{DD2}x^2 = \mathrm{DC}_1\lambda_{D1}\mathrm{DC}_2\lambda_{D2}x \qquad (\text{Н.43})$$

или

$$\mathrm{PFH} = \lambda_{DD1}\,\lambda_{DD2}\,T_2, \qquad (\text{Н.44})$$

где $P(t) = P_{DD1}(t)\,P_{DD2}(t) = \lambda_{DD1}\,\lambda_{DD2}\,t^2$ и $P'(t) = 2\,\lambda_{DD1}\,\lambda_{DD2}\,t$.

Н.13.3 Оценка PFH слагаемого B

Для периода $[0,\ T]$, $P_{DU1}(t) \approx \lambda_{DU1}\,t$, $P_{DU2}(t) \approx \lambda_{DU2}\,t$ формулу PFH можно записать как

$$\mathrm{PFH} = (1-\mathrm{DC}_1)\lambda_{D1}(1-\mathrm{DC}_2)\lambda_{D2}\left(\frac{T_{1o1}+T_{1o2}}{2}\right). \qquad (\text{Н.45})$$

Н.13.4 Оценка PFH слагаемого C и слагаемого D

Формулу для PFH можно записать как

$$\mathrm{PFH} = \lambda_{DU1}\lambda_{DD2}\left(\frac{T_{1o1}+x}{2}\right) + \lambda_{DU2}\lambda_{DD1}\left(\frac{T_{1o2}+x}{2}\right) \qquad (\text{Н.46})$$

или

$$\mathrm{PFH} = \lambda_{D1}\lambda_{D2}\left[(1-\mathrm{DC}_1)\mathrm{DC}_2\left(\frac{T_{1o1}+T_2}{2}\right) + (1-\mathrm{DC}_2)\mathrm{DC}_1\left(\frac{T_{1o2}+T_2}{2}\right)\right]. \qquad (\text{Н.47})$$

Н.13.5 PFH

Просуммировав члены в формулах (Н.44), (Н.45) и (Н.47), получают:

$$\mathrm{PFH} = \frac{\lambda_{D1}\lambda_{D2}}{2}\left[T_{1o1}(1-\mathrm{DC}_1) + T_{1o2}(1-\mathrm{DC}_2) + T_2(\mathrm{DC}_1+\mathrm{DC}_2)\right]. \qquad (\text{Н.48})$$

Н.13.6 Влияние CCF

Формула (Н.45) в этом случае принимает вид:

$$PFH = \lambda_{D1}^{CC}\lambda_{D2}^{CC}(1-DC_1)\frac{T_{1o1}}{2} + \lambda_{D1}^{CC}\lambda_{D2}^{CC}(1-DC_2)\frac{T_{1o2}}{2} + \lambda_{D1}^{CC}\lambda_{D2}^{CC}(DC_1+DC_2)\frac{T_2}{2} + \lambda_{CC}, \quad (Н.49)$$

где $\lambda_{CC} = \beta$ мин. (λ_{D1}, λ_{D2}), $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$, $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$, T_{1o1} и T_{1o2} представляют собой срок службы канала 1 и канала 2, λ_{D1} и λ_{D2} — интенсивность отказов каналов 1 и 2, DC_1 и DC_2 — охват диагностикой каналов 1 и 2 и T_2 — интервал диагностических проверок.

Приложение I
(справочное)

Примеры действующих норм с комментариями

I.1 Общие положения

Требования безопасности к машинному оборудованию существуют во всем мире. Метод регулирования или законодательные акты зависят от местных регламентов. Международные стандарты МЭК и ИСО полностью или частично могут быть включены в такие местные регламенты посредством ссылки. Принципиальные подходы перечислены в настоящем приложении только в иллюстративных целях. Следующие примеры приведены в информационных целях и не представляют собой исчерпывающий список. Любые комментарии к ним являются исключительно дополнительной информацией и не будут считаться официальными.

I.2 Европейский Союз

I.2.1 Общее европейское законодательство

Примечание — Дополнительная информация доступна по адресу: gost.e-ecolog.ru
mechanical-engineering/machinery/.

Использование машины регулируется требованиями Директивы 2009/104/ЕС Европейского парламента и Совета от 16 сентября 2009 г., касающейся минимальных требований безопасности и гигиены труда при использовании рабочего оборудования работниками на работе (вторая отдельная Директива в значении статьи 16(1) Директивы 89/391/ЕЕС), которая заменяет Директиву 89/655/СЕЕ.

Для сектора новых машин применимым официальным текстом является Директива по машинному оборудованию:

- Директива 2006/42/ЕС Европейского парламента и Совета от 17 мая 2006 г. о машинном оборудовании, вносящая поправки в Директиву 95/16/ЕС (переработанную), которая заменяет Директиву о машинном оборудовании 98/37/ЕС;
- Директива по машинному оборудованию 98/37/ЕС Европейского парламента и Совета от 22 июня 1998 г., которая вступила в силу 29 декабря 2009 г. и заменила Директиву по машинному оборудованию 89/392/ЕЕС;
- Директива Совета 89/392/ЕЕС от 14 июня 1989 г.

I.2.2 Новые предлагаемые правила в отношении машинного оборудования (в стадии подготовки)

В настоящее время разрабатывается новый регламент по машинному оборудованию, который заменит действующую Директиву по машинному оборудованию.

Этот пересмотр был основан на том, что если текст директивы в целом был «актуальным, эффективным, действенным и последовательным», то в нем подчеркивалась необходимость усовершенствований, упрощений и необходимость заполнения ряда пробелов.

Целью этого регулирования[1)] является устранение недостатков и содействие как цифровому переходу, так и укреплению единого рынка. Кроме того, новый регламент по машинному оборудованию будет реагировать на потребности рынка, внося большую юридическую ясность в действующие положения, упрощая административные барьеры и затраты для компаний, позволяя использовать цифровые форматы для документации и адаптируя сборы за оценку соответствия для МСП, обеспечивая при этом согласованность с законодательной базой ЕС по изделиям.

