ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72296— 2025

ЛИФТЫ

Электронные и программируемые системы, применяемые в цепях безопасности

(ISO 22201-1:2017, NEQ)

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Евразийской Лифтовой Ассоциацией (Ассоциация «ЕЛА»), Обществом с ограниченной ответственностью «Э-Лифт» (ООО «Э-Лифт»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 209 «Лифты, эскалаторы, пассажирские конвейеры и подъемные платформы для инвалидов»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 16 сентября 2025 г. № 1055-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО 22201-1:2017 «Лифты, эскалаторы и пассажирские конвейеры. Программируемые электронные системы, применяемые в цепях безопасности. Часть 1. Лифты» [ISO 22201-1:2017 «Lifts (elevators), escalators and moving walks — Programmable electronic systems in safety-related applications — Part 1: Lifts (elevators) (PESSRAL)», NEQ]

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, уведомление 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

© 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 1
3 Термины и определения 2
4 Требования 4
4.1 Общие положения 4
4.2 Применение настоящего стандарта 5
4.3 Требования к УПБ для функций безопасности 5
4.4 Требования к безопасному состоянию, относящиеся к УПБ и не относящиеся к УПБ 8
4.5 Требования к применению и проверке соответствия требованиям УПБ 16
Приложение А (обязательное) Меры по применению и проверке соответствия требованиям уровню полноты безопасности 17
Приложение Б (справочное) Пример таблицы принятия решений по снижению риска 29

Введение

Лифты являются одним из самых безопасных видов транспорта.

До настоящего времени их функции, связанные с безопасностью, по большей части реализовывались электромеханическими компонентами. Электронные компоненты до настоящего времени применялись для обеспечения безопасности на лифтах только в единичных случаях.

Программируемые системы (программируемые электронные системы), так называемые PESSRAL (программируемая система для лифтов, связанная с безопасностью), объединяют эти функции и, таким образом, заменяют механические компоненты, требующие интенсивного обслуживания и подверженные старению.

Настоящий стандарт устанавливает общий подход к обеспечению безопасности для всех стадий жизненного цикла систем, состоящих из электронных и/или программируемых (Э/ПЭ) элементов, которые используются для выполнения функций обеспечения безопасности. Этот подход принят для того, чтобы разработать рациональный и последовательный подход для всех электрических систем обеспечения безопасности. Для эффективного и безопасного использования технологии программируемых систем важно, чтобы лица, ответственные за принятие решений, были обеспечены рекомендациями по аспектам безопасности, на основе которых принимаются эти решения. В большинстве ситуаций безопасность достигается с помощью ряда защитных систем, которые основаны на многих технологиях (например, механических, гидравлических, пневматических, электрических, электронных, программируемых электронных устройствах). Таким образом необходимо, чтобы любая стратегия обеспечения безопасности учитывала не только все компоненты отдельной системы (например, датчики, управляющие устройства и пускатели), но и все связанные с безопасностью элементы, составляющие общую комбинацию систем, связанных с безопасностью.

Анализ рисков каждой функции безопасности, указанный в таблице 1, относится к классификации функций электробезопасности, с применением Э/ПЭ. В таблицах 1 и 2 приведены уровни целостности безопасности и функциональные требования, соответственно, для каждой функции электробезопасности.

Настоящий стандарт предоставляет поддающийся проверке метод установления необходимого уровня целостности безопасности для функций безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЛИФТЫ

Электронные и программируемые системы, применяемые в цепях безопасности

Lifts. Electronic and programmable systems in safety related circuits

Дата введения — 2026—01—01

1 Область применения

1.1 Настоящий стандарт распространяется на пассажирские и грузопассажирские лифты, используемые в жилых зданиях, офисах, больницах, гостиницах, промышленных предприятиях и т. д.

1.2 Настоящий стандарт устанавливает требования, которые необходимо учитывать при использовании электронных и/или программируемых (Э/ПЭ) систем для выполнения функций безопасности лифтов.

1.3 Настоящий стандарт не распространяется на опасности, связанные с оборудованием электронных систем, таких как поражение электрическим током и т. д.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ IEC 61508-3 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р 55490 Платы печатные. Общие технические требования к изготовлению и приемке

ГОСТ Р МЭК 60664.1—2012 Координация изоляции для оборудования в низковольтных системах. Часть 1. Принципы, требования и испытания

ГОСТ Р МЭК 61249-2-2 Материалы для печатных плат и других структур межсоединений. Часть 2-2. Материалы основания армированные фольгированные и нефольгированные. Листы армированные слоистые на основе целлюлозной бумаги, пропитанной фенольным связующим, фольгированные медью и обладающие высокими электрическими характеристиками

ГОСТ Р МЭК 61508-1—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-2 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам

ГОСТ Р МЭК 61508-5 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности

ГОСТ Р МЭК 61508-7—2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

Издание официальное

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **останавливающее устройство с ручным управлением:** Останавливающее устройство, которое приводится в действие и отключается с помощью вмешательства человека.

Пример — Тумблер, выключатель грибовидного типа или переключатель с ручным управлением.

3.2 **останавливающее устройство без ручного управления:** Останавливающее устройство, которое автоматически приводится в действие или деактивируется без вмешательства человека.

3.3 **уровень полноты безопасности;** УПБ: Дискретный уровень (один из четырех возможных) для определения требований к целостности функций безопасности, обеспечиваемых электронной и/или программируемой системой, связанной с безопасностью, где уровень целостности безопасности 4 имеет самый высокий уровень целостности безопасности, а уровень целостности безопасности 1 имеет самый низкий.

3.4 **требование к безопасности, не относящееся к уровню полноты безопасности:** Требование, которое включает запрос на включение функции безопасности с рейтингом УПБ, при этом функция, выполняющая этот запрос, может не иметь рейтинг УПБ.

Примечание — См. рисунок 4 и таблицу 2.

3.5 **программируемый элемент;** ПЭ: Устройство, основанное на компьютерной технологии, которое может состоять из технического оборудования, программного обеспечения и блоков ввода и/или вывода.

Примечание — Этот термин охватывает микроэлектронные устройства, основанные на одном или нескольких центральных процессорах (CPU), вместе с соответствующими запоминающими устройствами и т. д.

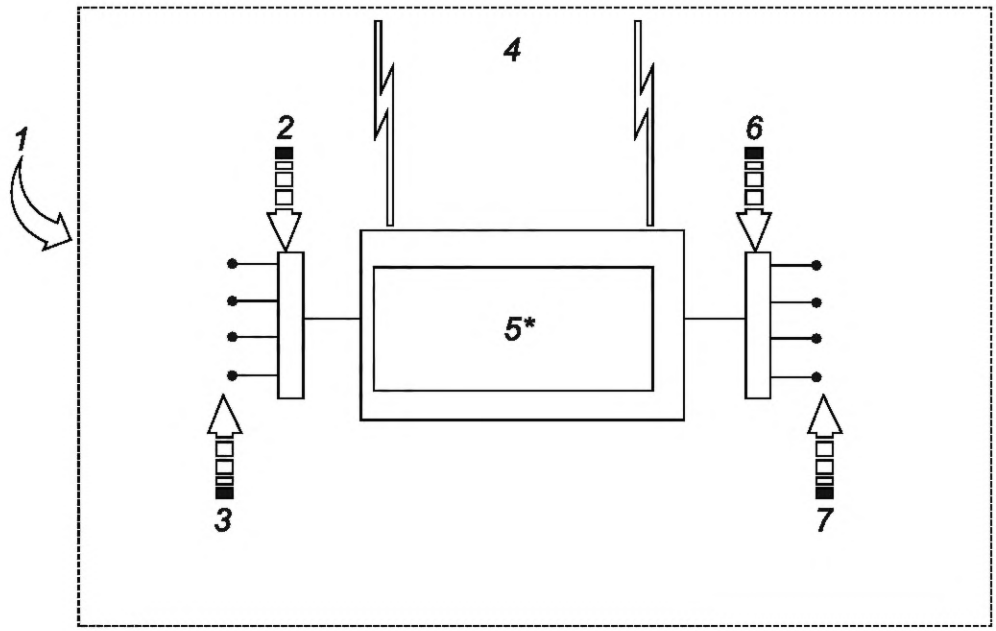
Примечание — К программируемым устройствам относятся:
- микропроцессоры;
- микроконтроллеры;
- программируемые контроллеры;
- программируемая логическая интегральная схема (FPGA);
- специализированные интегральные схемы (ASIC);
- программируемые логические контроллеры (ПЛК); и
- другие компьютерные устройства (например, интеллектуальные датчики, передатчики, пускатели).

3.6 **программируемая система;** ПЭС: Система управления, защиты или мониторинга, основанная на одном или нескольких программируемых электронных устройствах, включая все элементы системы, такие как источники питания, датчики и другие устройства ввода, магистрали передачи данных и другие каналы связи, а также пускатели и другие устройства вывода.

Примечания

1 См. рисунок 1.

2 ПЭС может включать элементы, соответствующие нормам УПБ, и элементы, не соответствующие нормам УПБ. Рейтинг УПБ требуется только для тех элементов, которые выполняют функциональные требования, соответствующие нормам УПБ.



* Программируемый элемент расположен в центре, но может находиться в нескольких местах в ПЭС.

