ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 14762— 2013

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Требования к функциональной безопасности электронных систем домов и зданий (ЭСДЗ)

ISO/IEC 14762:2009

Information technology – Functional safety requirements for home and building electronic systems (HBES)
(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации – «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода стандар-та, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 58 «Функциональная безопасность»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2013 г. № 1311-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 14762:2009 «Информационные технологии. Требования к функциональной безопасно-сти электронных систем домов и зданий (ЭСДЗ)» (IEC/ISO 14762:2009 «Information technology – Functional safety requirements for home and building electronic systems (HBES)», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 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.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть 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, определения и сокращения 2
4 Соответствие настоящему стандарту 4
5 Общие требования 4
6. Требования к функциональной безопасности 5
Приложение А (справочное) Пример метода определения уровней полноты безопасности 11
Приложение В (справочное) Опасности и разработка необходимых требований к функциональной безопасности 13
Приложение С (справочное) Примеры применения не связанных с безопасностью ЭСДЗ 25
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 27
Библиография 28

Введение

Готовые компоненты электронных систем жилых домов и зданий (ЭСДЗ), должны быть безопасными при их использовании по назначению.

Настоящий стандарт устанавливает общие требования к функциональной безопасности ЭСДЗ в соответствии с принципами базового стандарта по функциональной безопасности МЭК 61508.

Настоящий стандарт определяет требования к функциональной безопасности, относящиеся к готовым компонентам ЭСДЗ и их установке. Требования основаны на анализе рисков в соответствии с МЭК 61508.

Цель настоящего стандарта состоит в распределении, насколько это возможно, всех требований к безопасности компонентов электронных систем жилых домов и зданий (ЭСДЗ-компонент) на всем их жизненном цикле.

Настоящий стандарт применим только к компонентам электронных систем жилых домов и зданий.

Настоящий стандарт предназначен для применения техническими комитетами по стандартизации, которые разрабатывают или улучшают стандарты на компоненты электронных систем или на электронные системы жилых домов и зданий, а также для производителей компонентов ЭСДЗ, для которых не существует стандартов по функциональной безопасности.

В настоящем стандарте рассматриваются компоненты ЭСДЗ и домовых электронных систем (ДЭС), которые относятся к не связанным с безопасностью компонентам.

На сайте МЭК можно ознакомиться с другими аналогичными стандартами.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ СИСТЕМ ДОМОВ И ЗДАНИЙ (ЭСДЗ)

Information technology – Functional safety requirements for home and building electronic systems (HBES)

Дата введения — 2014—09—01

1 Область применения

Настоящий стандарт определяет требования к функциональной безопасности компонентов и систем для электронных систем жилых домов и зданий[1)] (ЭСДЗ), реализованных на основе многопользовательской системы с шинной организацией, в которой функции децентрализованы, распределены и связаны общим коммуникационным процессом. Требования настоящего стандарта также могут применяться к распределенным функциям любого оборудования, подсоединенного к электронной системе жилых домов и зданий, если отсутствует конкретный стандарт по функциональной безопасности для данного оборудования или системы.

Требования функциональной безопасности, изложенные в настоящем стандарте, применяются вместе с требованиями соответствующих стандартов (если такие имеются) на компоненты электронных систем жилых домов и зданий.

Настоящий стандарт не содержит требований к функциональной безопасности систем, связанных с безопасностью.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК 14543-2-1 Информационные технологии. Архитектура электронных систем домов. Часть 2.1. Введение и принцип модульности устройств (ISO/IEC 14543-2-1, Information technology – Home electronic systems (HES) architecture – Part 2-1: Introduction and device modularity)

Руководство ИСО/МЭК 51 Аспекты безопасности и их применение в стандартах (ISO/IEC Guide 51, Safety aspects – Guidelines for their inclusion in standards)

МЭК 61508 (все части) Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью (IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems)

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

МЭК 61508-4–1998 Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 4. Термины и сокращения. С поправкой 1 от апреля 1999 г. (IEC 61508-4:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations; including its corrigendum 1 from April 1999)

МЭК 61508-5–1998 Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 5. Примеры методов по определению уровней полноты безопасности систем. С поправкой от апреля 1999 г. (IEC 61508-5:1998, Functional safety of electrical/electronic/ programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels; including its corrigendum 1 from April 1999)

МЭК 61709–1996 Электронные компоненты. Безотказность. Справочные данные для интенсивности отказов и модели пересчета (IEC 61709:1996, Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion)

[1)] К жилым зданиям относятся также многофункциональные здания, в состав которых могут входить квартиры (гостиничные номера), небольшие магазины и офисные помещения.

Серия ИСО 9000 Системы менеджмента качества (ISO 9000 series, Quality management systems)

ЕН 50090-2-2 Электронные системы жилых домов и зданий (ЭСДЗ). Часть 2.2. Общие технические требования. (EN 50090-2-2, Home and Building Electronic Systems (HBES) – Part 2-2: System overview – General technical requirements)

3 Термины, определения и сокращения

В настоящем стандарте применены следующие термины с соответствующими определениями, а также сокращения:

3.1.1 **архитектура** (architecture): Конкретная конфигурация элементов комплектующего оборудования и программного обеспечения системы.

[МЭК 61508-4, определение 3.3.5]

3.1.2 **проверка подлинности** (authentication): Средства или способ удостоверения истинности лица, отправляющего сообщение или того, кто претендует им быть, и подтверждения того, что сообщение является идентичным тому, которое было отправлено.

3.1.3 **авторизация** (authorization): Механизм осуществления доступа к информации юридического или физического лица, имеющего на это право.

3.1.4. **нарушенная связь** (disturbed communication): Связь, при которой по какой-то причине переданное сообщение оказывается неполным, усеченным, содержит ошибки, либо имеет правильный формат, но заключает в себе информацию, которая выходит за пределы ожидаемых параметров для подобных сообщений.

3.1.5. **функциональная безопасность** (functional safety): Отсутствие неприемле-мого риска причинения вреда в связи с работой ЭСДЗ, в том числе при:

а) нормальной эксплуатации;

б) разумно предсказуемом неправильным использовании;

в) отказе;

г) временных нарушениях.

Примечания

1 См. определение 3.1.9 МЭК 61508-4. Часть общей безопасности, связанной с управляемым оборудованием (УО) и системой управления УО, которая зависит от правильного функционирования электрических/электронных/программируемых электронных (Э/Э/ПЭ) связанных с безопасностью систем, связанных с безопасностью систем на основе других технологий и внешних средств снижения риска.

2 Учтены определения, данные в [30] и [31].

3.1.6 **расстояние Хемминга** (hamming distance): Число битов, на которое отличаются два двоичных кода.

3.1.7 **вред** (harm): Физическое повреждение или ущерб, причиняемый здоровью людей, имуществу или окружающей среде как напрямую, так и косвенно.

[МЭК 61508-4, определение 3.1.1]

3.1.8 **опасность** (hazard): Потенциальный источник причинения вреда.

[ИСО/ МЭК Руководство 51, определение 3.5]

Примечание – Настоящий термин включает в себя возможную опасность для людей, возникающую за короткий период времени (например при пожаре или взрыве), а также опасность, имеющую долговременное воздействие на здоровье человека (например при утечке токсичных веществ).

[МЭК 61508-4, определение 3.1.2]

3.1.9 **опасное событие** (hazardous event): Ситуация, которая приводит к нарушению нормальной работы или ненормальным условиям.

Примечание – См. определения 3.1.3 и 3.1.4 МЭК 61508-4. Обстоятельства, при которых человек подвергается опасности (или нескольким опасностям), которые приводят к нанесению вреда.

3.1.10 **электронные системы жилых домов и зданий**, ЭСДЗ (home and building electronic systems, HBES): Многопользовательская система с шинной организацией, в которой функции распределены, децентрализованы и связаны общим коммуникационным процессом.

Примечания

1 ЭСДЗ используется в жилых домах и зданиях, включая их окружение. Функциями системы являются, например, переключение, управление с разомкнутым контуром управления, управление с замкнутым контуром управления, мониторинг и надзор.