Общие цели Директивы по машинному оборудованию заключаются в том, чтобы обеспечить не только свободное перемещение машинного оборудования на внутреннем рынке, но и высокий уровень защиты пользователей и других лиц, подвергающихся риску.

Документы представлены на веб-сайте Европы[2)], доступно несколько документов:

- Предложение по Регламенту Европейского Парламента и Совета по машиностроительной продукции;
- Приложение к предложению по постановлению Европейского парламента и Совета по машиностроительной продукции;
- Оценка влияния;
- Общая пояснительная записка к оценке влияния.

I.2.3 Соответствующее законодательство

Одним из основных законодательных актов, регулирующих гармонизацию основных требований по охране труда и технике безопасности для машин на уровне ЕС, является Директива по машинному оборудованию 2006/42/ЕС.

---

1) Новое Положение о машинном оборудовании призвано обеспечить, чтобы новое поколение машин гарантировало безопасность пользователей и потребителей и поощряло инновации. Хотя Постановление об искусственном интеллекте предназначено для устранения рисков безопасности, связанных с системами искусственного интеллекта, новое Положение о машинном оборудовании призвано обеспечить безопасную интеграцию системы искусственного интеллекта в общее оборудование. Предприятиям необходимо будет провести только одну оценку соответствия. gost.e-ecolog.ru

2) gost.e-ecolog.ru

Директива по машинному оборудованию:

- способствует свободному перемещению машинного оборудования на едином рынке;
- гарантирует высокий уровень защиты работников и граждан ЕС.

Поскольку это директива «нового подхода», она способствует гармонизации посредством сочетания обязательных требований по охране труда и технике безопасности и добровольных гармонизированных стандартов. Директива по машинному оборудованию применяется только к изделиям, которые впервые поставляются на рынок ЕС.

Директива по машинному оборудованию 2006/42/ЕС была опубликована 9 июня 2006 г. и вступила в силу 29 декабря 2009 г. В нее были внесены поправки Директивой 2009/127/ЕС Европейского парламента и Совета от 21 октября 2009 г. в отношении машинного оборудования для применения пестицидов, а также Регламент (ЕС) № 167/2013 Европейского парламента и Совета от 5 февраля 2013 г. об одобрении и надзоре за рынком сельскохозяйственной и лесохозяйственной техники.

Примечание — Законодательство ЕС, которое может применяться к машинному оборудованию в дополнение к Директиве по машинному оборудованию, в отношении опасностей, которые они охватывают более конкретно, чем Директива по машинному оборудованию, например:

- Директива 2014/34/EU49 по оборудованию и системам защиты, предназначенным для использования в потенциально взрывоопасных средах (Директива ATEX);
- Директива 2014/68/EU59 по оборудованию, работающему под давлением (PED);
- Директива 2014/53/EU65 по радиооборудованию (RED);
- Директива 2000/14/EC67 с поправками, внесенными Директивой 2005/88/EC68 о шумовом излучении в окружающую среду оборудованием, используемым вне помещений (OND);
- Директива 2014/30/EU73 по электромагнитной совместимости (EMCD).

I.2.4 Обязанности изготовителей машины

Согласно Директиве по машинному оборудованию, задачи изготовителя заключаются в следующем:

- провести оценку рисков, чтобы определить, какие требования по охране труда и технике безопасности применяются к их оборудованию;
- учитывать оценку риска при проектировании и производстве своего машинного оборудования;
- определить, какие ограничения существуют на использование машинного оборудования;
- выявить любые возможные опасности;
- оценить риск того, что их машинное оборудование может привести к серьезным травмам или повреждению, и принять меры для повышения безопасности своего оборудования;
- убедиться, что их машинное оборудование соответствует основным требованиям по охране труда и технике безопасности, перечисленным в приложении I к Директиве по машинному оборудованию;
- предоставить технический документ, подтверждающий, что машинное оборудование соответствует требованиям Директивы по машинному оборудованию;
- убедиться, что они применяют процедуры оценки соответствия и предоставляют всю необходимую информацию, включая инструкции по сборке и использованию;
- убедиться, что они заполнили декларацию соответствия ЕС и что на машинное оборудование нанесена маркировка соответствия CE, чтобы его можно было использовать в любой точке ЕС.

I.3 Северная Америка — США

Примечание — Соответствующие интернет-ссылки:

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

Примеры соответствующего законодательства и стандартов приведены в следующих документах:

- Безопасность машин: Кодекс федеральных правил (CFR), раздел 29; Часть 1910 г. (подчасть O — Машины и защита машин);
- Электробезопасность: Кодекс федеральных правил (CFR), раздел 29; Часть 1910 г. (подраздел S-Электрическое);
- NFPA 79, стандарт на электрооборудование машин и механизмов, соответствующий МЭК 60204-1;
- UL 508A, стандарт на электрооборудование для промышленных панелей управления;
- ANSI B11.0 (безопасность машин), ANSI B11.19 (требования к эффективности мер по снижению риска: защита и другие средства снижения риска) и ANSI B11.26 (требования к эффективности мер по снижению риска: меры безопасности и другие средства снижения риска).

I.4 Северная Америка — Канада

Примечание —Соответствующие интернет-ссылки:

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

Примеры соответствующего законодательства и стандартов приведены в следующих документах:

- Закон Канады о безопасности потребительских товаров;
- Безопасность продукции, O Reg 438/07;
- C22.1-18: Канадские электротехнические правила, часть I.
- CSA C22.2 № 0 — Общие требования, Электротехнические нормы и правила Канады, часть II и CSA C22.2 № 301 «Промышленное электрооборудование»; SU 2011 Оборудование для автоматизации производства и промышленное оборудование NFPA 79.