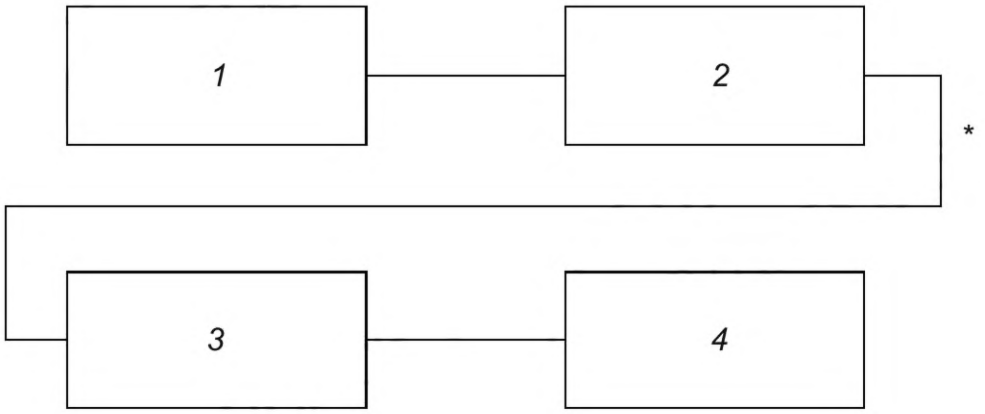
1 — область применения ПЭС; *2* — вводные интерфейсы (например, аналого-цифровые преобразователи); *3* — устройства ввода (например, датчики); *4* — средства связи; *5* — ПЭ; *6* — выходные интерфейсы (например, аналого-цифровые преобразователи); *7* — устройства вывода/конечные элементы (например, пускатели)

Рисунок 1 — Базовая структура ПЭС

3.7 **контрольный тест:** Периодический тест, проводимый для выявления опасных скрытых сбоев в системе, связанной с безопасностью, чтобы при необходимости ремонт мог восстановить систему до состояния «как новая» или максимально приближенного к этому состоянию.

3.8 **цепь безопасности:** Общая комбинация предохранительных устройств, выполняющих все функции безопасности лифта или их группу.

Примечание — См. рисунок 2.



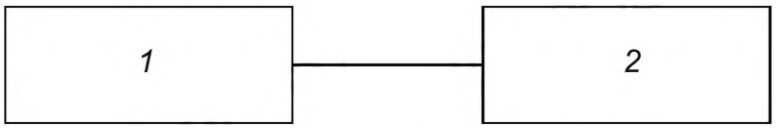
* Все или группа требуемых функций безопасности лифта (см. таблицу 1).

1 — устройство безопасности 1, функция 1; *2* — устройство безопасности 2, функция 2; *3* — устройство безопасности *n*, функция *n*; *4* — устройство безопасности (*n* + 1), функция (*n* + 1)

Рисунок 2 — Цепь безопасности

3.9 **устройство безопасности:** Часть системы, связанной с безопасностью, включая необходимые цепи безопасности, которая предназначена для самостоятельного выполнения функции безопасности лифта, и которая может состоять из ПЭ и элементов, не являющихся ПЭ.

Примечание — См. рисунок 3 и таблицу 1.



1 — элементы ПЭ; *2* — элементы, не являющиеся ПЭ

Рисунок 3 — Устройство безопасности

3.10 **функция безопасности:** Функция, реализуемая системой, связанной с безопасностью, которая предназначена для достижения или поддержания безопасного состояния лифта в отношении конкретного опасного события.

Примечания

1 См. таблицу 1.

2 Функция безопасности может включать требования, не относящиеся к УПБ (см. таблицу 2).

3.11 **система, связанная с безопасностью:** Одно или несколько предохранительных устройств, выполняющих одну или несколько функций безопасности, которые могут быть основаны на программируемых электронных, электронных и/или механических элементах лифта.

Примечания

1 УПБ указывает на частоту отказов, которая включает все причины отказов (как случайные сбои оборудования, так и систематические сбои), которые приводят к небезопасному состоянию, например сбои оборудования, сбои, вызванные программным обеспечением, и сбои из-за электрических помех.

2 В настоящем стандарте УПБ-3 — это наивысший уровень безопасности, который должен применяться к лифтам.

3.12 **функция безопасности лифта:** Система, которая состоит из узла, обеспечивающего соответствующий уровень безопасности по уровню полноты безопасности, и узла, который непосредственно не относится к обеспечению уровня безопасности по уровню полноты безопасности.

Примечание — См. рисунок 4 и таблицу 2.



1 — относящееся к УПБ требование (требования) безопасного состояния; *2* — не относящееся к УПБ требование (требования) безопасного состояния

Рисунок 4 — Функция безопасности лифта

3.13 **время реакции системы:** Сумма следующих двух значений:

а) период времени между возникновением неисправности в Э/ПЭ и началом соответствующего действия в лифте;

б) период времени, в течение которого лифт реагирует на действие, поддерживая безопасное состояние.

4 Требования

4.1 Общие положения

4.1.1 В таблице 1 указаны названия функций безопасности, описание соответствующих функций лифта, применимый тип лифта и требуемый УПБ для соответствующей части УПБ функции безопасности. Лифт может находиться в рабочем состоянии в нормальном режиме работы без перерыва до тех пор, пока не сработает одна из функций безопасности.

4.1.2 В таблице 2 определены требования к безопасному состоянию при срабатывании функций безопасности, указанных в таблице 1. При срабатывании функции безопасности, функция безопасности должна привести к возврату лифтовой системы в безопасное состояние, указанное в таблице 2.

4.1.3 Э/ПЭ должно учитывать время срабатывания лифта для ответа на функцию безопасности и обнаружения внутренних неисправностей за время, необходимое для достижения безопасного состояния без угрозы. Методы, обеспечивающие обнаружение внутренних неисправностей, должны учитывать необходимое время реакции системы, требуемое УПБ.

Пример — Если внутренняя неисправность обнаружена путем сравнения данных в системе с дублированием в течение времени, которое необходимо для обеспечения времени реакции системы, то допускается не выполнять проверку диапазона времени реакции системы с оперативной памятью, поскольку целостность безопасности проверяется благодаря дублированию.

4.2 Применение настоящего стандарта

4.2.1 Общие положения

Требования в 4.2.2—4.2.4 приведены для проверки УПБ и условий безопасного состояния для функций безопасности лифтов, которые являются новыми или отклоняются от требований, приведенных в 4.3 и 4.4.

4.2.2 Оценка риска

При поиске альтернатив требованиям 4.3 и/или 4.4 способы определения проверки требуемого уровня безопасности должны выполняться в соответствии с ГОСТ Р МЭК Р 61508-5. Те же способы следует использовать для обоснования новой функции Э/ПЭ и соответствующей УПБ или пересмотренной функции Э/ПЭ и/или УПБ, которые отличаются от требований 4.3 и 4.4. Средняя целевая частота отказов для наихудшего варианта тяжести последствий любого отдельного сценария потенциальной опасности не должна превышать частоту $5 \cdot 10^7$ в год.

4.2.3 Пределы для указания УПБ для Э/ПЭ

Целевые показатели отказа, необходимые для определения ПЭ в функции, связанной с безопасностью лифта, должны быть не ниже УПБ 1 и не выше УПБ 3. Если для целевого показателя отказа требуется значение УПБ выше, чем УПБ 3, следует рассмотреть возможность перепроектирования системы таким образом, чтобы требуемый показатель целевого отказа соответствовал значению УПБ 3 или меньше. Если требуется значение УПБ ниже УПБ 1, может использоваться ПЭ, не соответствующий нормам УПБ, но он не должен классифицироваться как Э/ПЭ. Ни один Э/ПЭ не должен иметь УПБ ниже УПБ 1, даже если он применяется для функции безопасности, требующей УПБ ниже УПБ 1.

Применение — Функции безопасности уровня целостности безопасности 4, как правило, не требуются в данной отрасли.

Таких применений следует избегать из-за сложности их реализации и поддержания таких высоких уровней безопасности на протяжении всего жизненного цикла защитного устройства. Если анализ приводит к присвоению функции безопасности лифта уровня целостности безопасности 4 или выше, следует рассмотреть возможность изменения конструкции процесса таким образом, чтобы он стал более безопасным, или путем добавления дополнительных уровней защиты. Эти усовершенствования, возможно, затем могут снизить требования к уровню целостности системы безопасности лифта. Если уровень целостности безопасности не может быть снижен, целевая мера отказа для функции безопасности должна быть распределена по нескольким Э/ПЭ УПБ 3 или ниже, которые являются достаточно независимыми и сертифицированы в применении.

4.2.4 Требования к безопасному состоянию

Для функций безопасности лифта, которые являются новыми или отличаются от указанных в 4.3 и 4.4, проектировщик должен определить требования к безопасному состоянию способом, аналогичным тому, в котором они описаны в таблице 2.

4.3 Требования к УПБ для функций безопасности

В таблице 1 приведены требуемые значения УПБ для каждой функции безопасности лифта.

Таблица 1 — Требования к функциям безопасности УПБ

Функция безопасности лифта	Описание функционала	Область применения	УПБ
1 Останавливающее устройство в приямке	Останавливающее устройство с ручным управлением	Все лифты	3
2 Останавливающее устройство в блочном помещении	Останавливающее устройство с ручным управлением	Все лифты	3
3 Контроль положения хранения приставной лестницы в приямке	Обнаруживает отсутствия положения хранения приставной лестницы в приямке	Все лифты	1
4 Контроль закрытого состояния дверей доступа, аварийных дверей и смотровых люков	Обнаруживает незакрытое состояние дверей доступа, аварийных дверей и смотровых люков	Все лифты	2
5 Контроль запирания двери кабины	Обнаруживает незапертую дверь (двери) кабины	Все лифты	2
6 Контроль неактивного состояния механического устройства	Обнаруживает правильное неактивное положение механического устройства, обеспечивающего защиту на кабине лифта	Все лифты	3
7 Контроль запертого состояния смотровых дверей или люков	Обнаруживает незакрытое состояние смотровых дверей и люков	Все лифты	2
8 Контроль открытого состояния любой двери, обеспечивающей доступ в приямок	Обнаруживает незакрытое состояние двери обеспечивающей доступ в приямок	Все лифты	2
9 Контроль неактивного состояния механического устройства	Обнаруживает правильное неактивное положение механического устройства, обеспечивающего защиту в приямке	Все лифты	3
10 Контроль активного состояния механического устройства	Обнаруживает правильное активное положение механического устройства, обеспечивающего защиту в приямке	Все лифты	3
11 Контроль отведенного положения рабочей платформы	Обнаруживает, полностью ли убрана выдвижная рабочая платформа	Все лифты	3
12 Контроль отведенного положения подвижных упоров	Обнаруживает, полностью ли отведены подвижные упоры	Все лифты	3
13 Контроль выдвинутого положения подвижных упоров	Обнаруживает, полностью ли выдвинуты подвижные упоры	Все лифты	3
14 Контроль запертого положения запирающего устройства двери шахты	Обнаруживает незапертое положение замков дверей шахты	Все лифты	3
15 Контроль закрытого положения дверей шахты	Обнаруживает незакрытое положение дверей шахты	Все лифты	3
16 Контроль закрытого положения створок, не запертых замком	Обнаруживает незакрытое положение створок дверей шахты, не оборудованных замком	Все лифты	3
17 Контроль закрытого положения двери кабины	Обнаруживает незапертую дверь (двери) кабины	Все лифты	2
18 Контроль запирания аварийного люка и аварийной двери в кабине	Обнаруживает не запертое состояние аварийного люка и аварийной двери в кабине	Все лифты	2
19 Останавливающее устройство на крыше кабины	Останавливающее устройство с ручным управлением	Все лифты	3
20 Контроль поднимания кабины или противовеса	Обнаруживает нахождение кабины или противовеса на буферах	Все лифты	2