2 Если ЭСДЗ используется в жилом здании, то ее часто называют домовой электронной системой (ДЭС).

3.1.11 **компонент ЭСДЗ** (HBES product): Устройство или устройства, такие как аппаратные средства, аппаратные средства со встроенными программами, их программное обеспечение и средства конфигурирования, предназначенные для использования в ЭСДЗ.

Примечание – Компоненты, которые используются для домовых электронных систем, часто называют компонентами ДЭС.

3.1.12 **компонент** (product): Устройство или устройства, такие как аппаратные средства, аппаратные средства со встроенными программами, их программное обеспечение и средства конфигурирования.

3.1.13 **документация на компонент** (product documentation): Документация производителя по установке и эксплуатации компонента, которая сопровождает компонент; информация о компоненте, содержащаяся в каталоге производителя и другие маркетинговые информационные материалы на компонент; описания, определения, литература о компоненте и его применении, представленная в электронном формате на сайте изготовителя (или поставщика) в сети Интернет.

3.1.14 **связанная с безопасностью система** (safety related system): Система, которая реализует требуемые функции безопасности, необходимые для достижения или поддержания безопасного состояния управляемого оборудования, а также предназначена для достижения самостоятельно или вместе с другими Э/Э/ПЭ связанными с безопасностью системами, связанными с безопасностью системами на основе других технологий или внешними средствами снижения риска, необходимой полноты безопасности для требуемых функций безопасности.

Примечания

1 Данный термин относится к системам, определенным как системы, связанные с безопасностью, целью которых является достижение необходимого снижения риска вместе с внешними средствами снижения риска (см. определение 3.4.3 МЭК 61508-4), чтобы соответствовать требуемому приемлемому риску (см. определение 3.1.6 МЭК 61508-4). См. также приложение А МЭК 61508-5.

2 Связанные с безопасностью системы предназначены для предотвращения перехода управляемого оборудования в опасное состояние путем принятия необходимых мер при получении команд. Отказ связанной с безопасностью системы должен быть включен в список событий, приводящих к опасности или опасностям. Хотя могут быть и другие системы, реализующие функции безопасности, рассматриваемые связанные с безопасностью системы – это такие системы, которые были специально предназначены для достижения необходимого приемлемого риска. Связанные с безопасностью системы можно разделить на связанные с безопасностью системы управления и связанные с безопасностью системы защиты. Они имеют два режима работы (определение 3.5.12 МЭК 61508-4).

3 Связанные с безопасностью системы могут быть неотъемлемой частью системы управления управляемого оборудования или могут быть связаны с управляемым оборудованием с помощью датчиков и (или) исполнительных механизмов. Это означает, что требуемый уровень полноты безопасности может быть достигнут путем реализации функций безопасности в системе управления управляемого оборудования (и, возможно, также с помощью дополнительных отдельных и независимых систем), или функции безопасности могут быть реализованы отдельными и независимыми системами, предназначенными для обеспечения безопасности.

4 Связанная с безопасностью система может быть предназначена для:

а) предотвращения опасного события (например, если связанные с безопасностью системы выполняют свои функции безопасности, то опасное событие не возникает);

б) смягчения последствий опасного события, тем самым снижая риск за счет уменьшения последствий;

в) совместного достижения целей перечислений а) и б).

5 Человек может стать частью системы обеспечения безопасности (см. определение 3.3.1 МЭК 61508-4). Например, человек может получать информацию от программируемого электронного устройства и выполнять действия по обеспечению безопасности, основанные на данной информации, или выполнять действия по обеспечению безопасности с помощью данного программируемого электронного устройства.

6 Данный термин включает в себя все аппаратные средства, программное обеспечение и средства поддержки (например, источники электропитания), необходимые для выполнения заданных функций безопасности (поэтому датчики, другие устройства ввода, исполнительные элементы (приводы) и другие устройства вывода включают в состав связанной с безопасностью системы).

7 Связанная с безопасностью система может основываться на широком спектре технологий, включая электрические, электронные, программируемые электронные, гидравлические и пневматические технологии.

[МЭК 61508-4, определение 3.4.1]

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

[ИСО/МЭК Руководство 51, определение 3.2]

[МЭК 61508-4, определение 3.1.5]

Примечание – О классах риска см. приложение А.

3.1.16 **разумно предсказуемое неправильное использование** (reasonably foreseeable misuse): Использование изделия, процесса или услуги в условиях или с целью, не предусмотренных поставщиком, но которое может произойти по причине использования изделия, процесса или услуги в сочетании с легко предсказуемым поведением человека или в результате легко предсказуемого поведения человека.

[МЭК 61508-4, определение 3.1.11]

3.1.17 **функция безопасности** (safety function): Функция, реализуемая Э/Э/ПЭ связанной с безопасностью системой, связанной с безопасностью системой, основанной на других технологиях, или внешними средствами снижения риска, которая предназначена для достижения и поддержания безопасного состояния управляемого оборудования в отношении конкретного опасного события (см. определение 3.1.4 МЭК 61508-4).

[МЭК 61508-4, определение 3.5.1]

3.2 Сокращения

ДЭС	–	домовая электронная система;
ПЗУ	–	постоянное запоминающее устройство
УО	–	управляемое оборудование;
ЭСДЗ	–	электронные системы жилых домов и зданий;
ALARP	–	разумная достаточность (от английского «As Low As Reasonably Practicable»).

4 Соответствие настоящему стандарту

Разработка и внедрение компонентов, которые соответствуют настоящему стандарту, должны быть проанализированы на возможные риски в соответствии с разделом 5.

Компоненты, которые соответствуют настоящему стандарту, должны соответствовать требованиям, установленным в разделе 6.

5 Общие требования

5.1 Основные положения

Функциональная безопасность системы учитывает как технические характеристики сети, так и технические характеристики компонентов ЭСДЗ, которые она связывает.

Отказ в сети или любого компонента ЭСДЗ не должен приводить к опасной ситуации в системе, других компонентах или управляемом оборудовании.

Обеспечение безопасности отдельных компонентов ЭСДЗ в процессе их эксплуатации не следует полностью возлагать на систему.

В процессе эксплуатации взаимодействие любого компонента с любым(и) другим(и) компонентом(ами) не должно приводить к опасной ситуации в системе.

5.2 Метод установления требований

5.2.1 Основные положения

Требования к функциональной безопасности устанавливают в соответствии с жизненным циклом, определенным в МЭК 61508-1:

a) разработка концепции компонентов;
b) определение окружающей среды применения;
c) идентификация опасностей и опасных событий;
d) анализ опасности и риска, меры по снижению риска;
e) реализация мер по снижению риска;
f) подтверждение соответствия;
g) техническое обслуживание;
h) установка и ввод в эксплуатацию;
i) вывод из эксплуатации.

Технические комитеты по стандартизации и (или) разработчики компонентов ЭСДЗ должны учитывать требования настоящего стандарта в целях удовлетворения требований к безопасности компонентов, но нет необходимости следовать самому процессу, представленному в МЭК 61508-1.

5.2.2 Определение области распространения ЭСДЗ

Следует учитывать окружающую среду применения ЭСДЗ.

5.2.3 Источники опасности

Должны быть рассмотрены следующие источники опасностей:

a) материалы и конструкция;
b) отказоустойчивость;

c) нормальное функционирование;
d) непреднамеренное взаимодействие с другими компонентами;
e) взаимодействие с другими компонентами ЭСДЗ;
f) ненормальные условия;
g) разумно предсказуемое неправильное использование, в том числе загрузка несанкционированных и вредоносных кодов;

Примечание – В том числе непреднамеренное изменение программного обеспечения.

h) срок службы;
i) окружающая среда.

5.2.4 Опасные события

При анализе информационной шины и сети электропитания должны быть учтены следующие опасные события:

1) нарушение электропитания;
2) короткое замыкание в шине;
3) перенапряжение на шине;
4) перенапряжение в сети электропитания;
5) повреждение изоляции (из-за температуры, скачка напряжения, механиче-ское);
6) неправильное подключение;
7) превышение температуры;
8) возгорание;
9) механический удар, вибрация;
10) коррозия;
11) электромагнитные помехи;
12) нарушение связи;
13) загрязнение;
14) завершение срока службы составляющих/компонентов;
15) разумно предсказуемое неправильное использование;
16) программный сбой;
17) перегрузка;
18) потеря безотказности;
19) разрушение материала (механическое);
20) ошибки проектирования/конструкции;
21) переключение поврежденного оборудования и подсистем;
22) дистанционное управление;
23) поступление команды от двух источников к одному компоненту (например к исполнительному механизму);
24) отказы системы.