I.5 Южная Америка — Бразилия

Пример соответствующего законодательства приведен в следующем документе:

Положение об оборудовании и машинах № 12 (Безопасность работы с машинами и оборудованием).

I.6 Китай

Пример соответствующего стандарта:

- МЭК 62061:2005 был преобразован в стандарт национальной безопасности Китая GB 28526-2012, опубликован и внедрен в 2012 году.

I.7 Япония

Примерами соответствующего законодательства являются:

- закон о промышленной безопасности и гигиене труда определяет роль работодателя в расследовании опасности или нанесении вреда и т. д., причиняемых зданиями, сооружениями (машинами, электроустановками), сырьем, газами, парами, пылью и т. д., а также тем, что появляется в результате производственных действий, и другие обязательства, а также меры по предотвращению опасностей или ухудшения здоровья работников.

Ссылки в Интернете:

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

- закон об электронном бизнесе дает определение «электрооборудованию».

Примечание — «Электрооборудование» подразделяются на категории «для коммерческого использования», «для общего использования», «для частного использования» и т. д.

Ссылка в Интернете: gost.e-ecolog.ru .

Приложение J
(справочное)

Комбинация режимов работы

J.1 Общие положения

Система управления технологическим оборудованием может использоваться для обеспечения безопасности людей, имущества и окружающей среды.

Эта система управления является частью так называемых функций безопасности приборных систем безопасности (SIF) согласно МЭК 61511, где учитываются требования безопасности и меры защиты. Частота запросов к SIF часто рассматривается в контексте режима работы с низким частотой запросов (менее или равного одному разу в год).

Примечание — См. МЭК 61511-1 для получения информации об приборных функциях безопасности (SIF).

Тем не менее, в такого рода приложениях можно использовать машины с функциями безопасности, работающими в режиме с высокой частотой запросов или с непрерывными запросами.

В J.2 представлен базовый подход к режиму работы с высокой частотой запросов (см. МЭК 61508 и МЭК 62061) и режиму работы с низкой частотой запросов (см. МЭК 61508 и МЭК 61511).

В J.3 даны рекомендации по проектированию SIF путем объединения подсистем, предназначенных для режима работы с низкой частотой запросов, и подсистем, разработанных для режима работы с высокой частотой запросов.

J.2 Основные подходы к различным режимам работы

J.2.1 Общие сведения

Принципиально подходы к режиму работы с высокой частотой запросов или с непрерывными запросами и режиму работы с низкой частотой запросов аналогичны и основаны на декомпозиции функции безопасности или функции безопасности приборной систем безопасности (SIF) на подсистемы, где отказ подсистемы приводит к отказу соответствующей функции, см. рисунок J.1 и рисунок J.2.

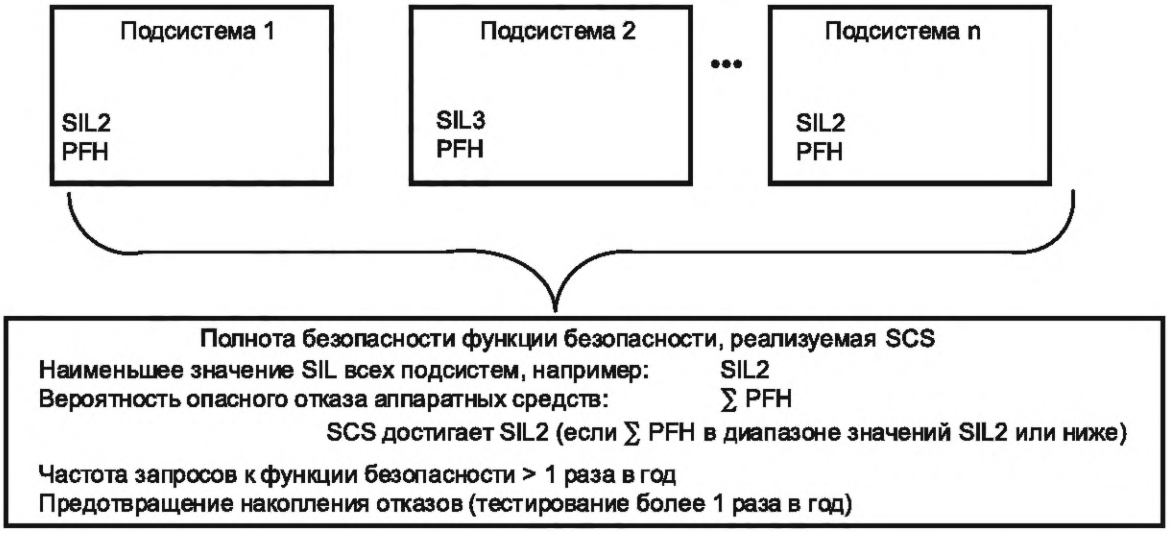


Рисунок J.1 — Базовый подход для режима работы с высокой частотой запросов или с непрерывными запросами на основе МЭК 61508 (и МЭК 62061)