Продолжение таблицы 1

Функция безопасности лифта	Описание функционала	Область применения	УПБ
21 Контроль ненормального относительного растяжения каната или цепи в случае использования двух подвешивающих канатов или цепей	Обнаруживает потерю натяжения в тросах или цепи, в случае двойных тросов или двойной цепи	Все лифты	1
22 Контроль слабины каната или слабины цепи для лифтов с позитивным и гидравлическим приводом	Обнаруживает потерю натяжения в тросах или цепи	Лифт с позитивным и гидравлическим приводом	2
23 Контроль устройства защиты от подскока	Определяет, были ли превышены пределы перемещения компенсационного средства фиксации (защита от подскока)	Лифт с приводом трения	3
24 Контроль срабатывания ловителя кабины	Обнаруживает, сработали ли ловители на кабине	Все лифты	3
25 Обнаружение превышения скорости	Обнаруживает превышение скорости кабины максимального предела, установленного до срабатывания ограничителя скорости; может быть автоматически сброшен	Все лифты	2
26 Контроль возврата ограничителя скорости в исходное состояние	Обнаруживает невозвращение в исходное положение ограничителя скорости	Все лифты	2
27 Контроль натяжения каната ограничителя скорости	Обнаруживает ослабление вытяжки каната, приводящего в действие ограничитель скорости	Все лифты	2
28 Контроль обрыва или ослабления каната безопасности	Обнаруживает ослабление или обрыв каната безопасности	Все лифты	2
29 Контроль выдвинутого положения отключающего рычага	Обнаруживает полностью выдвинутое положение отключающего рычага, воздействующего на ловители	Все лифты	2
30 Контроль отведенного положения отключающего рычага	Обнаруживает полностью отведенное положение отключающего рычага, воздействующего на ловители	Все лифты	2
31 Контроль отведенного положения упоров	Обнаруживает отведенное положение упоров	Лифт с гидравлическим приводом	2
32 Контроль возврата в нормальное выдвинутое положение буферов в том случае, когда буферы с рассеянием энергии используют вместе со стопорным устройством	Обнаруживает возврат в нормальное выдвинутое положение буферов	Лифт с гидравлическим приводом	2
33 Контроль средства защиты от превышения скорости поднимающейся вверх кабины	Обнаруживает превышение скорости поднимающейся вверх кабины	Все лифты	3
34 Обнаружение непреднамеренного передвижения кабины с открытыми дверями	Обнаруживает непреднамеренное передвижение кабины с открытыми дверями	Все лифты	2
35 Контроль возврата буферов в нормальное выдвинутое положение	Обнаруживает невозвращение буферов в нормальное выдвинутое положение	Все лифты	2
36 Контроль положения съемного штурвала	Обнаруживает наличие съемного штурвала на лебедке	Лифт с приводом трения	2

Окончание таблицы 1

Функция безопасности лифта	Описание функционала	Область применения	УПБ
37 Контроль отключения лифта несамовозвратным устройством в машинном помещении	Обеспечивает отключение лифта при необходимости	Все лифты	2
38 Контроль замедления в случае буферов с уменьшенным рабочим ходом	Обнаруживает, произошло ли замедление скорости до прибытия на крайние остановки	Лифт с приводом трения	3
39 Контроль выравнивания на этаже, повторного выравнивания и предварительных операций	Определяет, находится ли кабина вне зоны выравнивания, с открытыми дверями, во время выравнивания, или повторного выравнивания, или предварительных операций	Все лифты	2
40 Выключатель режима «Ревизия»	Обеспечивает отключение управления в нормальном режиме работы и в режиме управления из машинного помещения	Все лифты	3
41 Шунтирующее устройство для контактов дверей шахты и кабины	Обнаруживает, активирован ли режим шунтирования двери шахты или кабины	Все лифты	3
42 Останавливающее устройство в режиме «Ревизия»	Останавливающее устройство с ручным управлением	Все лифты	3
43 Останавливающее устройство в панели для эвакуации и испытаний	Останавливающее устройство с ручным управлением	Все лифты	3
44 Контроль натяжения в устройстве для передачи положения кабины (предельные концевые выключатели)	Обнаруживает отсутствие натяжения в устройстве для передачи положения кабины	Лифт с приводом трения, лифт с позитивным приводом	1
45 Контроль натяжения в устройстве для передачи положения поршня (предельные концевые выключатели)	Обнаруживает отсутствие натяжения в устройстве для передачи положения поршня	Лифт с гидравлическим приводом	1
46 Предельные концевые выключатели	Обнаруживает, если кабина заходит за них	Все лифты	1

4.4 Требования к безопасному состоянию, относящиеся к УПБ и не относящиеся к УПБ

В таблице 2 представлена требуемая реакция системы управления лифтом на срабатывание функции безопасности лифта, указанные в таблице 1, а также уровень УПБ и требования, не относящиеся к УПБ, для каждой реакции при срабатывании этой функции.

В таблице обозначение «X» указывает, что данная реакция системы требуется для безопасного состояния, когда срабатывает функция безопасности или когда Э/ПЭ обнаруживает состояние неисправности. Там, где необходимо более подробное разъяснение, в таблице вместо «X» приведены конкретные пояснения (см. примечание таблицы).

Таблица 2 — Реакция системы управления лифтом на срабатывание устройства безопасности лифта

Функции безопасности лифта	Связано с УПБ				Не связано с УПБ									
	Отключение питания с двигателя лебедки и тормоза (тяговые лифты), соответственно, с двигателя и/или задействованного каната (канатов) (лифты с гидравлическим приводом)	Блокирование (предотвращение) автоматического функционирования лифта (R26)	Ограничение дальности перемещения	Прерывание цепи питания катушки автоматического выключателя контактора	Операция перехода в режим ревизии	Ограничение скорости кабины	Ограничение движения кабины в направлении	Требуется ручной сброс	Игнорировать* проверке дверь кабины закрыта и/или заперта	Игнорировать* проверке дверь шахты закрыта и/или заперта	Блокирование (предотвращение) автоматического функционирования дверей	Блокировать (предотвратить) операцию аварийный режим электроснабжения	Блокировать (предотвратить) операцию антипроскальзывание (только для гидравлики)	Блокировать (предотвратить) операцию ревизии на кабине	Блокировать (предотвратить) операцию доступа в шахту	Разрешен профиль скорости старт-стоп	Активизировать сигнализацию
1 Останавливающее устройство в приямке	x	—	—	—	—	—	—	—	—	x	x	—	—	—	—	—	—
2 Останавливающее устройство в блочном помещении	x	—	—	—	—	—	—	—	—	x	x	—	—	—	—	—	—
3 Контроль положения хранения приставной лестницы в приямке	x	—	—	—	—	—	—	—	—	x	x	—	—	—	—	—	—
4 Контроль закрытого состояния дверей доступа, аварийных дверей и смотровых люков	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
5 Контроль запирания двери кабины	R24	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
6 Контроль неактивного состояния механического устройства	x	—	—	—	—	R5	—	—	—	—	—	—	—	—	—	—	—
7 Контроль запертого состояния смотровых дверей или люков	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
8 Контроль открытого состояния любой двери, обеспечивающей доступ в приямок	R24	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
9 Контроль неактивного состояния механического устройства в приямке	R21	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Продолжение таблицы 2

Функции безопасности лифта	Связано с УПБ				Не связано с УПБ									
	Отключение питания с двигателя лебедки и тормоза (тяговые цепи), соответственно, с двигателя и/или задействованного клапана (клапанов) (цепи с гидравлическим приводом) (R26)	Блокирование (предотвращение) автоматического функционирования лифта	Ограничение длительности перемещения	Прерывание цепи питания катушки автоматического выключателя контактора	Операция перехода в режим ревизии	Ограничение скорости кабины	Ограничение движения кабины в направлении	Требуется ручной сброс	Игнорировать* проверки дверь кабины закрыта и/или заперта	Игнорировать* проверки дверь шахты закрыта и/или заперта	Блокирование (предотвращение) автоматического функционирования дверей	Блокировать (предотвратить) операцию аварийный режим электроснабжения	Блокировать (предотвратить) операцию антипроскальзывание (только для гидравлики)	Блокировать (предотвратить) операцию ревизии на кабине	Блокировать (предотвратить) операцию доступа в шахту	Разрешен профиль скорости старт-стоп	Активизировать сигнализацию
10 Контроль активного состояния механического устройства в приямке	R23	—	x	—	—	R5	—	—	—	—	—	—	—	—	—	—	—
11 Контроль отведенного положения рабочей платформы	R20	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
12 Контроль отведенного положения подвижных упоров	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
13 Контроль выдвинутого положения подвижных упоров	R22	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
14 Контроль запертого положения запирающего устройства двери шахты	R17	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
15 Контроль закрытого положения дверей шахты	R17	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
16 Контроль закрытого положения створок, незапертых замком	R17	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
17 Контроль закрытого положения двери кабины	R17	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
18 Контроль запирания аварийного люка и аварийной двери в кабине	R17	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Продолжение таблицы 2