5.2.5 Формирование требований

Для каждого опасного события должен быть проведен анализ риска (см. приложение В). Для этого должна быть оценена вероятность возникновения события, и должен быть учтен класс риска в соответствии с методом, описанным в приложении А.

Если оценка класса риска указывает на неприемлемый риск, то требуется применение мер по снижению риска, а также определение результирующего снижения риска и его подтверждение соответствия. Также указываются некоторые меры по снижению риска, включенные в стандарт на соответствующий компонент. Если производители планируют разрабатывать компоненты ЭСДЗ или системы, которые обнаруживают опасные события, не учтенные в 5.2.4, то для таких событий должен быть выполнен анализ риска в соответствии с МЭК 61508.

6 Требования к функциональной безопасности

Примечание – В скобках ( ) даны ссылки на опасные события, перечисленные в 5.2.4.

6.1 Основные положения

Анализ, выполняемый в соответствии с МЭК 61508-1, указывает на то, что функциональная безопасность зависит как от процессов проектирования и производства компонентов, так и от правильного использования компонента при установке.

Требования к компонентам ЭСЗ и к обеспечению информацией, необходимой для правильной установки, эксплуатации и технического обслуживания данных компонентов содержатся в п. 6.2–6.7.

Если необходимо, следует соблюдать требования, установленные для компонентов, а также

проверять предоставленную необходимую информацию.

Все упомянутые испытания компонентов являются типовыми испытаниями.

Основания и причины представленных далее требований приведены в приложении В.

6.2 Электропитание

6.2.1 Безопасный запуск после восстановления подачи электропитания (1)

При восстановлении подачи электропитания в случае его сбоя должен быть обеспечен безопасный перезапуск компонентов.

Безопасный перезапуск может быть выполнен с помощью:

- сохранения информации о состоянии компонентов и использования данной информации для восстановления функционирования после подачи электропитания;
- переключения в заданное состояние компонента в зависимости от его сферы применения;
- расчета безопасного состояния, основанного на доступной информации в системе (в контроллере, при его наличии, и (или) в каждом компоненте),
- поддержания достаточного запаса мощности (обеспечивающего соответствующее резервное время для компонента и (или) блока питания), для обеспечения перехода подключенных компонентов в безопасное состояние.

6.2.2 Маркировка компонента и инструкции для предотвращения риска неправильного подключения (3) (6)

Маркировка и инструкции для компонентов должны быть разработаны таким образом, чтобы избежать риска неправильного подключения.

Маркировка компонента должна быть выполнена отчетливо и прочно.

Проверку соответствия проводят путем проверки документации на компонент и, если необходимо, путем испытаний прочности и отчетливости маркировки компонента по соответствующим стандартам на компонент.

6.2.3 Конструирование и разработка компонентов, предотвращающие неправильное подключение

Конструкция и исполнение компонента должны обеспечивать предотвращение неправильного подключения.

Неправильное подключение можно избежать применением соответствующего группирования разъемов. (6)

Проверку соответствия выполняют тестированием компонента.

6.3 Окружающая среда

6.3.1 Компонент, разработанный для применения в определенной окружающей среде и заданном диапазоне температур (7)

Компоненты должны быть рассчитаны на рабочую температуру, соответствующую максимальному номинальному напряжению, необходимому для окружающей среды применения, и должны стабильно работать в указанном температурном диапазоне.

Проверку соответствия выполняют тестированием компонента согласно требованиям соответствующего для него стандарта, а в случае отсутствия такового, согласно требованиям ЕН 50090-2-2 и соответствующих базовых стандартов по безопасности.

6.3.2 Устойчивость к высоким температурам и предотвращение распространения огня (8)

Компоненты и их составляющие должны быть рассчитаны на устойчивость к повышенной температуре и нераспространению огня.

Проверку соответствия выполняют тестированием компонента согласно требованиям соответствующего для него стандарта, а в случае отсутствия такового, согласно требованиям соответствующих базовых стандартов по безопасности.

6.3.3 Устойчивость к механическим нагрузкам, соответствующим применению(ям) (9)

Компонент должен быть устойчивым к механическим нагрузкам, соответствующим применению(ям).

Проверку соответствия выполняют тестированием компонента согласно требованиям соответствующего для него стандарта, а в случае отсутствия такового, согласно требованиям ЕН 50090-2-2 и соответствующих базовых стандартов по безопасности.

6.4 Срок службы

Компонент должен быть спроектирован на указанный срок службы в соответствии с МЭК 61709:1996, п. 5.2 и приложением А настоящего стандарта или на определенное количество циклов переключения при нормальных условиях. Для достижения заданного срока службы в документацию на компонент, если необходимо, следует включать инструкцию по техническому обслуживанию. (14)

Проверку соответствия следует проводить путем проверки документации на компонент.

6.5 Разумно предсказуемое неправильное использование

6.5.1 Сведение к минимуму нежелательной загрузки неверного программного обеспечения или параметров (15)

Риск нежелательной загрузки неверного программного обеспечения или параметров в данный компонент должен быть минимизирован.

Могут быть применены следующие меры:

разработка средств конфигурирования;

- использование идентификации компонентов и сравнение их профилей на уровне управления сетью;
- установление пароля;
- использование удостоверения подлинности;
- подготовка документации на компонента;
- обучение операторов и специалистов по установке компонент.

Проверку соответствия следует проводить путем тестирования компонента и (или) проверки документации на компонент.

6.5.2 Правильность конфигурирования и связанных с ним параметров (15)

Следует обеспечить правильность конфигурирования и связанных с ним параметров.

Могут быть применены следующие меры:

- строгая спецификация диапазона параметров;
- ограничение возможности по конфигурированию для конечного пользователя;
- допуск к конфигурированию только опытных сотрудников (см. ИСО/МЭК 14543-2-1);
- проверка на совместимость техническими средствами или специалистом по монтажу;
- проверка конфигурации на соответствие требованиям.

Проверку соответствия проводят сравнением полученной конфигурации с планируемой.

6.5.3 Обнаружение и (или) отображение отсутствующих или неполностью настроенных компонентов в процессе конфигурирования (15)

Следует принимать меры для обнаружения и (или) отображения отсутствующих или неполностью сконфигурированных компонентов в процессе конфигурации.

Могут быть применены следующие меры:

- разработка средств конфигурирования;
- следование формальным процедурам установки.

Проверку соответствия следует проводить путем тестирования компонента и (или) проверки документации на компонент.

6.6 Программное обеспечение и передача данных

6.6.1 Соответствие процесса разработки требованиям ИСО 9000 или аналогичных стандартов (16)

Процесс разработки программного обеспечения должен соответствовать требованиям ИСО 9000 или аналогичных стандартов.

Проверку соответствия проводят путем проверки процесса ведения рабочей документации или соответствующих сертификатов соответствия.

6.6.2 Проверка корректности работы программного обеспечения компонента и полноты конфигураций (16)

Должны быть предусмотрены меры для проверки корректности работы программного обеспечения компонента и полноты конфигурации. Если обнаруживается неправильная работа, то компонент должен восстановить корректные значения или перейти к заданному состоянию.

Проверку соответствия проводят путем проверки проектной документации на компонент (программное обеспечение).

6.6.3 Ограничение нагрузки трафика на каналы передачи данных (12), (17)

Если необходимо для компонента должны быть предусмотрены меры по ограничению нагрузки трафика на каналы передачи данных.

Возможны следующие меры:

- ограничение циклической передачи данных;
- снижение числа сообщений в единицу времени для каждого компонента;
- ограничение циклов опроса.

Проверку соответствия компонента проводят путем проверки документации на компонент и, если возможно, путем его тестирования.