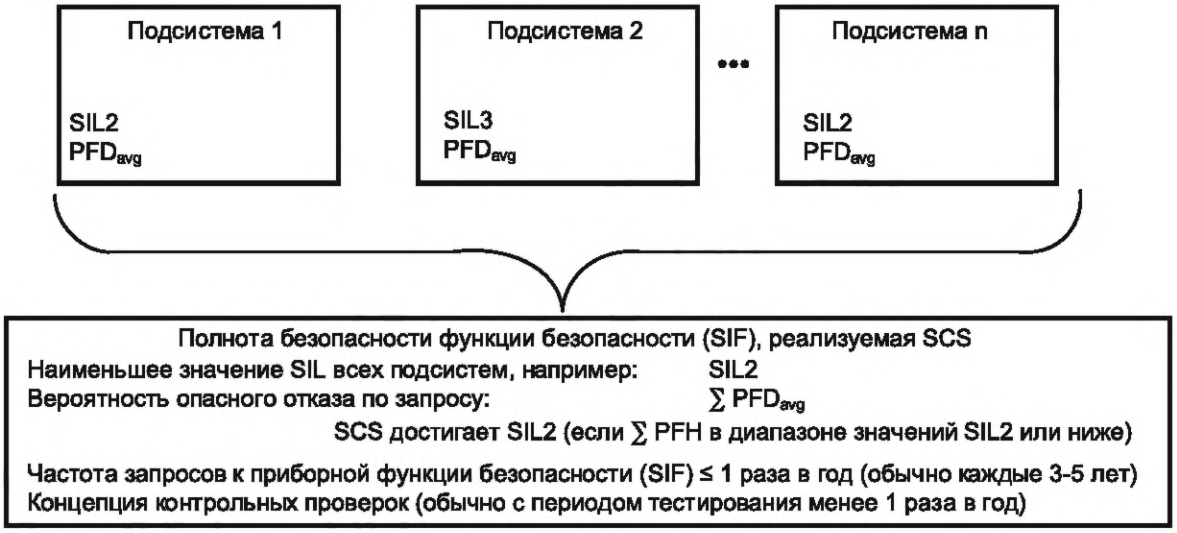


Рисунок J.2 — Базовый подход в режиме работы с низкой частотой запросов на основе МЭК 61508 (и МЭК 61511)

J.2.2 Меры по снижению риска в режиме работы с низкой частотой запросов

В контексте функций безопасности приборных систем безопасности (SIF) согласно МЭК 61511 (см. также 5.3) и режима работы с низкой частотой запросов важны следующие основные аспекты:

- реализованные SIF в основном предназначены для защиты процесса, а затем людей;
- операторы имеют подробную информацию о проекте SIF, системы управления и самого управления технологическим процессом;
- можно использовать несколько слоев защиты, и в этом случае такой подход учитывает использование и оценку базовой системы управления процессом (BPCS), выполняющей управление процессом.

Примечание 1 — Хотя в режиме работы с низкой частотой запросов можно использовать уровень защиты, но при проектировании и оценке функций безопасности в режиме работы с высокой частотой запросов уровни защиты не рассматриваются. При этом на требуемое значение SIL система управления машиной или квалификация оператора не влияет;

- частота запросов к SIF может быть низкой и, как ожидается, будет находиться в интервале продолжительностью более одного или нескольких лет;
- время реакции SIF, как правило, намного больше, чем для функций безопасности в режиме работы с высокой частотой запросов.

Концепция, используемая в контексте перерабатывающей промышленности, допускает конкретные действия, когда в приборной системе безопасности (SIS согласно МЭК 61511) обнаружен опасный сбой (путем диагностических тестов, контрольных испытаний или любыми другими способами), после чего будут приняты компенсирующие меры для обеспечения безопасной эксплуатации.

Примечание 2 — Компенсирующие меры, необходимые для продолжения безопасной эксплуатации, могут зависеть от требований полноты безопасности, допустимого риска, связанного с опасным событием, отказоустойчивости аппаратных средств SIS, ожидаемого MRT («среднего времени ремонта») и наличия любых других уровни защиты. В некоторых случаях может быть достаточно обеспечить принятие мер по устранению опасного отказа в пределах предполагаемого MPRT («максимально допустимого времени ремонта») при расчете PFD_{avg}, но в других случаях может быть необходимо предусмотреть другие меры по компенсации снижения риска до полного восстановления SIS.

Подход к обработке сбоев, используемый в контексте безопасности машин для режима работы с высокой частотой запросов, не рассматривает компенсирующие меры: любой опасный сбой, обнаруженный в подсистеме, спроектированной с отказоустойчивостью аппаратных средств, равной 1, приводит к безопасному состоянию. Только после ремонта неисправной подсистемы можно снова возобновить работу машины.

J.3 Использование подсистем с разными режимами работы

J.3.1 Общие положения

Иногда возникает необходимость включения SIF, работающей в режиме работы с низкой частотой запросов, в систему управления, связанную с безопасностью, которая выполняет функции безопасности в режиме работы с высокой частотой запросов, реализованную в рамках ИСО 12100.

Далее представлена информация по проектированию SIF при объединении подсистем, предназначенных для режима работы с низкой частотой запросов, с подсистемами, предназначенными для режима работы с высокой частотой запросов.

Проектирование подсистем не входит в область применения настоящего приложения, и предполагается, что вся информация, относящаяся к интеграции подсистем (включая параметры, связанные с безопасностью), доступна.

J.3.2 Пример с различными режимами работы

Следующие примеры согласно ИСО 13577-4:2022, рисунок Е.14 («контроль высокой температуры») и рисунок Е.17 («контроль низкого давления») представляют собой примеры функциональной безопасности в контексте промышленных печей.

Рассматриваются следующие функции безопасности:

- функция безопасности для «контроля низкого давления» работает в режиме с высокой частотой запросов, когда два реле низкого давления («входная подсистема, реле давления»), установленные на газовом тракте, вызывают закрытие двух двухпозиционных газовых клапанов («выходная подсистема, клапаны»), установленных на том же газовом тракте;

- SIF для «контроля высокой температуры» работает в режиме с низкой частотой запросов, когда две термопары, обнаруживающие критическое значение температуры («входная подсистема, термопары и TLC», спроектированные для режима работы с низкой частотой запросов), запускают включение/выключение двух газовых клапанов («выходная подсистема, клапаны»).

Требуемое значение SIL для SIF в режиме работы с низкой частотой запросов и функции безопасности в режиме работы с высокой частотой запросов должно составлять SIL2.