Функции безопасности лифта	Связано с УПБ				Не связано с УПБ									
	Отключение питания с двигателя лебедки и тормоза (тяговые лифты), соответственно, с двигателя и/или заделанного каната (канатов) (лифты с гидравлическим приводом)	Блокирование (предотвращение) автоматического функционирования лифта (R26)	Ограничение длительности перемещения	Прерывание цепи питания катушки автоматического выключателя контактора	Операция перехода в режим ревизии	Ограничение скорости кабины	Ограничение движения кабины в направлении	Требуется ручной сброс	Игнорировать* проверке дверь кабины закрыта и/или заперта	Игнорировать* проверке дверь шахты закрыта и/или заперта	Блокирование (предотвращение) автоматического функционирования дверей	Блокировать (предотвратить) операцию аварийный режим электроснабжения	Блокировать (предотвратить) операцию антипроскальзывание (только для гидравлики)	Блокировать (предотвратить) операцию ревизии на кабине	Блокировать (предотвратить) операцию доступа в шахту	Разрешен профиль скорости старт-стоп	Активизировать сигнализацию
19 Останавливающее устройство на крыше кабины	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
20 Контроль поднимания кабины или противовеса	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
21 Контроль ненормального относительного растяжения каната или цепи в случае использования двух подвешивающих канатов или цепей	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
22 Контроль слабины каната или слабины цепи для лифтов с позитивным приводом и гидравлических лифтов	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
23 Контроль устройства защиты от подскока	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
24 Контроль срабатывания ловителя кабины	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
25 Обнаружение превышения скорости	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
26 Контроль возврата ограничителя скорости в исходное состояние	R1	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Продолжение таблицы 2

Функции безопасности лифта	Связано с УПБ				Не связано с УПБ									
	Отключение питания с двигателя лебедки и тормоза (тяговые цепи), соответственно, с двигателя и/или задействованного клапана (клапанов) (цепи с гидравлическим приводом)	Блокирование (предотвращение) автоматического функционирования лифта (R26)	Ограничение длительности перемещения	Прерывание цепи питания катушки автоматического выключателя контактора	Операция перехода в режим ревизии	Ограничение скорости кабины	Ограничение движения кабины в направлении	Требуется ручной сброс	Игнорировать* проверки дверь кабины закрыта и/или заперта	Игнорировать* проверки дверь шахты закрыта и/или заперта	Блокирование (предотвращение) автоматического функционирования дверей	Блокировать (предотвратить) операцию аварийный режим электроснабжения	Блокировать (предотвратить) операцию антипроскальзывание (только для гидравлики)	Блокировать (предотвратить) операцию ревизии на кабине	Блокировать (предотвратить) операцию доступа в шахту	Разрешен профиль скорости старт-стоп	Активизировать сигнализацию
27 Контроль натяжения каната ограничителя скорости	x	—															
28 Контроль обрыва или ослабления каната безопасности	x	—															
29 Контроль выдвинутого положения отключающего рычага	x	x															
30 Контроль отведенного положения отключающего рычага	x	x															
31 Контроль отведенного положения упоров	x	x															
32 Контроль возврата в нормальное выдвинутое положение буферов в том случае, когда буферы с рассеянием энергии используют вместе со стопорным устройством	R13	—				—	R14										
33 Контроль средства защиты от превышения скорости поднимающейся вверх кабины	x	—				x											

Продолжение таблицы 2

Функции безопасности лифта	Связано с УПБ				Не связано с УПБ												
	Отключение питания с двигателя лебедки и тормоза (тяговые лифты), соответственно, с двигателя и/или задействованного клапана (клапанов) (лифты с гидравлическим приводом)	Блокирование (предотвращение) автоматического функционирования лифта (R26)	Ограничение дальности перемещения	Прерывание цепи питания катушки автоматического выключателя контакора	Операция перехода в режим ревизии	Ограничение скорости кабины	Ограничение движения кабины в направлении	Требуется ручной сброс	Игнорировать* проверьте дверь кабины закрыта и/или заперта	Игнорировать* проверьте дверь шахты закрыта и/или заперта	Блокирование (предотвращение) автоматического функционирования дверей	Блокировать (предотвратить) операцию аварийный режим электроснабжения	Блокировать (предотвратить) операцию антипроскальзывание (только для гидравлики)	Блокировать (предотвратить) операцию ревизии на кабине	Блокировать (предотвратить) операцию доступа в шахту	Разрешен профиль скорости старт-стоп	Активизировать сигнализацию
34 Обнаружение непреднамеренного передвижения кабины с открытыми дверями	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
35 Контроль срабатывания защиты от непреднамеренного передвижения кабины с открытыми дверями	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
36 Контроль возврата буферов в нормальное выдвинутое положение	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
37 Контроль положения съемного штурвала	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
38 Контроль отключения лифта несамовозвратным устройством в машинном помещении	x	—	—	x	—	—	—	—	—	—	—	—	—	—	—	—	—
39 Контроль замедления в случае буферов с уменьшенным рабочим ходом	R13	—	—	—	—	x	—	—	—	—	—	—	—	—	—	—	—
40 Контроль выравнивания на этаже, повторного выравнивания и предварительных операций	x	—	R4	—	—	R2	—	—	R3	R3	—	—	—	—	—	—	—
41 Выключатель режима «Ревизия»	x	x	R11	—	—	R5	R12	—	—	—	—	x	x	x	x	x	—

Продолжение таблицы 2

Функции безопасности лифта	Связано с УПБ				Не связано с УПБ									
	Отключение питания с двигателя лебедки и тормоза (тяговые цепи), соответственно, с двигателя и/или задействованного клапана (клапанов) (цепи с гидравлическим приводом)	Блокирование (предотвращение) автоматического функционирования лифта (R26)	Ограничение длительности перемещения	Прерывание цепи питания катушки автоматического выключателя контактора	Операция перехода в режим ревизии	Ограничение скорости кабины	Ограничение движения кабины в направлении	Требуется ручной сброс	Игнорировать* проверки дверь кабины закрыта и/или заперта	Игнорировать* проверки дверь шахты закрыта и/или заперта	Блокирование (предотвращение) автоматического функционирования дверей	Блокировать (предотвратить) операцию аварийный режим электроснабжения	Блокировать (предотвратить) операцию антипроскальзывание (только для гидравлики)	Блокировать (предотвратить) операцию ревизии на кабине	Блокировать (предотвратить) операцию доступа в шахту	Разрешен профиль скорости старт-стоп	Активизировать сигнализацию
42 Контроль кнопок в сочетании с режимом «Ревизия»	x	x	R11	—	—	R5	R12	—	—	—	—	x	x	—	—	x	—
43 Выключатель аварийной электрической операции	R15	x	—	—	—	—	—	—	—	—	—	R16	x	—	—	x	—
44 Шунтирующее устройство для контактов дверей шахты и кабины	x	x	—	—	—	R8	—	R7	R9	R10	—	—	—	—	—	—	R25
45 Останавливающее устройство в режиме «Ревизия»	x	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
46 Останавливающее устройство в панели для эвакуации и испытаний	x	x	—	—	—	—	—	—	—	—	x	—	—	—	—	—	—
47 Контроль натяжения в устройстве для передачи положения кабины (предельные концевые выключатели)	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
48 Контроль натяжения в устройстве для передачи положения поршня (предельные концевые выключатели)	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
49 Предельные концевые выключатели	x	—	x	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Окончание таблицы 2

Примечание — В настоящей таблице приведены следующие обозначения:

- R1 — если после снятия с ловителей ограничитель скорости автоматически не сбрасывается, электрическое устройство безопасности должно предотвращать запуск лифта, пока ограничитель скорости не находится в положении сброса;
- R2 — скорость кабины ограничена максимальным выравниванием 0,8 м/с и максимальным повторным выравниванием 0,3 м/с;
- R3 — игнорирование контроля в зоне разблокировки целевой посадки;
- R4 — движение кабины ограничено только в пределах зоны разблокировки;
- R5 — скорость кабины не должна превышать 0,75 м/с;
- R6 — скорость кабины ограничена скоростью ревизии;
- R7 — активация и сброс осуществляются только вручную с помощью специального инструмента;
- R8 — скорость кабины не должна превышать 0,75 м/с, за исключением случаев пожарного режима;
- R9 — игнорирование контроля при включенном bypass двери кабины;
- R10 — игнорирование контроля при включенном bypass двери шахты;
- R11 — ограничение движения кабины в пределах конечного предела терминалов. Для гидравлических систем разрешено движение в направлении, превышающем нижний конечный предел;
- R12 — ограничение движения кабины в направлении, удаленном от конца терминала, где был достигнут конечный предел;
- R13 — контроль только при движении вниз;
- R14 — ограничение движения кабины в направлении вверх;
- R15 — при включении должно быть разрешено отключать его независимо или в составе группы:

а) средства контроля срабатывания ловителей (идентификационный номер 24);

б) средства контроля превышения скорости (идентификационные номера 25, 26);

в) средства контроля превышения скорости кабины при подъеме (идентификационный номер 33);

г) средства контроля неконтролируемого движения кабины (идентификационные номера 34, 35);

д) средства контроля выдвижения буфера (идентификационный номер 32);

е) средства контроля конечного предела (идентификационный номер 49);

- R16 — разрешается только одна аварийная электрическая операция. Любая разрешенная инспекционная операция должна иметь приоритет перед аварийной электрической операцией;
- R17 — во время предварительной операции и повторного выравнивания допускается игнорирование этой проверки;
- R18 — ручной сброс требуется только для гидравлических лифтов;
- R19 — игнорирование контроля, когда включена операция осмотра машинного помещения;
- R20 — игнорирование контроля, когда платформа и подвижные упоры находятся в полностью выдвинутом положении;
- R21 — игнорирование контроля только тогда, когда механическое предохранительное устройство полностью включено и включен режим «Ревизия» в приямке;
- R22 — игнорирование контроля только тогда, когда подвижные упоры полностью выдвинуты;
- R23 — игнорирование контроля только тогда, когда устройство находится в полностью убранном и отключенном положении;
- R24 — игнорирование контроля только в том случае, если включена операция осмотра в приямке и механическое устройство защиты полностью выдвинуто (идентификационный номер 10);
- R25 — включение на кабине звуковых и видимых сигналов;
- R26 — любой тип автоматического управления, включая одиночное, выборочное, групповое, аварийную пожарную службу, неотложную помощь в больнице, аварийное питание и т. д.