6.6.4 Правильное функционирование компонента и предотвращение опасностей при получении сообщений от разных источников (23)

Прием сообщений от нескольких источников не должен приводить к нарушению нормального функционирования компонента и вызывать опасные события.

Возможны следующие меры:

- проверка адреса источника, если существует иерархия источников;
- применение правила: обработка в порядке поступления;
- применение правила: последнее сообщение – решающее;
- обеспечение безопасности процесса, завершение его до того, как поступят новые сообщения, которые могут на него повлиять;
- обеспечение безопасности процесса путем его останова и перезапуска;
- обеспечение безопасности процесса путем его блокирования и разблокирования.

Проверку соответствия компонента проводят путем проверки документации на компонент и, если возможно, путем его тестирования.

6.6.5 Заданное состояние после сброса системы (если предусмотрено) (24)

Если был осуществлен сброс системы (если он предусмотрен), то компоненты должны переходить в заданное состояние.

Проверку соответствия компонента проводят путем проверки документации на компонент и, если возможно, путем его тестирования.

6.6.6 Ограничение доступа к ручному конфигурированию параметров системы (24)

Должна быть предусмотрена возможность ограничения доступа к ручному конфигурированию параметров системы.

Возможно применение следующих мер или исключений:

- использование инструментальных средств конфигурирования (аппаратных или программных);
- использование пароля и (или) проверки подлинности;
- установка защиты от несанкционированного доступа;
- выполнение параллельных или последовательных действий;
- использование скрытых средств конфигурирования;
- исключение случаев явного подробного описания ручного конфигурирования в руководстве по применению (а также в случае автоматического конфигурирования).

Проверку соответствия компонента проводят путем проверки документации на компонент и, если возможно, путем его тестирования.

6.6.7 Нарушение передачи данных

6.6.7.1 Независимость безопасной работы компонента от работы других компонентов системы или приложения (12)

Безопасная работа компонента не должна зависеть от работы других компонентов в системе или приложении.

Для этого могут быть приняты следующие меры:

- использование циклической передачи данных;
- выполнение проверки диапазона полученных значений переменных.

Проверку соответствия проводят путем проверки результатов испытаний компонента или проверки документации на компонент.

6.6.7.2 Идентификация нарушенных сообщений и меры по обеспечению безопасной работы (11), (12)

Нарушенные сообщения должны успешно идентифицироваться. В случае обнаружения нарушения сообщения следует предпринять определенные меры по обеспечению безопасной работы. Значение расстояния Хемминга должно быть не меньше 2.

Возможны следующие меры:

- приемник компонента может отклонить или изменить сообщение;
- отправитель может повторить своё сообщение.

Проверку соответствия проводят путем проверки результатов испытаний компонента или проверки документации на компонент.

6.6.7.3 Предотвращение ложных сообщений

Необходимо предотвращать рассылку ложных, но формально правильных сообщений.

Проверку соответствия проводят путем соответствующих испытаний на электромагнитную совместимость по ЕН 50090-2-2. (11), (12)

6.6.7.4 Отображение и повторение потерянных сообщений (12), (17)

Если сообщения потеряны, то необходимо предпринять меры, чтобы эта потеря была отображена, а сообщения были переданы повторно.

Возможны следующие меры:

- использование механизмов подтверждения в коммуникационных средствах или в средствах применения;
- использование индикации или визуализации полученной информации о состоянии коммуникационных средств;

- применение соответствующего систематического повтора для компонента с однонаправленной передачей.

Проверку соответствия проводят путем проверки результатов испытаний компонента или проверки документации на компонент.

6.7 Дистанционное управление

6.7.1 Основные рекомендации

Предыдущие требования распространяются также на режим дистанционного управление компонентами внутри помещения.

Розетки для дистанционного управления должны быть помечены таким образом, чтобы они заметно отличались от других розеток, используемых пользователем. Или их конструкция должна быть такова, чтобы исключить возможность их использования с вилками, не предназначенными для подключения удаленных компонентов. (22)

6.7.2 Дистанционное управление изнутри отдельного здания или в непосредственной близости от него

Компоненты или подсистемы, связанные с компонентом, который может причинить вред, и дистанционно управляемые изнутри отдельного здания или в непосредственной близости от него, должны быть оснащены автономными средствами управления или средствами включения/отключения дистанционного управления.

Возможны следующие меры:

- автономные средства управления в потенциально опасных компонентах;
- автономные средства управления, установленные рядом с потенциально опасными компонентами;
- коммуникационные входы для поддержки автономного управления.

Проверку соответствия проводят путем проверки компонента или документации на компонент.

6.7.3 Дистанционное управление снаружи здания

6.7.3.1 Обеспечение средствами автономного управления в случае дистанционного управления снаружи здания

Компоненты или подсистемы, которые могут причинить вред и которые предназначены для дистанционного управления снаружи здания, должны быть обеспечены средствами автономного управления в случае дистанционного управления снаружи здания.

Возможны следующие меры:

- местные средства управления, установленные на потенциально опасных компонентах;
- местные средства управления, установленные вблизи потенциально опасных компонентов;
- коммуникационные входы, позволяющие поддерживать местное управление;
- местные средства отключения межсетевого шлюза или других средств удаленного доступа к компоненту.

Проверку соответствия проводят путем проверки компонента или документации на компонент.

6.7.3.2 Авторизация или проверка подлинности дистанционного управления, снаружи здания (22)

Следует использовать особый механизм для авторизации или проверки подлинности дистанционного управления снаружи здания (см. также таблицу 1). (22). Такой механизм может быть реализован в системе (сетевой экран или межсетевой шлюз) или на уровне компонента.

Авторизация может быть следующих видов:

- с использованием пароля для проверки подлинности или авторизации;
- с доступом по выделенному каналу.

Проверку соответствия проводят путем проверки компонента или документации на компонент.

6.7.4 Менеджмент

6.7.4.1 Авторизация и проверка подлинности дистанционного управления включая конфигурирование и загрузку снаружи здания (22)

Следует использовать особый механизм авторизации или проверки подлинности дистанционного управления, включая конфигурирование и загрузку снаружи здания (см. также таблицу 1) (22). Такой механизм может быть реализован в системе (сетевой экран или межсетевой шлюз) или на уровне компонента.

Авторизация может быть следующих видов:

- с использованием пароля для проверки подлинности или авторизации;
- с доступом по выделенному каналу.

Проверку соответствия проводят путем проверки компонента или документации на компонент.

6.7.4.2 Соответствие между реальной сетью и ее удаленным представлением (22)

Следует предпринять соответствующие меры для обеспечения точного соответствия реальной сети ее удаленному представлению (22).

Возможны следующие меры:

- предусмотреть процедуру, гарантирующую существование единственной достоверной копии системной базы данных;
- использовать механизмы подтверждения соответствия удаленной системной базы данных реальной сети;
- предусмотреть функцию автодокументирования в системе (централизованную или распределенную).

Проверку соответствия проводят путем проверки компонента или документации на компонент.

Таблица 1 – Требования по предотвращению случайных операций и возможные пути их достижения

Требования	Пути достижения выполнения требований
Предотвратить непреднамеренное срабатывание	Ограничить внешние операции, оставив только: - авторизованные пользователями, например, с задерж-кой по времени; - прошедшие через межсетевой шлюз
Не допускать непреднамеренного управления операциями сети	Использовать инструментальные средства (физические или программные) или следующие методы кодирования доступа: - простой код, 4 символа; - более длинный код*; - шифрование и (или) проверка подлинности
Проверять подлинность целевого компонента и «загрузчика»	Например использовать «сертифицированный экземпляр программного обеспечения»
* Простой и более длинный коды используются в закрытой среде передачи данных, однако они не применимы для открытой среды, поскольку являются более доступными.	

Приложение А
(справочное)

Пример метода определения уровней полноты безопасности

А.1 Общие положения

Настоящий метод позволяет описать допустимый риск для:

- электрических/электронных/программируемых электронных (Э/Э/ПЭ) систем, связанных с безопасностью;
- других связанных с безопасностью систем, основанных на других технологиях;
- внешних средств уменьшения риска, подлежащих определению.