Примечание 1 — В МЭК 62061:2021, приложение А, представлен возможный метод определения требуемого значения SIL для функций безопасности.

Функциональное представление показано на рисунке J.3, логическое представление — на рисунке J.4, а декомпозиция — на рисунке J.5.

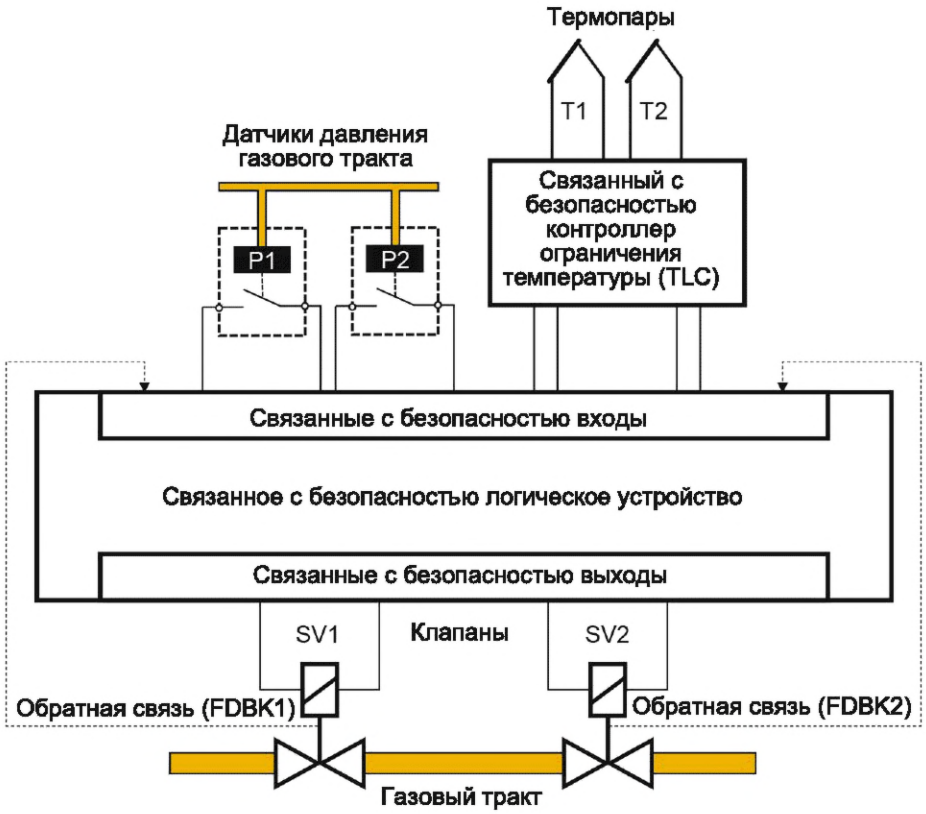


Рисунок J.3 — Функциональное представление

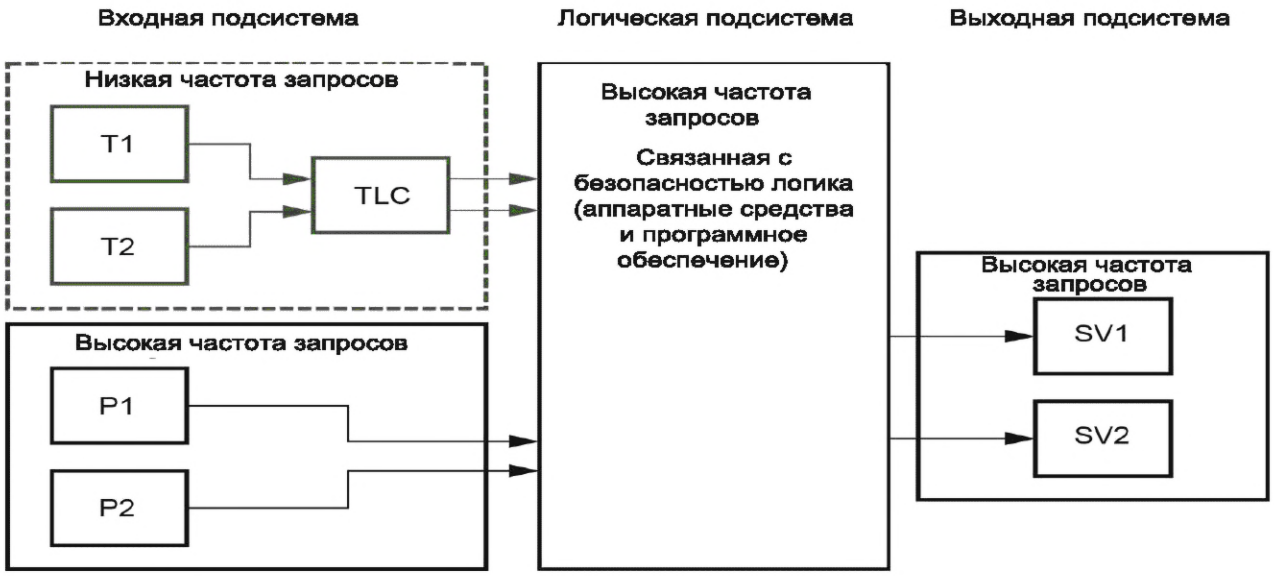


Рисунок J.4 — Логическое представление

Примечание 2 — Проект связанного с безопасностью программного обеспечения системы управления в режиме с низкой частотой запросов, реализованный в «Логической подсистеме», будет отличаться от связанного с безопасностью программного обеспечения подсистем, используемых в режиме работы с высокой частотой запросов. Обе части программного обеспечения, связанные с безопасностью, будут управлять «Выходной подсистемой».