4.5 Требования к применению и проверке соответствия требованиям УПБ

4.5.1 Общие положения

Уровень целостности безопасности Э/ПЭ должен быть проверен в соответствии с требованиями настоящего раздела.

4.5.2 Необходимые меры для применения и проверки ПЭС соблюдения заданных уровней целостности безопасности

4.5.2.1 Меры, необходимые для применения и проверки соответствия с УПБ 1 до УПБ 3, удовлетворяются методами и средствами по приложению А.

4.5.2.2 Если две или более функции безопасности лифта реализованы с использованием общих цепей в цепи безопасности, уровень УПБ этих общих цепей должен быть по меньшей мере таким же высоким, как наивысший уровень квалификации функций безопасности лифта, включенных в эти цепи.

4.5.3 Потеря питания после срабатывания ПЭ

4.5.3.1 Если для функции не требуется ручной сброс, ПЭ должно быть разрешено вернуться к нормальному рабочему режиму после условия восстановления питания, а выходное состояние устройства должно определяться входными условиями, существующими после восстановления питания.

4.5.3.2 Если требуется ручной сброс (см. таблицу 2), выход ПЭ должен вернуться в исходное состояние непосредственно перед отключением питания.

Приложение А
(обязательное)

Меры по применению и проверке соответствия требованиям уровню полноты безопасности

А.1 Общие положения

В настоящем приложении рассматриваются меры по применению и проверке соответствия ПЭ УПБ.

А.1.1 Меры для удовлетворения требованиям УПБ

Меры, необходимые для внедрения и демонстрации соответствия ПЭ УПБ, должны быть выполнены путем:

а) конкретного применения мер, предусмотренных в А.2, или

б) применение мер, описанных в А.3, согласно ГОСТ Р МЭК 61508-2 и ГОСТ IEC 61508-3, и в руководстве по эксплуатации по А.1.2.

Изготовитель должен предоставить руководство по эксплуатации.

Если функциональная проверка лифта невозможна при нормальной эксплуатации лифта, в руководстве по эксплуатации должна быть указана информация, позволяющая провести функциональную проверку.

Руководство по эксплуатации также должно содержать информацию о следующих действиях, чтобы их можно было выполнять эффективно и без опасности:

- сборка;
- подключение;
- регулировка;
- техническое обслуживание и ремонт;
- идентификация, маркировка, наклеивание этикеток;
- периодичность функциональной проверки.

А.1.2 Общие требования к руководству по эксплуатации по техническому обслуживанию и ремонту

Руководство по эксплуатации должно содержать:

- требования и/или меры предосторожности для обучения обслуживающего персонала поддержанию полной функциональной работоспособности ПЭ в соответствии с его УПБ;
- контрольные испытания, профилактические работы и мероприятия по техническому обслуживанию после поломки;
- меры, используемые для технического обслуживания;
- требования к проверке и документации для соблюдения мероприятий по техническому обслуживанию;
- временны́е интервалы проведения работ по техническому обслуживанию;
- обеспечение надлежащей калибровки и технического обслуживания испытательного оборудования, используемого во время работ по техническому обслуживанию;
- необходимые мероприятия по техническому обслуживанию и ремонту при возникновении неисправностей в ПЭ, включая:
  - мероприятия по диагностике и ремонту неисправностей,
  - мероприятия по повторной валидации,
  - требования к техническому обслуживанию и отчетности об отказах.

А.1.3 Требования к конструкции для технического обслуживания или ремонтопригодности

Конструкция ПЭ должна допускать проведение испытаний как комплексных, так и частичных.

К комплексным относятся испытания от конца датчика до срабатывания в безопасном состоянии.

Если ожидаемый интервал между запланированными испытаниями превышает интервал пробных испытаний, используемый для поддержания рейтинга УПБ ПЭ, то требуются соответствующие условия для тестирования. Когда требуется автоматическое контрольное тестирование, неотъемлемой частью конструкции, рассчитанной на уровень УПБ, должны быть предусмотрены условия для тестирования на наличие необнаруженных отказов.

А.2 Меры по применению и проверке соответствия требованиям УПБ

А.2.1 Общие положения

Для ПЭС, спроектированных в соответствии с настоящим приложением, дополнительная оценка последствий сочетания двух или более неисправностей не требуется.

Минимальные требования к функциям безопасности, общим для всех УПБ, перечислены в таблицах А.1—А.3. Кроме того, конкретные меры, требуемые для УПБ 1, 2 и 3, перечислены, соответственно, в таблицах А.4—А.6.

Примечание — Положения ГОСТ Р МЭК 61508-7, перечисленные в таблицах А.1—А.6, относятся к соответствующим требованиям ГОСТ Р МЭК 61508-2 и ГОСТ IEC 61508-3.

А.2.2 Требования к оборудованию

А.2.2.1 Печатная плата

Короткое замыкание может быть исключено при условии, что:

- общие технические характеристики печатной платы соответствуют ГОСТ Р 55490;

- материал основы соответствует спецификациям ГОСТ Р МЭК 61249-2-2;

- печатная плата изготовлена в соответствии с вышеуказанными требованиями, а минимальные значения приведены в ГОСТ Р МЭК 60664.1 при следующих условиях:

  - степень загрязнения — 3;
  - группа материала — III;
  - поле неоднородно.

Столбец «Материал для печатных плат» таблицы F.4 ГОСТ Р МЭК 60664.1—2012 не используется. Это означает, что расстояние утечки составляет 4 мм, а зазор — 3 мм при 250 Vrms.

Если степень защиты печатной платы IP5X или выше, или используемый материал более высокого качества, расстояние утечки может быть уменьшено до значения зазора, например 3 мм при 250 Vrms.

Для многослойных плат, состоящих по меньшей мере из трех препрегов или других тонких листовых изоляционных материалов, короткое замыкание может быть исключено.

А.2.2.2 Совместно используемое оборудование

Если ПЭ и система, не связанная с безопасностью, используют одну и ту же печатную плату, для разделения двух систем должно применяться следующее:

- если степень защиты равна IP4X или ниже, зазоры должны составлять не менее 3 мм, а расстояние утечки — не менее 4 мм;

- если степень защиты выше IP4X, расстояние утечки может быть уменьшено до 3 мм. Если ПЭС, не связанная с безопасностью, использует одно и то же оборудование, связанное с устройствами безопасности, то должны выполняться требования к ПЭ.

А.2.2.3 Другие требования

Общие меры по предотвращению и обнаружению сбоев, связанных с аппаратным обеспечением, приведены в таблице А.1.

Таблица А.1 — Общие меры по предотвращению и обнаружению сбоев, связанных с аппаратным обеспечением

Объект	Действие	Структурный элемент ГОСТ Р МЭК 61508-7—2012
1 Процессор	Использование сторожевого таймера	А.9
2 Выбор компонентов	Использование компонентов только в соответствии с их спецификациями	—
3 Устройства ввода-вывода и интерфейсы, включая каналы связи	Заданное безопасное состояние в случае сбоя питания или сброса	—
4 Питание	Заданное безопасное отключение источника питания в случае перенапряжения или понижения напряжения	А.8.2
5 Оперативная память	Использование только твердотельных запоминающих устройств	—
	Проверка чтения/записи памяти переменных данных во время процедуры загрузки	—
	Удаленный доступ только к информативным данным (например, статистике)	—
6 Память программы	Нет возможности изменять программный код либо автоматически системой, либо удаленным вмешательством	—
	Проверка памяти программного кода и памяти фиксированных данных во время процедуры загрузки методом, по меньшей мере (контрольная сумма)	А.4.2

А.2.3 Требования к программному обеспечению

Общие меры по предотвращению и обнаружению сбоев, связанных с разработкой программного обеспечения, приведены в таблице А.2.

Таблица А.2 — Общие меры по предотвращению и обнаружению сбоев, связанных с разработкой программного обеспечения

Объект	Действие	Структурный элемент ГОСТ Р МЭК 61508-7—2012
1 Структура	Структура программы (т. е. модульность, обработка данных, определение интерфейса) в соответствии с современным уровнем техники (см. ГОСТ IEC 61508-3)	B.3.4, C.2.1, C.2.9, C.2.7
2 Процедура загрузки	Во время процедур загрузки необходимо поддерживать безопасное состояние лифта	—
3 Прерывание	Ограниченное использование прерываний; использование вложенных прерываний только в том случае, если все возможные последовательности прерываний предсказуемы	C.2.6.5
	Не запускается сторожевой таймер процедурой прерывания, за исключением случаев, когда это происходит в сочетании с другими условиями последовательности выполнения программы	A.9.4
4 Отключение питания	Процедуры отключения питания, такие как сохранение данных, для функций, связанных с безопасностью, не требуются	A.8.3
5 Управление памятью	Менеджер стека в аппаратном и/или программном обеспечении с соответствующей процедурой реагирования	C.2.6.4, C.5.4
6 Программа	Циклы итерации короче времени реакции системы, например, за счет ограничения количества циклов или проверки времени выполнения	—
	Проверка смещения указателя массива, если оно не включено в используемый язык программирования	C.2.6.6
	Определенная обработка исключений (например, деление на ноль, переполнение, проверка диапазона переменных и т. д.), которая переводит систему в определенное безопасное состояние	—
	Не допускается рекурсивное программирование, за исключением хорошо зарекомендовавших себя стандартных библиотек, одобренных операционных систем или компиляторов языков высокого уровня. Для этих исключений должны быть предусмотрены отдельные стеки для отдельных задач, которые должны контролироваться модулем управления памятью	C.2.6.7
	Документация по интерфейсам библиотек программирования и операционным системам, по крайней мере, такая же полная, как и сама пользовательская программа	—
	Проверка достоверности данных, относящихся к функциям безопасности, например, шаблонов ввода, диапазонов ввода, внутренних данных	C.2.5, C.3.1
	Если для целей тестирования или валидации может быть задействован какой-либо режим работы, нормальная работа лифта должна быть невозможна до тех пор, пока этот режим не будет отключен	См. ГОСТ Р МЭК 61508-1—2012, подпункт 7.7.2.1
7 Система связи (внешняя и внутренняя)	Достижение безопасного состояния с должным учетом времени реакции системы в системе шин связи с функциями безопасности в случае потери связи или неисправности в участнике шины	A.7, A.9
8 Система шины	Не допускается реконфигурация системы CPU-bus, за исключением процедур загрузки. Примечание — Периодическое обновление системы CPU-bus не рассматривается как реконфигурация.	C.3.10

Окончание таблицы А.2

Объект	Действие	Структурный элемент ГОСТ Р МЭК 61508-7—2012
9 Обработка ввода-вывода	Не допускается реконфигурация линий ввода-вывода, за исключением процедур загрузки. Примечание — Периодическое обновление регистров конфигурации ввода-вывода не рассматривается как реконфигурация.	С.3.10

А.2.4 Требования к разработке и применению

Общие меры, относящиеся к разработке и применению, приведены в таблице А.3.