На рисунке А.1 показана общая система снижения риска, см. МЭК 61508-5, рисунок А.1.

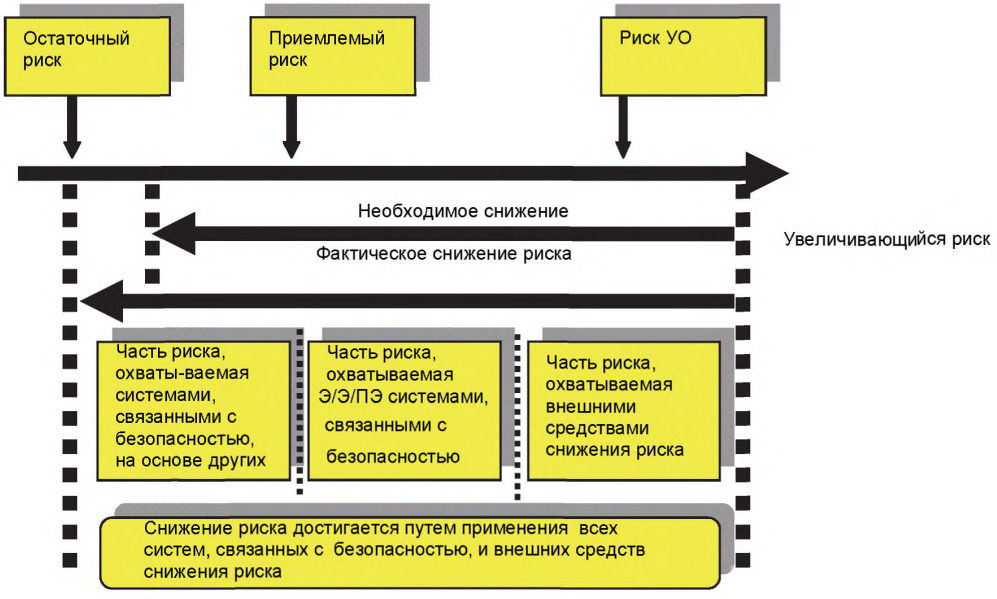

Рисунок А.1 – Снижение риска – общая концепция

А.2 Термины и определения

В настоящем приложении, применены следующие термины с соответствующими определениями.

А.2.1 **полнота безопасности** (safety integrity): Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех установленных условиях в установленном интервале времени.

[МЭК 61508-4, определение 3.5.2, модифицированное]

А.2.2 **уровень полноты безопасности** (safety integrity level): Дискретный уровень (принимающий одно из четырех возможных значений), определяющий требования к полноте безопасности функций безопасности, которые реализуются Э/Э/ПЭ системами, связанными с безопасностью; уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности; уровень, равный 1, отвечает наименьшей полноте безопасности.

[МЭК 61508-4, определение 3.5.6]

А.3 Концепции разумной достаточности (ALARP) и приемлемого риска

В настоящем приложении приведены некоторые сведения, указанные в МЭК 61508-5, приложение В.

В таблице А.1 показана взаимосвязь вероятности (частоты) риска, его последствий и классов, а в таблице А.2 отражена классификация классов риска с использованием понятия разумной достаточности ALARP.

Таблица А.1 – Пример классификации рисков несчастных случаев

Частота событий	Последствия			
	Катастрофические	Критические	Граничные	Несущественные
Частые	Класс I	Класс I	Класс I	Класс II
Возможные	Класс I	Класс I	Класс II	Класс III
Случайные	Класс I	Класс II	Класс III	Класс III
Маловероятные	Класс II	Класс III	Класс III	Класс VI
Практически невероятные	Класс III	Класс III	Класс VI	Класс VI
Невероятные	Класс VI	Класс VI	Класс VI	Класс VI
Примечание – Фактическое распределение риска по классам I, II, III и IV должно зависеть от конкретной области применения, а также от реальных значений частот, вероятностей и т.д. Таким образом, настоящую таблицу следует рассматривать как пример того, как такая таблица может быть заполнена, а не в качестве перечня требований для будущего применения.				

Таблица А.2 – Интерпретация классов риска

Класс риска	Интерпретация
Класс I	Неприемлемый риск
Класс II	Риск нежелателен и допустим, если снижение риска практически невозможно или затраты непропорциональны по отношению к получаемой выгоде
Класс III	Приемлемый риск, если затраты на снижение риска будут превышать получаемую выгоду
Класс VI	Незначительный риск

Приложение В
(справочное)

Опасности и разработка необходимых требований к функциональной безопасности

В настоящем приложении представлен полученный в результате анализа набор необходимых методов снижения риска для опасных событий, указанных в 5.2.4, и соответствующих элементов этих событий. Результатом данного анализа являются требования, изложенные в разделе 6.

При выполнении этих требований остаточный риск становится допустимым (класс III) или незначительным (класс IV).

В стандарты на компонент должны входить требования и меры по снижению риска до уровня допустимого, как показано в таблице В.1.

Таблица В.1 – Требования к безопасности и снижению риска

№	Опасное событие, п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
1	Неисправность сети питания	1-1 Отключение питания шины	Только в шине	Компонент должен сохранять всю информацию о состоянии, необхо-димую для предотвращения риска в случае включения питания и (или) для перевода системы/ком-понента в безопасный режим в случае необходимости
		1-2 Питание в шине отсутствует	–	
		1-3 Возобновление питания в шине	–	См. 1-1
		1-4 Отключение питания шины от сети 230 В	–	См. 1-1. БП должен работать до 80 мс. (БП – блок питания)
		1-5 Кратковременное отсутствие питания в шине от сети 230 В	Например, 80 мс	
		1-6 Отключение резервного питания компонента	–	См. 1-1. Шина компонента должна сохра-нять всю информацию о состоя-нии, необходимую для предотвра-щения риска в случае включения питания и (или) для перевода сис-темы/компонента в безопасный режим в случае необходимости – это зависит от применения
		1-7 Кратковременное отсутствие резервного питания компонента	–	
		1-8 Возобновление только питания в сети	–	См. 1-1
		1-9 Возобновление питания в сети и в шине	–	См. 1-1

Продолжение таблицы В.1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
2	Короткое замыкание в шине питания	2-1 Полное корот-кое замыкание	Компоненты с пита-нием от сети в 230 В и (или) от допол-нительного источ-ника питания не получают питание от шины, несмотря на наличие питания	См. 1-1. - Цепи шины должны быть защищены от перегрузки по току, см. ЕН 50090-2-2
		2-2 Неполное ко-роткое замыкание	Шина частично может обеспечить электропитание; нет сигнала в БП	См. 12 для устройств без связи См. 1-1 для компонентов при отсутствии питания в шине
		2-3 Чрезмерный ток в шине	Шина питания компонента отключается (от сети) с помощью ее средств защиты	См. 12. – другой вариант: отключается БП (ЕН 50090-2-2) и (или) обеспечивается индикация; – другой вариант решения проблемы: сегментация компонента с независимыми шинами и БП + защита от локальных отказов
3	Перенапряжен ие на шине	3-1 Нет последствий	–	Выполняются требования ЕН 50090-2-2. При электростатических и индуктивных наводках: - использование систем безо-пасного сверхнизкого напря-жения (SELV) с защитным импедансом заземления для временного перенапряжения; - использование систем безо-пасного сверхнизкого напря-жения (SELV) снижает риск возникновения постоянных опасных перегрузок. При повреждении изоляции: - изоляция компонентов ЭСДЗ и ДЭС от прочих сетей с $U_R \geq 250$ V и $U_R \geq 80$ V переменно-го тока проверяется, как для PELV или SELV, согласно ЕН 50090-2-2; - дополнительно: применение (со стороны сети) устройства защитного отключения (УЗО)
		3-2 Автоматичес-кий сброс	–	Дополнительные меры не требуются
		3-3 Ручной сброс	–	Дополнительные меры не требуются
		3-4 Неисправност ь компонента	–	Даже если компонент ЭСДЗ подключен к сети с напряжени-ем 230 V, он не должен причинить вреда (вред должен быть маловероятен из-за отличия разъема для SELV)