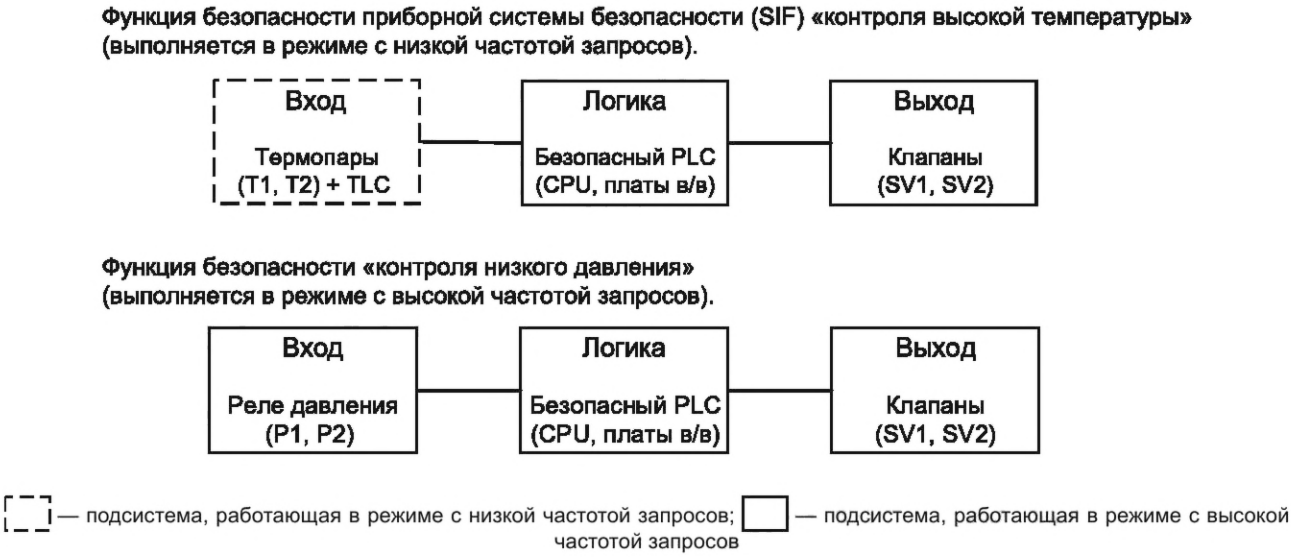


Рисунок J.5 — Представление декомпозиции

J.3.3 Подсистема(ы), используемая(ые) для различных режимов работы

J.3.3.1 Общие положения

На рисунке J.5 показаны подсистема «Логика» и подсистема «Выход», которые будут использоваться для обоих режимов работы.

Простое совместное рассмотрение всей системы управления, связанной с безопасностью, может привести к проблемам из-за базового подхода, основанного на режиме работы с низкой частотой запросов и режиме работы с высокой частотой запросов или с непрерывными запросами (например, PFH в сравнении с PFD_{avg}).

Для оценки SIF «ограничение температуры» будут учитываться следующие аспекты:

- аппаратные средства, программное обеспечение и системные аспекты будут рассматриваться отдельно для обоих режимов работы;

- подсистема «Вход» в режиме работы с низкой частотой запросов будет оцениваться с учетом базовых принципов безопасности, проверенных принципов безопасности и, где это применимо, проверенных компонентов (см. также ИСО 13849-2:2012, приложения A — D);

- количественная оценка подсистемы «Вход» будет рассматриваться, как описано в J.3.3.2;

- для подсистем «Логика» и «Выход» будет не менее одного запроса в год на обнаружение накопления сбоев и необнаруженных сбоев (см. МЭК 62061:2021, 7.3.3.4).

Примечание 1 — В приведенном выше примере это обеспечивается тем, что подсистемы «Логика» и «Выход» также используются в функции безопасности «ограничение давления». В случае сомнений будут приняты технические или организационные меры, обеспечивающие не менее одного срабатывания функции безопасности в год;

- подсистемы, используемые для режима работы с высокой частотой запросов или с непрерывными запросами, не будут оцениваться в контексте режима работы с низкой частотой запросов: функции безопасности и SIF не разрабатываются и не проверяются вместе, но будет рассматриваться общая интеграция программного обеспечения.

Примечание 2 — Подсистема «Вход» будет оцениваться как подсистема SIF в режиме работы с низкой частотой запросов. Подсистемы «Логика» и «Выход» будут оцениваться как подсистемы функции безопасности в режиме работы с высокой частотой запросов. После отдельного проектирования и валидации обеих частей на уровне подсистем выполняется валидация интеграции всех трех подсистем с учетом взаимосвязи и совместимости интерфейсов.

Примечание 3 — Общий подход к функциональной безопасности, начиная со спецификации требований безопасности, проектирование систем управления, связанных с безопасностью, и валидация окончательного решения, будет применяться для обоих режимов работы. Подсистемы «Логика» и «Выход» будут общими для обоих режимов работы, и необходимы дальнейшие исследования, например относительно контрольных проверок, диагностических функций и реализации программного обеспечения (см. также стандарт типа C);

- подсистемы, используемые для обоих режимов работы, будут достигать как минимум одного и того же уровня полноты безопасности (SIL) в режиме работы с низкой частотой запросов и в режиме работы с высокой частотой запросов или с непрерывным режимом работы.

Поскольку комбинация различных режимов работы отсутствует, функция безопасности «ограничение давления» полностью оценивается в режиме работы с высокой частотой запросов, как того требует МЭК 62061.

В этом примере, поскольку «контроль высокой температуры» (подсистема «Вход») работает в режиме с низкой частотой запросов, она оценивается в соответствии с требованиями МЭК 61511 или МЭК 61508.