Таблица А.3 — Общие меры, относящиеся в разработке и применению

Действие	Структурный элемент ГОСТ Р МЭК 61508-7—2012
1 Оценка функциональных, экологических и интерфейсных аспектов применения	А.14, В.1
2 Техническое задание, включая требования безопасности	В.2.1
3 Обзоры всех технических характеристик	—
4 Проектная документация в соответствии с требованиями А.2.6.2, включая: - описание функций, включая архитектуру системы и взаимодействие аппаратного и программного обеспечения; - документация по программному обеспечению, включая описание функций и последовательности выполнения программы	С.5.9
5 Отчеты об обзоре проекта	В.3.7, В.3.8, С.5.16
6 Проверка надежности с использованием такого метода, как анализ режима отказа и последствий (FMEA)	В.6.6
7 Спецификация испытаний производителя, протоколы испытаний производителя и отчеты о полевых испытаниях	В.6.1
8 Документы с инструкциями, включая ограничения по использованию по назначению	В.4.1
9 Повторение и обновление вышеупомянутых мер, если продукт модифицирован	С.5.23
10 Реализация контроля версий аппаратного и программного обеспечения и его совместимости	С.5.24

А.2.5 Конкретные меры, относящиеся к категории УПБ

А.2.5.1 Конкретные меры для УПБ1 приведены в таблице А.4.

Таблица А.4 — Конкретные меры для УПБ 1

Компоненты объекта и функции	Требования[1)]	Действия	Номер пункта таблицы А.7 настоящего стандарта	Структурный элемент ГОСТ Р МЭК 61508- 7—2012
Структура	Структура должна быть такой, чтобы обнаруживался любой единичный случайный сбой, и система переходила в безопасное состояние	Одноканальная структура с самотестированием или два канала или более со сравнением	М.1.1, М.1.3	А.3.1, А.2.5

Окончание таблицы А.4

Компоненты объекта и функции	Требования[1)]	Действия	Номер пункта таблицы А.7 настоящего стандарта	Структурный элемент ГОСТ Р МЭК 61508- 7—2012
Обрабатывающие узлы	Должны быть обнаружены сбои в процессорах, которые могут привести к неправильным результатам. Если такой сбой может привести к опасной ситуации, система должна перейти в безопасное состояние	Аппаратное обеспечение для устранения сбоев, или самотестирование с помощью программного обеспечения, или компаратор для двухканальной структуры, или обратное сравнение с помощью программного обеспечения для двухканальной структуры	М.2.1, М.2.2, М.2.4, М.2.5	А.3.4, А.3.1, А.1.3, А.3.5
Инвариантные диапазоны памяти	Некорректное изменение информации, т. е. все нечетные или двухразрядные сбои и некоторые трехразрядные и многоразрядные сбои должны быть обнаружены не позднее следующего перемещения лифта	Следующие меры относятся только к одноканальной структуре: одноразрядная избыточность (бит четности) или безопасность блока с избыточностью в одно слово	М.3.5, М.3.1	А.5.5, А.4.3
Переменные диапазоны памяти	Глобальные сбои при адресации, записи, сохранении и считывании, а также все нечетные и двухразрядные сбои и некоторые трехразрядные сбои и многоразрядные сбои должны быть обнаружены не позднее следующего перемещения лифта	Следующие меры относятся только к одноканальной структуре: сохранение слов с многоразрядной избыточностью или проверка с помощью тестового шаблона на наличие статических или динамических сбоев	М.3.2, М.4.1	А.5.6, А.5.2
Блоки ввода-вывода и интерфейсы, включая, каналы связи	Статические сбои и перекрестные помехи на линиях ввода-вывода, а также случайные и систематические сбои в потоке данных должны быть обнаружены не позднее следующего перемещения лифта	Безопасность кода или тестовый шаблон	М.5.4, М.5.5	А.6.2, А.6.1
Часы	Сбои в генерации тактовых импульсов для процессорных блоков, такие как изменение частоты или поломка, должны быть обнаружены не позднее следующего перемещения лифта	Сторожевой таймер с отдельной временной базой или взаимный мониторинг	М.6.1, М.6.2	А.3.5, А.9.1, А.9.2
Последовательность выполнения программы	Неправильная последовательность выполнения программы и неподходящее время выполнения функций, связанных с безопасностью, должны быть обнаружены не позднее следующего перемещения лифта	Сочетание синхронизации и логического контроля последовательности выполнения программы	М.7.1	А.9.4

[1)] В результате обнаружения неисправности должно поддерживаться безопасное состояние лифта.

А.2.5.2 Конкретные меры для УПБ2 приведены в таблице А.5.

Таблица А.5 — Конкретные меры для УПБ2

Компоненты объекта и функции	Требования[1)]	Действия	Номер пункта таблицы А.7 настоящего стандарта	Структурный элемент ГОСТ Р МЭК 61508-7—2012
Структура	Структура должна быть такой, чтобы любой единичный случайный сбой обнаруживался с должным учетом времени реакции системы, и чтобы система переходила в безопасное состояние	Один канал с самотестированием и мониторингом, или два канала или более со сравнением	М.1.2, М.1.3	А.3.3, А.2.5
Обрабатывающие узлы	Сбои в процессорах, которые могут привести к неправильным результатам, должны выявляться с должным учетом времени реакции системы. Если такой сбой может привести к опасной ситуации, система должна перейти в безопасное состояние	Аппаратная коррекция сбоев и самотестирование программного обеспечения, поддерживаемое аппаратным обеспечением для одноканальной структуры, или компаратором для двухканальной структуры, или обратное сравнение программным обеспечением для двухканальной структуры	М.2.1, М.2.3, М.2.4, М.2.5	А.3.4, А.3.3, А.1.3, А.3.5
Инвариантные диапазоны памяти	Некорректное изменение информации, т. е. все нечетные или двухразрядные сбои, а также некоторые трехразрядные и многоразрядные сбои, должны быть обнаружены с учетом времени реакции системы	Следующие меры относятся только к одноканальной структуре: защита блоков с избыточностью в одно слово или сохранение слов с многоразрядной избыточностью	М.3.1, М.3.2	А.4.3, А.5.6
Переменные диапазоны памяти	Глобальные сбои при адресации, записи, сохранении и чтении, а также все нечетные и двухразрядные сбои и некоторые трехразрядные сбои и многоразрядные сбои должны обнаруживаться с учетом времени реакции системы	Следующие меры относятся только к одноканальной структуре: сохранение слов с многоразрядной избыточностью или проверка с помощью тестового шаблона на наличие статических или динамических сбоев	М.3.2, М.4.1	А.5.6, А.5.2
Блоки ввода-вывода и интерфейсы, включая, каналы связи	Статические сбои и перекрестные помехи на линиях ввода-вывода, а также случайные и систематические сбои в потоке данных должны обнаруживаться с учетом времени реакции системы[2)]	Безопасность кода или тестовый шаблон	М.5.4, М.5.5	А.6.2, А.6.1
Часы	Сбои в генерации тактовых импульсов для процессорных блоков, такие как изменение частоты или выход из строя, должны обнаруживаться с учетом времени реакции системы	Сторожевой таймер с отдельной временной базой или взаимный мониторинг	М.6.1, М.6.2	А.3.5, А.9.1, А.9.2

Окончание таблицы А.5

Компоненты объекта и функции	Требования[1)]	Действия	Номер пункта таблицы А.7 настоящего стандарта	Структурный элемент ГОСТ Р МЭК 61508-7—2012
Последовательность выполнения программы	Неправильная последовательность программ и неподходящее время выполнения функции безопасности должны быть обнаружены с учетом времени реакции системы	Сочетание синхронизации и логического контроля последовательности выполнения программы	М.7.1	А.9.4

[1)] В результате обнаружения неисправности должно поддерживаться безопасное состояние лифта.
[2)] Не относится к активаторам, таким как реле безопасности или эквивалентные электронные средства, например, в цепи безопасности.

А.2.5.3 Конкретные меры для УПБ 3 приведены в таблице А.6.