Продолжение таблицы В.1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
4	Перенапряжение сети питания	4-1 Не влияет на БП	–	Сеть: Компоненты должны соответ-ствовать требованиям [25] и ЕН 50090-2-2. Испытательное напряжение для твердой изоляции или герме-тичных компонентов, изолирую-щих ЭСДЗ от сети питания, равно 4 kV переменного тока (тестирование проводится в соответствии с [27])
		4-2 Автоматичес-кий сброс БП	–	Дополнительные меры не требуются
		4-3 Ручной сброс БП	–	Дополнительные меры не требуются
		4-4 Неисправность БП	–	БП не должен стать причиной пожара или взрыва
5	Повреждение изоляции (из-за температуры, ска-чка напряжения, механического воздействия)	5-1 Короткое замыкание	–	Должны быть установлены: - в сети – защита от больших токов, в соответствии с [26]; - в шине –: ограничение тока (см. ЕН 50090-2-2)
		5-2 Передача опасного напряжения	–	Следует соблюдать: - для компонентов и сетевых кабелей – правила установки по [26]; - для компонентов и кабелей шин – требования к SELV
		5-3 Доступность к токоведущим частям	–	См. ЕН 50090-2-2. Разработчики компонента должны устанавливать уровень устойчивости к механическим воздействиям с учетом окружающей среды и, если необходимо, добавлять дополнительную внешнюю защиту

Продолжение таблицы В.1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
6	Неправильное подключение	6-1 на стороне шины	Неправильная поляризация	Монтаж и проектирование должны быть выполнены так, чтобы избежать неправильного соединения. Маркировка и описание должны быть выполнены так, чтобы избежать неправильного соединения. Неправильно подключенный к шине компонент не должен работать. Компонент не должен вызывать пожар, взрыв или негативно влиять на электробезопасность
		6-2 на стороне сети	Подключение разъема шины к сети питания	См. 3-4 и 6-1. Разъемы шины и сети не должны быть взаимозаменяемыми. Монтаж и проектирование должны быть выполнены так, чтобы избежать неправильного соединения. Маркировка и описание должны быть выполнены так, чтобы избежать неправильного соединения. Компонент не должен вызывать пожар, взрыв или негативно влиять на электробезопасность
		6-3 Соединение компонентов с системами на различных физических уровнях или с шиной в диапазоне безопасного сверхнизкого напряжения (SELV)	–	Монтаж и проектирование должны быть выполнены так, чтобы избежать неправильного соединения. Маркировка и описание должны быть выполнены так, чтобы избежать неправильного соединения. Компонент не должен вызывать пожар, взрыв или негативно влиять на электробезопасность
7	Превышение температуры	7-1 Нарушение функционирования	–	Компонент должен правильно работать в заданном диапазоне температур. См. ЕН 50090-2-2
		7-2 Окружающая среда	–	Должен быть обеспечен контроль над подсистемами, работающими при температуре (внешней среды и (или) поверхности) > 60 °С: - компонент разрабатывается для более высоких температур внешней среды; - в случае отказа шины подсистема должна перейти в безопасный режим (что может быть выполнено и вручную)
8	Возгорание		–	Стандарты на компоненты должны устанавливать требования к огнестойкости
9	Механический удар, вибрация		–	Компоненты ЭСДЗ должны соответствовать ЕН 50090-2-2. Разработчики компонента могут добавить дополнительные требования, зависящие от условий применения

Продолжение таблицы В.1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
10	Коррозия	–	–	В стандарты на компонент должны быть включены соответствующие требования
11	Электромагнит-ная совмести-мость	–	–	В процессе тестирования на электромагнитную совместимость по ЕН 50090-2-2: - должно быть обеспечено выявление нарушенных сообщений; - не должны возникать ложные, но формально правильные сообщения
12	Нарушение передачи данных	12-1 Наруше-ние сигнала	–	Должно быть обеспечено выявление нарушенных сообщений. Расстояние Хемминга, частота повтора, зависящая от среды. Необходимое расстояние Хемминга должно быть более 2. Даже в случае коллизий должны прини-маться верные сообщения (защита от коллизий, обнаружение коллизий, повто-рение, подтверждение сообщений и т.д.)
		12-2 Наруше-ние работы участка шины	Например, датчик грозы	Должны быть установлены датчики, работающие постоянно или циклически. Безопасная работа компонента не должна зависеть от работы других компонентов
13	Загрязнение	–	–	Руководствоваться ЕН 50090-2-2

Продолжение таблицы В1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
14	Окончание срока службы компонента/из-делия	Общие	–	Разработчики компонента должны установить требования к минимальному сроку службы (отказоустойчивость, периоды испытаний) и (или) если необходимо разработать правила эксплуатации компонента. Например, указать дату изготовления
		14-1 Перегрев или возгорание	Работает неправильно	См. 7 и 8
		14-2 Ошибка ► Выход из строя	Устройство не работает или работает неправильно	См. 12-2
		14-3 Разрыв соединения или коррозия контакта	Устройство не работает, или работает не-правильно, или наблюдается перегрев, или возгорание	См.10, 12 и 7
		14-4 Потеря или изменение информации в памяти	Устройство связи не рабо-тает или рабо-тает непра-вильно	См. 16
		14-5 Потеря связи	Отказ связи	См. 12
		14-6 Внутренняя потеря питания	Устройство не работает	См. 12-2

Продолжение таблицы В.1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
14	Окончание срока службы компонента/из-делия	14-7 Отказ оборудования, реализующего локальное управление	Внешние операции не выполняются	Устранимо, нет дополнительного риска
		14-8 Отказ оборудования, влияющего на комуникацион-ную часть	–	См. 12
		14-9 Повреждение прошивки	–	См. 16
		14-10 Кроткое замыкание в шине	–	См. 2
15	Разумно предсказуемое некорректное использование. Диверсии для компонентов ЭСЗ не рассма-триваются	15-1 Загрузка некорректного программного обеспечения	Нестабиль-ность програм-много обеспе-чения	Предотвращать загрузку некорректного программного обеспечения, например: - используя инструментальные средства; - применяя идентификацию компонента и его возможности по управлению сетью; - используя пароль; - обучив оператора работе с устройством
		15-2 Непра-вильные конфигурация или параметры	–	В зависимости от применения разработ-чики компонента должны установить ограничения параметров. Конечный пользователь должен обла-дать ограниченными возможностями по конфигурированию. Только профессионалы могут выпол-нять конфигурирование с помощью доступных для этого средств. Проверка соответствия, например, с помощью инструментальных средств или средств конфигурации. Проверка соответствия может произво-диться специалистом по установке
		15-3 Неполное конфигуриро-вание	Отсутствие компонента	См.12. Средства конфигурирования должны оповещать об этом в ходе конфигурирования
		15-4 Непра-вильное ис-пользование типов перемен-ных или команд	–	Только профессионалы могут выполнять конфигурирование с помощью доступных для этого средств. Проверка правил взаимодействия средствами конфигурирования. Компоненты/системы/ приложения ЭСДЗ должны соблюдать правила взаимодей-ствия

Продолжение таблицы В.1

№	Опасное событие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
16	Отказ программного обеспечения	16-1 Ошибка программного обеспечения	–	Процесс разработки должен соответствовать стандартам серии ИСО 9000 или подобным
		16-2 Ошибка памяти	–	Необходимо постоянно выполнять проверку целостности данных в памяти, применяя соответствующие меры
17	Перегрузка	17-1 Перегрузка трафика шины	Задержка передачи сигналов	Должны быть установлены датчики, работающие постоянно или циклически. Должны учитываться возможности среды передачи данных при оптималь-ном или максимальном трафике. Необходимо оптимизировать трафик шины при разработке приложения
		–	Потеря передаваемого блока информации	Использование протокола поможет устранить потерю сообщений (например, используя его повторную передачу). Отображение состояния
18	Безотказность	–	–	Это не опасное событие, а только единица измерения его частоты
19	Повреждение материала (механическое)	19-1 Отказ в ре-зультате износа	Открыты токоведущие части	Для соблюдения электрической безопасности следует: - руководствоваться стандартами на компоненты или общим стандартом EH 50090-2-2; - проверить включены ли в инструкцию указания по монтажу
		19-2 Неподходящий для применения	Открыты токоведущие части	
		19-3 Неправильный монтаж	Открыты токоведущие части	
		19-4 Неверный тип материала	Открыты токоведущие части	