J.3.3.2 Количественная оценка SIL (режим работы с низкой и высокой частотой запросов)

Оценку системы, связанной с безопасностью, на базе подсистем можно провести следующим образом:

- для каждой подсистемы определяется количественный параметр «отношение вероятности отказов» (RPF, выраженный в процентах) по отношению к целевому SIL;

- целевое значение SIL может быть достигнуто, когда сумма этих отношений вероятности отказов составляет менее 100 %.

Рисунок J.6 иллюстрирует этот подход.

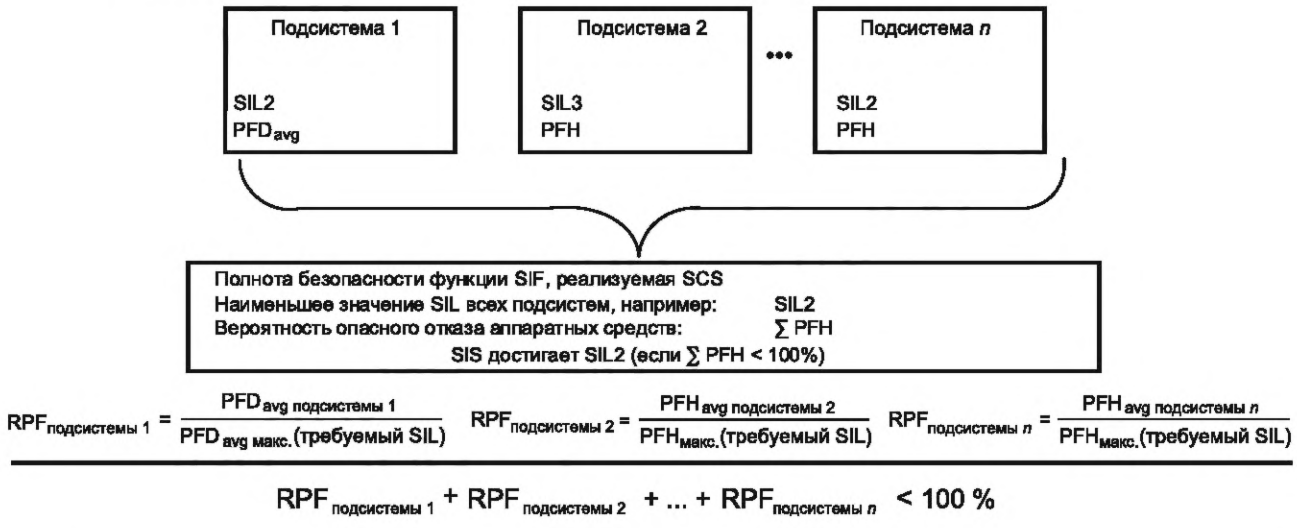
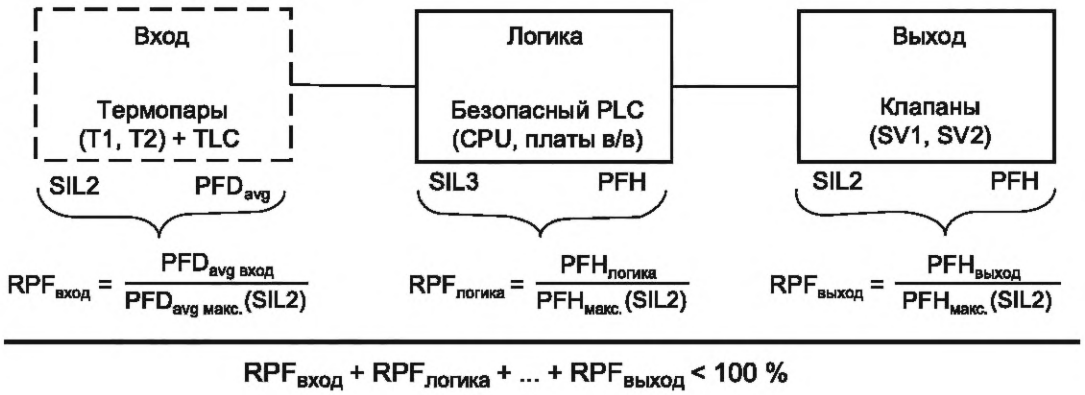


Рисунок J.6 — Количественная оценка SIL с использованием подхода отношения вероятностей отказов каждой подсистемы PFD

J.3.3.3 Пример количественной оценки SIL (режим работы с низкой и высокой частотой запросов)
Рисунок J.7 иллюстрирует этот подход, например, с целевым значением SIL 2 для SIF.



Примечание — В этом примере $PFD_{avg\ макс.}$ и $PFH_{макс.}$ соответствуют SIL 2. Тем не менее, PFH или PFD_{avg} подсистемы могут достигать уровня SIL 3.

Рисунок J.7 — Пример количественной оценки SIL с использованием подхода отношения вероятности отказов каждой подсистемы

В таблице J.1 показаны максимальные значения PFD_{avg} и PFH для соответствующего целевого значения SIL.

Таблица J.1 — $PFD_{avg\ макс.}$ и $PFH_{макс.}$ для соответствующего целевого значения SIL

SIL	$PFD_{avg\ макс.}$	$PFH_{макс.}$, $ч^{-1}$
1	10^{-1}	10^{-5}
2	10^{-2}	10^{-6}
3	10^{-3}	10^{-7}

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным и национальным стандартам

Таблица ДА.1 — Сведения о соответствии ссылочных международных стандартов межгосударственным и национальным стандартам

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 62061:2021	—	*, [1]
IEC TR 63074:2019	IDT	ГОСТ Р 59506—2021/IEC TR 63074:2019 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности»
ISO 12100:2010	IDT	ГОСТ ISO 12100—2013 «Безопасность машин. Основные принципы конструирования. Оценки риска и снижения риска»
ISO 13849-1:2015	—	*, [2]
ISO 13850:2015	—	*
ISO 13851:2019	—	*, [3]
ISO 14118:2017	IDT	ГОСТ ISO 14118—2023 «Безопасность машин. Предотвращение непреднамеренного пуска»
ISO 14119:2013	IDT	ГОСТ ISO 14119—2023 «Безопасность машин. Блокировочные устройства для защитных ограждений. Принципы конструирования и выбора»

* Соответствующий национальный 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.

[1] Действует ГОСТ Р МЭК 62061—2015 «Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью», идентичный МЭК 62061:2005.

[2] Действует ГОСТ ISO 13849-1—2014 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования», идентичный ИСО 13850:2006.

[3] Действует ГОСТ ИСО 13851—2006 «Безопасность оборудования. Двуручные устройства управления. Функциональные аспекты и принципы конструирования», идентичный ИСО 13851:2002.

Библиография

IEC 60204-1:2016 Safety of machinery — Electrical equipment of machines — Part 1: General requirements (Безопасность машин. Электрооборудование машин и механизмов. Часть 1. Общие требования)

IEC 60947-5-3:2013 Low-voltage switchgear and controlgear — Part 5-3: Control circuit devices and switching elements — Requirements for proximity devices with defined behaviour under fault conditions (PDDB) (Аппаратура коммутационная и механизмы управления низковольтные. Часть 5-3. Устройства и коммутационные элементы цепей управления. Требования к близко расположенным устройствам с определенным поведением в условиях отказа)

IEC 60947-5-8:2020 Low-voltage switchgear and controlgear — Part 5-8: Control circuit devices and switching elements — Three-position enabling switches (Аппаратура распределения и управления низковольтная. Часть 5-8. Аппараты и элементы коммутации для цепей управления. Трехпозиционные выключатели блокировки)

IEC 60947-7-1 Low-voltage switchgear and controlgear — Part 7-1: Ancillary equipment — Terminal blocks for copper conductors (Аппаратура распределения и управления низковольтная. Часть 7-1. Электрооборудование вспомогательное. Колодки клеммные для медных проводников)

IEC 60947-7-2 Low-voltage switchgear and controlgear — Part 7-2: Ancillary equipment — Protective conductor terminal blocks for copper conductors (Аппаратура распределения и управления низковольтная. Часть 7-2. Электрооборудование вспомогательное. Колодки клеммные защитных проводников для присоединения медных проводников)

IEC 61000-6-7 Electromagnetic compatibility (EMC) — Part 6-7: Generic standards — Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations (Электромагнитная совместимость (ЭМС). Часть 6-7. Общие стандарты. Требования помехоустойчивости для оборудования, предназначенного для выполнения функций в системе, связанной с безопасностью (функциональная безопасность) в промышленных расположениях)

IEC 61025:2006 Fault tree analysis (FTA) (Анализ диагностического дерева неисправностей)

IEC 61496-1:2016 Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests (Безопасность механизмов. Защитная электрочувствительная аппаратура. Часть 1. Общие требования и испытания)

IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 1: General requirements (see gost.e-ecolog.ru Functional Safety and IEC 61508) (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 1. Общие требования)

IEC 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 4: Definitions and abbreviations (see gost.e-ecolog.ru Functional Safety and IEC 61508) (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 4. Определения и сокращения)

IEC 61508-5:2010 Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 5: Examples of methods for the determination of safety integrity levels (see gost.e-ecolog.ru ch/functionalsafety Functional Safety and IEC 61508) (Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 5. Примеры методов для определения уровней целостности защиты)

IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see gost.e-ecolog.ru functionalsafety Functional Safety and IEC 61508) (Системы электрические/электронные/программируемые электронные, связанные с функциональной безопасностью. Часть 6. Руководящие указания по применению стандартов IEC 61508-2 и IEC 61508-3)

IEC 61508-7:2010 Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 7: Overview of techniques and measures (see gost.e-ecolog.ru Functional Safety and IEC 61508) (Функциональная безопасность электрических/электронных/программируемых электронных систем, обеспечивающих безопасность. Часть 7. Обзор методов и средств измерения)

IEC 61800-5-2:2016 Adjustable speed electrical power drive systems — Part 5-2: Safety requirements — Functional (Системы силовых электрических приводов с регулируемой скоростью. Часть 5-2. Требования к функциональной безопасности)

IEC 61511 (all parts)	Functional safety — Safety instrumented systems for the process industry sector [Безопасность функциональная. Системы безопасности приборные для промышленных процессов (все части)]
IEC 61649:2008	Weibull analysis (Анализ Вейбулла)
IEC TS 62998-1:2019	Safety of machinery — Safety-related sensors used for the protection of persons (Безопасность механизмов. Датчики, связанные с безопасностью, используемые для защиты людей)
ISO 11161:2007	Safety of machinery — Integrated manufacturing systems — Basic requirements (Безопасность машин и механизмов. Интегрированные производственные системы. Основные требования)
ISO 13855:2010[1)]	Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body (Безопасность машин. Позиционирование защитного оборудования с учетом скорости сближения частей человеческого тела)
ISO 13856:2013	Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for the design and testing of pressure-sensitive mats and pressure-sensitive floors (Безопасность машин. Сенсорные защитные устройства. Часть 1. Общие принципы расчета и испытания сенсорных ковриков и полов)

[1)] Заменен на ISO 13855:2024. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

УДК 62-783:614.8:331.454.004.056.5:006.354

ОКС 13.110
29.020
25.040.99

Ключевые слова: функциональная безопасность, безопасность машин и механизмов, уровень полноты безопасности, уровень эффективности защиты, оценка рисков, требования безопасности, параметры безопасности

Редактор *М.В. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректоры *Е.Д. Дульнева*, *М.И. Першина*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 01.10.2025. Подписано в печать 21.10.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 13,02. Уч.-изд. л. 11,78.

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

gost.e-ecolog.ru