Таблица А.6 — Конкретные меры для УПБ 3

Компоненты объекта и функции	Требования[1)]	Действия	Номер пункта таблицы А.7 настоящего стандарта	Структурный элемент ГОСТ Р МЭК 61508-7—2012
Структура	Структура должна быть такой, чтобы любой единичный случайный сбой обнаруживался с учетом времени реакции системы, и чтобы затем система переходила в безопасное состояние	Два канала или более со сравнением	М.1.3	А.2.5
Обрабатывающие узлы	Сбои в процессорах, которые могут привести к неправильным результатам, должны выявляться с учетом времени реакции системы. Если такой сбой может привести к опасной ситуации, система должна перейти в безопасное состояние	Компаратор для двух каналов или обратное сравнение с помощью программного обеспечения для двухканальной структуры	М.2.4, М.2.5	А.1.3, А.3.5
Инвариантные диапазоны памяти	Некорректное изменение информации, т. е. все одноразрядные или многоразрядные сбои, должны обнаруживаться с учетом времени реакции системы	Процедура защиты блока с репликацией блока или защита блока с многословной избыточностью	М.3.3, М.3.4	А.4.5, А.4.4
Переменные диапазоны памяти	Глобальные сбои при адресации, записи, хранении и чтении, а также сбои статических битов и динамические соединения должны обнаруживаться с учетом времени реакции системы	Процедура обеспечения безопасности блоков с репликацией блоков или инспекционными проверками	М.4.2, М.4.3	А.5.7, А.5.3
Блоки ввода-вывода и интерфейсы, включая, каналы связи	Статические сбои и перекрестные помехи на линиях ввода-вывода, а также случайные и систематические сбои в потоке данных должны обнаруживаться с учетом времени реакции системы[2)]	Многоканальный параллельный ввод и многоканальный параллельный вывод, или обратное считывание выходных данных, или безопасность кода, или тестовый шаблон	М.5.1, М.5.3, М.5.2, М.5.4, М.5.5	А.6.5, А.6.3, А.6.4, А.6.2, А.6.1

Окончание таблицы А.6

Компоненты объекта и функции	Требования[1)]	Действия	Номер пункта таблицы А.7 настоящего стандарта	Структурный элемент ГОСТ Р МЭК 61508-7—2012
Часы	Сбои в генерации тактовых импульсов для процессорных блоков, такие как изменение частоты или выход из строя, должны обнаруживаться с учетом времени реакции системы	Сторожевой таймер с отдельной временной базой или взаимный мониторинг	М.6.1, М.6.2	А.3.5, А.9.1, А.9.2
Последовательность выполнения программы	Неправильная последовательность выполнения программы и неподходящее время выполнения функции безопасности должны быть обнаружены с учетом времени реакции системы	Сочетание синхронизации и логического контроля последовательности выполнения программы	М.7.1	А.9.4

[1)] В результате обнаружения неисправности должно поддерживаться безопасное состояние лифта.
[2)] Это не относится к активаторам, таким как реле безопасности или эквивалентные электронные средства, например, в цепи безопасности.

А.2.6 Процедуры испытаний для подтверждения соответствия

А.2.6.1 Общие положения

Подтверждение соответствия изделия требованиям настоящего стандарта осуществляется по результатам проведения испытаний и измерений.

А.2.6.2 Положения для печатных плат или эквивалентных сборок

Заявитель должен указать лаборатории:

а) идентификацию платы/узла;

б) условия работы;

в) перечень используемых компонентов;

г) расположение печатной платы/узла;

д) расположение гибридов и меток дорожек, используемых в цепях безопасности;

е) описание функций;

ж) электрические данные, включая схему подключения, если применимо, с определениями входных и выходных параметров платы/узла;

и) документы и описания, относящиеся к мерам, перечисленным в таблице А.3;

к) общее описание используемого программного обеспечения (например, правила программирования, язык);

л) описание функций, взаимодействие аппаратного и программного обеспечения;

м) описание блоков, модулей, данных, переменных и интерфейсов.

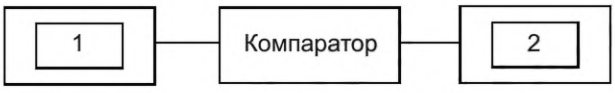
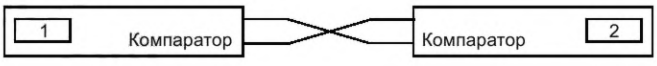
А.2.7 Описание возможных мер

Описание возможных мер по контролю отказов приведено в таблице А.7.

Таблица А.7 — Описание возможных мер по контролю отказов

Компоненты объекта и функции	Номер пункта	Описание действий
Структура	М.1.1	Одноканальная структура с самотестированием Описание: несмотря на то, что структура состоит из одного канала, должны быть предусмотрены резервные выходные пути для обеспечения безопасного отключения. Самотестирование (циклическое) применяется к подразделениям PESSRAL с интервалами времени, которые могут зависеть от применения. Эти тесты (например, тесты процессора или памяти) предназначены для обнаружения скрытых сбоев, которые не зависят от потока данных. Обнаруженный сбой должен привести к переходу системы в безопасное состояние

Продолжение таблицы А.7

Компоненты объекта и функции	Номер пункта	Описание действий
Структура	М.1.2	Одноканальная структура с самотестированием и мониторингом Описание: одноканальная структура с самотестированием и мониторингом состоит из отдельного блока аппаратного мониторинга, который, независимо от применения, периодически получает тестовые данные из системы, которые могут быть получены в результате процедур самотестирования. В случае неверных данных система должна перейти в безопасное состояние. Необходимы по крайней мере два независимых пути отключения, чтобы отключение могло быть вызвано либо самим процессором, либо блоком мониторинга
	М.1.3	Два или более каналов со сравнением Описание: двухканальная конструкция, связанная с безопасностью, состоит из двух независимых функциональных блоков без обратной связи. Это позволяет выполнять указанные функции независимо в каждом канале. Для двухканального PESSRAL, предназначенного исключительно для функции одного предохранительного устройства, конструкция каналов может быть идентичной с точки зрения аппаратного и программного обеспечения. При использовании двухканального PESSRAL для сложных решений (например, комбинаций нескольких функций безопасности) и там, где процессы или условия не поддаются однозначной проверке, следует учитывать разнообразие аппаратного и программного обеспечения. Структура включает в себя функцию, которая сравнивает внутренние сигналы (например, сравнение шин) и/или выходные сигналы, имеющие отношение к функциям безопасности, чтобы помочь в обнаружении неисправностей. Необходимы по меньшей мере два независимых канала отключения, чтобы отключение могло быть вызвано либо самими каналами, либо компаратором. Это необходимо, чтобы само сравнение также было подвержено распознаванию ошибок
Обрабатывающие устройства	М.2.1	Аппаратное обеспечение, исправляющее сбои Описание: такие устройства могут быть реализованы с использованием специальных схем распознавания отказов или их коррекции. Эти методы известны для простых конструкций
	М.2.2	Самотестирование с помощью программного обеспечения Описание: все функции процессора, которые используются в приложениях, связанных с безопасностью, должны проверяться циклически. Эти тесты могут быть объединены с тестированием подкомпонентов, например памяти, ввода-вывода и т. д.
	М.2.3	Самотестирование программного обеспечения, поддерживаемое аппаратным обеспечением Описание: для обнаружения сбоев используется специальное аппаратное обеспечение, поддерживающее функции самотестирования, например блок мониторинга, который проверяет периодический вывод определенных битовых комбинаций
	М.2.4	Компаратор (сравниватель) для двухканальных структур  Описание: два канала с аппаратным компаратором: а) сигналы обоих процессорных блоков сравниваются с помощью аппаратного блока циклически или непрерывно. Компаратор может быть блоком внешнего тестирования или сконструирован как устройство самоконтроля, или б) сигналы обоих каналов сравниваются с помощью блока обработки. Компаратор может быть блоком внешнего тестирования или сконструирован как устройство самоконтроля
	М.2.5	Взаимное сравнение двух каналов  Описание: используются два резервных блока обработки, которые взаимно обмениваются данными, относящимися к безопасности. Сравнение данных выполняется каждым блоком

Продолжение таблицы А.7

Компоненты объекта и функции	Номер пункта	Описание действий
Неизменяемые диапазоны памяти (ROM, EPROM...)	М.3.1	Процедура блокировки с избыточностью в одно слово (например, формирование подписи через ROM шириной в одно слово) Описание: в этом тесте содержимое ROM сжимается по определенному алгоритму по крайней мере до одного слова в памяти. Алгоритм, например циклическая проверка избыточности (CRC), может быть реализован с использованием аппаратного или программного обеспечения
Неизменяемые диапазоны памяти (ROM, EPROM...)	М.3.2	Сохранение слов с многоразрядной избыточностью (например, модифицированный код Хэмминга) Описание: каждое слово памяти расширяется на несколько избыточных битов для получения модифицированного кода Хэмминга с расстоянием Хэмминга не менее четырех. Каждый раз, когда читается слово, можно определить, имело ли место повреждение, проверяя избыточные биты. Если обнаружено различие, необходимо, чтобы система перешла в безопасное состояние
	М.3.3	Процедура обеспечения безопасности блоков с репликацией блоков Описание: адресное пространство оборудовано двумя запоминающими устройствами. Первое запоминающее устройство работает обычным образом. Второе запоминающее устройство содержит ту же информацию, и доступ к нему осуществляется параллельно с первым. Выходные данные сравниваются, и при обнаружении разницы предполагается сбой. Для обнаружения определенных видов битовых ошибок данные должны храниться в обратном порядке в одном из двух запоминающих устройств и повторно инвертироваться при считывании. В программной процедуре содержимое обеих областей памяти циклически сравнивается с помощью программы
	М.3.4	Блочно-безопасная процедура с многословной избыточностью Описание: эта процедура вычисляет подпись с использованием алгоритма CRC, но результирующее значение имеет размер не менее двух слов. Расширенная подпись сохраняется, пересчитывается и сравнивается, как в случае с одним словом. При возникновении разницы выдается сообщение об ошибке
Неизменяемые диапазоны памяти (ROM, EPROM...)	М.3.5	Избыточность в один бит, сохраняющая слово (например, мониторинг ROM с битом четности) Описание: каждое слово в памяти расширяется на один бит (бит «четности»), который завершает каждое слово четным или нечетным числом логических единиц. Четность слова данных проверяется при каждом его считывании. Если найдено неправильное число 1, выдается сообщение об ошибке. Выбор четной или нечетной четности должен быть сделан таким образом, чтобы в случае сбоя любое из нулевых слов (ничего, кроме 0s) и одного слова (ничего, кроме 1s) было более неблагоприятным, тогда слово не является допустимым кодом. Проверка четности также может использоваться для обнаружения сбоя адресации, когда проверка четности вычисляется для объединения слова данных и его адреса
Переменные диапазоны памяти	М.4.1	Проверка с помощью тестового шаблона наличия статических или динамических неисправностей, например тест оперативной памяти «дорожка обхода» Описание: тестируемый диапазон памяти инициализируется однородным потоком битов. Затем первая ячейка инвертируется, а оставшаяся область памяти проверяется, чтобы убедиться в правильности фона. После этого первая ячейка повторно инвертируется, чтобы вернуться к исходному значению, и весь процесс повторяется для следующей. Выполняется второй запуск «модели блуждающего бита» с обратным предварительным назначением фона. Если возникает разница, необходимо, чтобы система перешла в безопасное состояние

Продолжение таблицы А.7

Компоненты объекта и функции	Номер пункта	Описание действий
Переменные диапазоны памяти	М.4.2	Процедуры обеспечения безопасности блоков при репликации блоков, например двойная оперативная память с аппаратным или программным сравнением Описание: адресное пространство оборудовано двумя запоминающими устройствами. Первое запоминающее устройство работает обычным образом. Второе запоминающее устройство содержит ту же информацию, и доступ к нему осуществляется параллельно с первым. Выходные данные сравниваются, и при обнаружении разницы предполагается сбой. Для обнаружения определенных видов битовых ошибок данные должны быть сохранены в обратном порядке в одном из двух запоминающих устройств и снова инвертированы при считывании. В процедуре программного обеспечения данные должны быть сохранены в обратном порядке в одном из двух запоминающих устройств. Содержимое обеих областей памяти циклически сравнивается с помощью программы
Переменные диапазоны памяти	М.4.3	Проверка на наличие статических и динамических неисправностей, например GALPAT Описание: а) тест оперативной памяти GALPAT: обратный элемент записывается в стандартную предварительно назначенную память, а затем проверяются все оставшиеся ячейки, чтобы убедиться в правильности их содержимого. После каждого доступа для чтения к одной из оставшихся ячеек в дополнение к этому также проверяется и считывается обратно описанная ячейка. Этот процесс повторяется для каждой ячейки. Выполняется второй запуск с обратным предварительным назначением. Предполагается сбой, если есть разница, или б) прозрачный тест GALPAT: в начале теста с помощью программного или аппаратного обеспечения формируется подпись относительно содержимого тестируемого диапазона памяти, и это сохраняется в регистре. Это соответствует предварительному назначению памяти в тесте GALPAT. Содержимое теперь записывается в тестовую ячейку перевернутым образом и проверяется содержимое остальных ячеек. Содержимое тестовой ячейки также считывается после каждого обращения для чтения к одной из этих ячеек. Поскольку содержимое остальных ячеек действительно неизвестно, их содержимое проверяется не по отдельности, а путем повторного формирования подписи. После этого первого запуска для первой ячейки выполняется второй запуск для этой ячейки с содержимым, которое было инвертировано несколько раз: т. е. содержимое, которое снова является реальным. Таким образом, восстанавливается исходное содержимое памяти. Все остальные ячейки памяти тестируются таким же образом. Предполагается сбой, если есть разница
Блоки ввода-вывода и интерфейсы	М.5.1	Многоканальный параллельный вход Описание: это зависящее от потока данных сравнение независимых входных данных, соответствующих определенной области допуска (значению времени)
	М.5.2	Обратное считывание выходных данных (контролируемый выходной сигнал) Описание: это зависящее от потока данных сравнение выходных данных с независимыми входными данными, соответствующими определенной области допусков (время, значение). Сбой не всегда может быть связан с дефектным выходным сигналом
	М.5.3	Многоканальный параллельный выход Описание: это избыточность выходных данных, зависящая от потока данных. Распознавание сбоев происходит непосредственно в рамках технического процесса или с помощью внешних компараторов
	М.5.4	Безопасность кода Описание: эта процедура защищает входную и выходную информацию в отношении совпадающих сбоев и систематических сбоев. Она обеспечивает распознавание сбоев в блоках ввода и вывода в зависимости от потока данных с информационной избыточностью и/или временной избыточностью

Окончание таблицы А.7

Компоненты объекта и функции	Номер пункта	Описание действий
Блоки ввода-вывода и интерфейсы	М.5.5	Тестовый образец (модель) Описание: это независимое от потока данных циклическое тестирование входных и выходных блоков, выполняемое с помощью определенной схемы тестирования для сравнения наблюдений с соответствующими ожидаемыми значениями. Информация о шаблоне тестирования, прием шаблона тестирования и оценка шаблона тестирования должны быть независимы друг от друга. Следует предположить, что протестированы все возможные входные шаблоны
Часы	М.6.1	Сторожевой таймер с отдельной временной базой Описание: аппаратный таймер с отдельной временной базой срабатывает при правильной работе программы
	М.6.2	Взаимный мониторинг Описание: аппаратный таймер с отдельной временной базой запускается при правильной работе программы другого процессора
Последовательность выполнения программы	М.7.1	Сочетание синхронизации и логического контроля последовательности выполнения программы Описание: средство, отслеживающее последовательность выполнения программы по времени, повторно запускается только в том случае, если последовательность разделов программы выполнена правильно

А.3 Меры по применению и проверке соответствия УПБ согласно ГОСТ Р МЭК 61508-2 и ГОСТ IEC 61508-3

А.3.1 Общие требования

А.3.1.1 Для целей настоящего стандарта УПБ представляет требования к устройству, работающему в режиме низкой нагрузки, и вероятность невыполнения его функции безопасности по требованию (см. ГОСТ Р МЭК 61508-1—2012, таблица 2).

Однако там, где ПЭ используется для постоянного контроля за поддержанием функциональной безопасности, УПБ должен соответствовать требованиям к ПЭ, который считается работающим в режиме повышенной нагрузки, и должна использоваться частота опасных отказов (см. ГОСТ Р МЭК 61508-1—2012, таблица 3).

Когда существует вероятность того, что некоторая комбинация выходных состояний подсистемы может непосредственно вызвать опасное событие, тогда необходимо рассматривать обнаружение опасных неисправностей в подсистеме как функцию безопасности, работающую в непрерывном режиме.

А.3.1.2 Устройства и программное обеспечение, используемые для выполнения требований, не соответствующих нормам УПБ, не должны использоваться для реализации УПБ соответствующих требований к ПЭ, если только эти устройства и программное обеспечение также не были включены в рейтинг УПБ для функций, связанных с безопасностью.

А.3.1.3 Обнаружение опасной неисправности (с помощью диагностических тестов, контрольных испытаний или другими способами) в любой подсистеме ПЭ, которая может выдержать однократную неисправность, должна привести к указанному в таблице 2 безопасному состоянию. При необходимости для сохранения целостности ПЭ и поддержания безопасного состояния до возникновения второй неисправности в той же подсистеме, которая может привести к опасному состоянию, должен быть выполнен ручной сброс для вывода ПЭ из безопасного состояния. Если вышеуказанные действия зависят от оператора или удаленной подсистемы, предпринимающих конкретные действия в ответ на сигнал тревоги об опасной неисправности, то сигнал тревоги должен рассматриваться как часть соответствующей УПБ функции ПЭ.

А.3.2 Применение и соответствие требованиям УПБ

Применение и соответствие требованиям УПБ для ПЭ должно осуществляться в соответствии с руководящими принципами и мерами ГОСТ Р МЭК 61508-2 для аппаратного обеспечения и ГОСТ IEC 61508-3 для программного обеспечения.

Смотрите также ГОСТ Р МЭК 61508-7, в котором содержится обзор различных методов и мер безопасности, относящихся к ГОСТ Р МЭК 61508-2 и ГОСТ IEC 61508-3.

Примечание — Возможно использование нескольких систем с более низким уровнем целостности безопасности для удовлетворения потребности в функции с более высоким уровнем целостности безопасности при условии достижения надлежащего уровня независимости и того, что они сертифицированы для данного применения.

Приложение Б
(справочное)

Пример таблицы принятия решений по снижению риска

Пример таблицы принятия решений по снижению риска для применения ПЭ и соответствующие корректирующие действия приведены в таблице Б.1.

Потенциальные последствия подразделяют следующим образом:

а) катастрофические — полная потеря цели обеспечения безопасности в рамках настоящего стандарта;

б) критические — постоянная частичная потеря цели обеспечения безопасности в рамках настоящего стандарта;

в) предельные — временная потеря цели обеспечения безопасности в рамках настоящего стандарта;

г) незначительные — незначительная потеря цели обеспечения безопасности или ее отсутствие в рамках настоящего стандарта.

Таблица Б.1 — Таблица принятия решений по снижению риска

Частота последствий F в год на единицу (лифт)		Потенциальное последствие для безопасности			
Диапазон	Среднее значение	Катастрофическое	Критическое	Предельное	Незначительное
1 E-3 ≤ FI	>0,5 E-2	IA	IA	IA	IIIA
1 E-4 ≤ FI < 1 E-3	0,5 E-3	IB	IB	IIB	IIIB
1 E-5 ≤ FI < 1 E-4	0,5 E-4	IC	IIC	IIIC	IVC
1 E-5 ≤ FI < 1 E-5	0,5 E-5	IID	IIID	IIID	IVD
1 E-5 ≤ FI < 1 E-6	0,5 E-6	IIIE	IIIE	IVE	IVE
FI < 1 E-7	< 0,5 E-7	< 0,5 E-7	Не используется	Не используется	Не используется

Примечания

1) IA, IB, IC, IIB, IIIA — корректирующие действия, необходимые для смягчения воздействия и, если это практически возможно, устранения его;
2) IIC, IIIB — корректирующие действия, необходимые для смягчения последствий;
3) IID, IIIC, IIID — анализ и определение, возможно ли технически какое-либо дальнейшее смягчение последствий;
4) IIIE, IVC, IVD, IVE — никаких действий не требуется.

УДК 692.66:006.354 ОКС 91.140.90

Ключевые слова: лифты, электронные и программируемые системы, применяемые в цепях безопасности

Редактор *Е.В. Якубова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 17.09.2025. Подписано в печать 30.09.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,35.

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