Продолжение таблицы В.1

20	Ошибки в проекте или конструкции	20-1 Существенно сокращен срок службы	–	См. 14
		20-2 Возгорание или взрыв из-за перегрузки	–	Необходимые меры должны быть изложены в стандартах на компоненты
		20-3 Перегрев из-за перегрузки	–	
		20-4 Разрыв соеди-нительных кабелей	–	
		20-5 Механическая блокировка меха-низма переключе-ния из-за деформа-ции корпуса	–	
		20-6 Механическая блокировка из-за коррозии	–	
		20-7 Травма / вред, причиненный краями корпуса	–	
		20-8 Открыты опас-ные токоведущие части	–	
		20-9 Выход из строя из-за перегрузки	–	
		20-10 Выход из строя из-за недостаточной электромагнитн ой совместимости	–	

Продолжение таблицы В.1

№	Опасное собы-тие п. 5.2.4	Элементы событий	Детали	Требования/меры по снижению риска
21	Отключение поврежден-ного оборудо-вания и подсистем	21-1 Разрушение корпуса	– Возгорание, взрыв. – Не гаснущий дуговой разряд. – Короткое замыкание. – Открыты токоведущие части	Стандарты на само оборудование должны также учитывать правила функциональной безопасности
		21-2 Блокировка механических частей	– Устройство не функциони-рует. – Перегрузка с последующим повреждением	
		21-3 Повреждение разъема или кабе-ля из-за согнутого электрического контакта	–	
		21-4 Повреждение электронной схемы	– Устройство не функциони-рует. – Сбой в устройстве. – Короткое замыкание, приводящее к перегреву	
22а	Дистанци онное управлен ие внутри одного помещен ия	–	–	Нет дополнительных опасностей

Продолжение таблицы В.1

22b	Дистанционное управление внутри здания	22b-1 Пуск вращающихся машин	Движение не управляется оператором	Эту функцию не выполнять. Применять стандарты на устройства. Использовать внешние меры, например аварийную кнопку. Использовать автономные средства
		22b-2 Рост температуры компонента, находящегося в воспламеняемом окружении	–	Использовать внешние меры, напри-мер биметаллические датчики. Допускается дистанционное управле-ние, если оно предварительно автори-зовано, или применение иных мер.Применять аутентификацию персоны. Использовать автономные средства или меры
		22b-3 Прекращается функционирование оборудования	Текущий про-цесс становит-ся неконтроли-руемым	Отключить дистанционную остановку оборудования во время выполнения процесса или принять внешние меры
		22b-4 Дистанционное управление розетками электропитания	Например с использованием световых индикаторов	Розетки электропитания с дистанцион-ным управлением должны быть марки-рованы
		22b-5 Дистанционная перенастройка	–	Допускается только внутри зданий
22c	Внешнее дистанционное управление (из вне здания)	22c-1 1 Пуск вращающихся машин	Движение не управляется оператором	Использовать внешние меры, например аварийную кнопку. Использовать автономные средства. Применять аутентификацию персоны
		22c-2 Рост температуры компонента, находящегося в воспламеняемом окружении	–	Использовать внешние меры, напри-мер биметаллические датчики. Допускается дистанционное управле-ние, если оно предварительно автори-зовано, или применение иных мер. Применять аутентификацию персоны
		22c-3 Прекращается функционирование оборудования	Текущий про-цесс становит-ся неконтроли-руемым	Отключить дистанционную остановку оборудования во время выполнения процесса или принять внешние меры. Применять авторизацию персоны
		22c-4 Дистанционное управление розетками электропитания	Например с использованием световых индикаторов	Розетки электропитания с дистанци-онным управлением должны быть маркированы. Применять аутентификацию персоны
		22c-5 Дистанционная перенастройка	–	Применять аутентификацию персоны

Окончание таблицы В.1

23	Команда от двух источников на один компонент (привод)	23-1 Несогласованный множественный доступ	–	Применить переконфигурирование, например: - использовать источники только с уче-том их иерархии, проверяя адреса; - применить правило: обработка в по-рядке поступления
		23-2 Команда помещается в очередь	Непредсказу-емые результа-ты	Обеспечить защиту компонентов. Применить блокировку/деблокировку /механизм приоритета для компонента или реализуемой им функции. Применить совместное использова-ние переменных. Защитить процесс путем инкапсуляции, не допуская ввода (команды)
24	Отказы системы	24-1 Система не реагирует	Устройство не функционирует	Выполнить сброс системы и перевести ее в определенное состояние
		24-2 Поврежденное сообщение	Электромагнит-ная совмести-мость	См. 12
		24-3 Неправильное сообщение	С крайне малой вероятностью возможно ини-циирование неправильных действий	См. 12
		24-4 Непреднаме-ренное изменение элементов шины	Неверная кон-фигурация или параметры. Самонастройка	См. 15-4. Выполнить авторизацию доступа иден-тифицированного производителя или его аутентификацию для конфигуриро-вания программного обеспечения
		24.5 Система занята	Устройство не функционирует	См. 17
Примечание – Настоящий стандарт не содержит требований, относящихся к рискам (номера 4, 5, 8, 10, 13, 18, 19, 20, 21), которые должны быть рассмотрены в других стандартах.				

Приложение С
(справочное)

Примеры применения не связанных с безопасностью ЭСДЗ

В – Вопрос, О – Ответ

С.1 Общие положения

Ниже приводятся примеры из различных сфер деятельности, показывающие возможные проблемы и способы их решения. Эти примеры могут оказаться полезными для различных разработчиков компонентов. Примеры не были проверены или одобрены каким-либо комитетом, который может дать другие рекомендации по разработке конкретных компонентов.

С.2 Пример 1. Печь

В: Можно ли с помощью ЭСДЗ включить печь или кухонную плиту на расстоянии?

О: Да, в пределах одной кухни.

В: Что произойдет, если я нахожусь на другом конце квартиры, а тем временем кто-то положил что-либо огнеопасное в печь? Возможно ли удаленно управлять печью по телефону? Это не запрещено?

О: Уже на протяжении многих лет многие печи оборудуются таймерами – между ними и дистанционным управлением нет никакой разницы.

В: Но когда мы устанавливаем таймер, мы делаем это вручную, стоя рядом с печью и отдаем себе отчет в своих действиях.

О: Печь оборудована кнопкой включения дистанционного управления, её следует нажать, прежде чем печь можно будет включить на расстоянии. Нет необходимости снова нажимать эту кнопку, если вы хотите выключить дистанционное управление. Печь должна соответствовать всем национальным стандартам по безопасности, которые применяются к традиционным печам.

В: Однако для кухонных плит проблема дистанционного управления остается нерешенной, поскольку доступ к ним невозможно контролировать.

О: Дистанционное управление кухонной плитой ограничено расстоянием в несколько метров внутри одной комнаты. Возможно, стоит разрешить только один доступ к управляющему устройству (в отличие от контролирования процесса). Так будет легче гарантировать, что управление происходит правильно и с полноценным знанием дела, в ходе установки и запуска. Для контролирования процесса можно разрешить несколько точек доступа (например, для того чтобы показать используемый режим или потребление энергии).

С.3 Пример 2. Устройства с высоким потенциальным риском возникновения опасности

Использование некоторых устройств по признанию их изготовителей связано с высоким риском возникновения опасности. Работа с такими устройствами предполагает присутствие локального оператора.

В: Такие устройства могут запускаться, только если из точки запуска непосредственно видно устройство?

О: Да, если таково требование производителей.

В: Значит ли это, что использование доступа ЭСДЗ к таким продуктам невозможно?

О: Необязательно. Инфракрасное излучение, осуществляющее доступ ЭСДЗ, требует, чтобы устройство находилось в пределах видимости оператора.

В: Таким образом, удаленный оператор может управлять устройством с помощью межсетевого шлюза между другой информационной средой и инфракрасным датчиком?

О: Команды, которые передаются через межсетевой шлюз от другой информационной среды к инфракрасному датчику, должны быть распознаны как исходящие извне (или вообще не должны передаваться). Так можно избежать определенных проблем.

С.4 Пример 3. Вилки, розетки и цепи электросети

Сетевые вилки, розетки и цепи электросети, управляемые с помощью ЭСДЗ в распределительном шкафу, являются:

- полезными, поскольку благодаря им можно подключить классические устройства к сетевым вилкам, розеткам и магистральным цепям, управляемым с помощью ЭСДЗ, поскольку ни один из изготовителей крупных бытовых приборов и электротехники не может предложить полный ряд компонент ЭСДЗ на первом этапе;
- потенциально опасными, поскольку с их помощью можно подключить устройства любого типа. Такие устройства могут выполнять действия, ранее не предусмотренные изготовителем или специалистом по установке вилки, розетки и цепи электросети.

Правила установки уже позволяют устанавливать розетки, которые управляются с помощью дистанционных переключателей, которые, как правило, расположены в одном помещении. «Дополнительные устройства» для розеток, которые являются времязадающими или дистанционно управляемыми переключателями (проводные или использующие радиочастоты) можно приобрести в хозяйственных магазинах. Такие устройства могут создать такую же угрозу безопасности, как и розетки или гнезда, управляемые с помощью ЭСДЗ.

За все несут ответственность специалист по установке и пользователь. Возможным решением было бы ввести при конфигурировании и вводе в эксплуатацию инструментарий, который бы четко разделял различные схемы сети (освещение, отопление и др.). Другой альтернативой было бы принятие нового стандарта на новые вилки и розетки для дистанционно управляемых устройств. Такая розетка не будет подходить для обычных вилок, а новая вилка подойдет как для старых, так и новых розеток. Новую вилку можно использовать только для устройств, которые являются безопасными для дистанционного управления и которые могут быть подсоединены к старым или новым розеткам в зависимости от того, будет пользователь применять устройство локально или дистанционно.

С.5 Пример 4. Регулировка температуры воды

В: Какие механизмы следует задействовать, чтобы специалист по установке мог установить верхний предел при установке и при этом сделать так, чтобы пользователь не мог изменить значение этого верхнего предела? Например, следует ли использовать какой-то специальный инструмент, чтобы установить температуру выше 60 °С? Каково должно быть значение верхнего предела температуры по умолчанию, если оно не установлено специалистом?

О: Обычно максимальная температура домашнего резервуара для воды не должна превышать определенное значение (около 60 °С), чтобы не допустить получения ожогов. Очевидно, что пользователь захочет понизить это значение, и он сможет сделать это. В обогреватель может быть встроено программное обеспечение или аппаратное средство, не позволяющее пользователю установить температуру выше 60 °С. Однако такие меры могут быть неуместными в тех случаях, когда нагреватель имеет промышленное применение, при котором требуется более высокая уставка, или в конкретной установке имеются и другие механизмы для предотвращения ожогов, такие как термостатические смесители на всех кранах и душевых головках.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 14543-2-1	–	*
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты»
МЭК 61508 (все части)	IDT	ГОСТ Р МЭК 61508-2012 (все части) «Функцио-нальная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
МЭК 61508-1:1998	IDT	ГОСТ Р МЭК 61508-1–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие положения, термины и определения»
МЭК 61508-4:1998	IDT	ГОСТ Р МЭК 61508-4–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и сокращения»
МЭК 61508-5:1998	IDT	ГОСТ Р МЭК 61508-5–2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов по определению уровней полноты безопасности систем»
МЭК 61709–1996	–	*
ИСО 9000 (вся серия)	–	*
ЕН 50090-2-2	–	*

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

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

IDT – идентичные стандарты.

Библиография

1 ISO/IEC 14543-3-1 Information technology – Home electronic system (HES) architecture – Part 3-1: Communication layers – Application layer for network based control of HES Class 1

2 ISO/IEC 145433-2 Information technology – Home electronic system (HES) architecture – Part 3-2: Communication layers – Transport, network and general parts of data link layer for network based control of HES Class 1

3 ISO/IEC 14543-3-3 Information technology – Home electronic system (HES) architecture – Part 3-3: User process for network base control of HES Class 1

4 ISO/IEC 14543-3-4 Information technology – Home electronic system (HES) architecture – Part 3-4: System Management – Management procedures for network based control of HES Class 1

5 ISO/IEC 14543-3-5 Information technology – Home electronic system (HES) architecture – Part 3-5: Media and media dependent layers – Power line for network based control of HES Class 1

6 ISO/IEC 14543-3-6 Information technology – Home electronic system (HES) architecture – Part 3-6: Media and media dependent layers – Twisted pair for network based control of HES Class 1

7 ISO/IEC 14543-3-7 Information technology – Home electronic system (HES) architecture – Part 3-7: Media and media dependent layers – Radio frequency for network based control of HES Class 1

8 ISO/IEC TR 14543-4 Information technology – Home electronic system (HES) architecture – Part 4: Home and building automation in a mixed-use building

9 ISO/IEC 14709-1 Information technology – Configuration of customer premises cabling (CPC) for applications – Part 1: Integrated services digital network (ISDN) basic access

10 ISO/IEC 14709-2 Information technology – Configuration of customer premises cabling (CPC) for applications – Part 2: Integrated services digital network (ISDN) primary rate

11 ISO/IEC TR 14762 Information technology – Home control Systems – Guidelines for functional safety

12 ISO/IEC 14763-1 Information technology – Implementation and operation of customer premises cabling – Part 1: Administration

13 ISO/IEC 14763-2 Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation

14 ISO/IEC 14763-3 Information technology – Implementation and operation of customer premises cabling – Part 3: Testing of optical fibre cabling

15 ISO/IEC 15018 Information technology – Generic cabling for homes

16 ISO/IEC TR 15044 Information technology – Terminology for home electronic system (HES)

17 ISO/IEC 15045-1 Information technology – Home electronic system (HES) gateway – Part 1: A residential gateway model for HES

18 ISO/IEC TR 15067-2 Information technology – Home electronic system (HES) application model – Part 2: Lighting model for HES

19 ISO/IEC TR 15067-3 Information technology – Home electronic system (HES) application model – Part 3: Model of an energy management system

20 ISO/IEC TR 15067-4 Information technology – Home electronic system (HES) application model – Part 4: Security system for HES

21 ISO/IEC 18010 Information technology – Pathways and spaces for customer premises cabling

22 ISO/IEC 18012-1 Information technology – Home electronic system – Guidelines for product interoperability – Part 1: Introduction

23 ISO/IEC TR 24704 Information technology – Customer premises cabling for wireless access points

24 ISO/IEC TR 24746 Information technology – Generic cabling for customer premises – Mid-span DTE power insertion

25 IEC 60038 IEC standard voltages

26 IEC 60364 (all parts) Electrical installations of building (HD 384 series, modified)

27 IEC 60664-1 Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests

28 IEC 60948 Numeric keyboard for home electronic systems (HES)

29 IEC 60950-1 Information technology equipment – Safety – Part 1: General requirements (EN 60950-1, modified)

30 IEC TS 61000-1-2 Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of the functional safety of electrical and electronic equipment with regards to electromagnetic phenomena

31 IEC 61000-2-1 Electromagnetic compatibility (EMC) – Part 2-1: Environment – Description of the environment – Electromagnetic environment for low-frequency conducted diturbances and signalling in public power supply systems

32 IEC 61000-6-1 Electromagnetic compatibility (EMC) – Part 6-1: Generic standards – Immunity for residential, commercial and light-industrial environments (EN 61000-6-1, mod.)

33 IEC 61000-6-2 Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments (EN 61000-6-2, modified)

УДК 62-783:614.8:331.454:006.354 ОКС 13.110, 13.120, 35.240.99

Ключевые слова: безопасность функциональная; электронные системы; общие требования; электронные системы домов и зданий; функциональная безопасность; электронные системы домов и зданий, связанные с безопасностью

Подписано в печать 01.08.2014. Формат 60x84 1/8.
Усл. печ. л. 4,19. Тираж 33 экз. Зак. 2954.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru