ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ЕН 50491-4-1–2014

Общие требования к электронным системам жилых домов и общественных зданий (ЭСДЗ) и системам управления и автоматизации общественных зданий (СУАЗ)

Часть 4-1

Общие требования к функциональной безопасности изделий, предназначенных для включения в ЭСДЗ и СУАЗ

EN 50491-4-1:2012

General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) - Part 4-1: General functional safety requirements for products intended to be integrated in Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)
(IDT)

Москва
Стандартинформ
2014

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» и Федеральным государственным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации - «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык европейского регионального стандарта, 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 России от 10 июня 2014 г. № 520-ст

4 Настоящий стандарт идентичен европейскому региональному стандарту ЕН 50491-4-1:2012 «Общие требования к электронным системам жилых домов и общественных зданий (ЭСДЗ) и системам управления и автоматизации общественных зданий (СУАЗ). Часть 4-1. Общие требования к функциональной безопасности изделий, предназначенных для включения в ЭСДЗ и в СУАЗ» (EN 50491-4-1:2012 «General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) - Part 4-1: General functional safety requirements for products intended to be integrated in Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS)»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, 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 ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет (gost.ru)

Содержание

Введение

Строительство индивидуальных домов и аналогичных помещений обитания человека требуют различных электронных устройств для решения различных задач. Такие устройства, если они связаны через цифровые сети передачи данных, называют электронными системами жилых домов и общественных зданий (ЭСДЗ) и системами управления и автоматизации общественных зданий (СУАЗ).

Примерами ЭСДЗ/СУАЗ являются системы управления освещением, отоплением, водоснабжением, пожарной сигнализацией, жалюзи, различного уровня защиты и безопасности и т.д.

Сети ЭСДЗ/СУАЗ могут использовать различные средства коммуникации: шины электропитания, витые пары, коаксиальный кабель, радиочастотные или инфракрасные средства коммуникации, а также могут быть подключены к внешним сетям: телефонным, широкополосным, телевизионным, энергоснабжения и аварийной сигнализации.

Некоторые стандарты данного комплекса способствуют осуществлению общественных интересов, как это отражено в директивах Европейской Комиссии.

Изделия ЭСДЗ/СУАЗ, используемые в ЭСДЗ/СУАЗ, должны быть безопасными.

Настоящий стандарт устанавливает общие требования к функциональной безопасности для ЭСДЗ/СУАЗ в соответствии с принципами базового стандарта по функциональной безопасности ЕН 61508.

Настоящий стандарт определяет требования функциональной безопасности к изделиям и их установке. Данные требования основаны на анализе рисков в соответствии с ЕН 61508.

Целью настоящего стандарта является определение, насколько это возможно, всех требований к безопасности всех стадий жизненного цикла изделий ЭСДЗ/СУАЗ.

Настоящий стандарт применим только к ЭСДЗ/СУАЗ.

Настоящий стандарт предназначен для применения техническими комитетами по стандартизации при разработке или изменении стандартов на изделия/системы ЭСДЗ/СУАЗ и для производителей.

Изделия ЭСДЗ/СУАЗ, рассматриваемые в настоящем стандарте, не предназначены для безопасного применения. Дополнительные требования, связанные с безопасностью ЭСДЗ/СУАЗ, в соответствии с ЕН 61508 будет определены в части 4-2 комплекса стандартов ЕН 50491.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЩИЕ ТРЕБОВАНИЯ К ЭЛЕКТРОННЫМ СИСТЕМАМ ЖИЛЫХ ДОМОВ И ОБЩЕСТВЕННЫХ ЗДАНИЙ (ЭСДЗ) И СИСТЕМАМ УПРАВЛЕНИЯ И АВТОМАТИЗАЦИИ ОБЩЕСТВЕННЫХ ЗДАНИЙ (СУАЗ)

ЧАСТЬ 4-1

ОБЩИЕ ТРЕБОВАНИЯ К ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ИЗДЕЛИЙ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ВКЛЮЧЕНИЯ В ЭСДЗ И СУАЗ

General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS). Part 4-1.
General functional safety requirements for products intended to be integrated in HBES and BACS

Дата введения – 2015 – 05 - 01

1 Область применения

Настоящий стандарт определяет требования функциональной безопасности к изделиям и системам электронных систем жилых домов и общественных зданий (ЭСДЗ) и систем управления и автоматизации общественных зданий (СУАЗ), многоцелевой магистральной системе, в которой функции децентрализованы, распределены и связаны при помощи общего коммуникационного процесса. Данные требования также могут быть применены к распределенным функциям, реализуемым любым оборудованием, подсоединенным к ЭСДЗ, в случае если нет определенного стандарта функциональной безопасности для данного оборудования или системы.

Требования функциональной безопасности настоящего стандарта применяются вместе с соответствующими стандартами на изделие, если они имеется.

Настоящий стандарт входит в комплекс стандартов ЕН 50491.

Настоящий стандарт не обеспечивает требования функциональной безопасности для систем, связанных с безопасностью.

2 Нормативные ссылки

Для датированных ссылок применяют только указанное издание, для недатированных ссылок – последнее издание ссылочного документа, включая любые поправки.

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ЕН 50491-2 Общие требования к электронным системам жилых домов и общественных зданий (ЭСДЗ) и системам управления и автоматизации общественных зданий (СУАЗ). Часть 2. Условия окружающей среды (EN 50491-2, General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 2: Environmental conditions)

ЕН 50491-3 Общие требования к электронным системам жилых домов и общественных зданий (ЭСДЗ) и системам управления и автоматизации общественных зданий (СУАЗ). Часть 3. Требования электробезопасности (EN 50491-3, General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 3: Electrical safety requirements)

ЕН 50491-5 (все части) Общие требования к электронным системам жилых домов и общественных зданий (ЭСДЗ) и системам управления и автоматизации общественных зданий (СУАЗ) (EN 50491-5 (all parts), General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS))

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

ЕН 61709:1998 (МЭК 61709:1996) Электронные компоненты. Надежность. Нормальные условия для интенсивности отказов и моделей нагрузок для

преобразования (EN 61709:1998, Electronic components – Reliability – Reference conditions for failure rates and stress models for conversion (IEC 61709:1996))

ИСО 9000 Системы менеджмента качества. Основные положения и словарь (ISO 9000, Quality management systems – Fundamentals and vocabulary)

3 Термины и определения

3.1 **архитектура** (architecture): Особая конфигурация элементов комплектующего оборудования и программного обеспечения в системе.

[ЕН 61508-4:2010, статья 3.3.4]

3.2 **проверка подлинности** (authentication): Предназначено для удостоверения того, что компания, отправляющая сообщение, является тем, кого она подразумевает, и для подтверждения того, что сообщение идентично тому, которое было отправлено.

3.3 **авторизация** (authorization): Механизм по обеспечению того, что организация либо лицо, имеющее доступ к информации, функциям или услугам, имеют право на это.

3.4. **прерванная связь** (disturbed communication): Событие, когда по каким-либо причинам сообщение, подлежащее передаче, не завершено, обрезано, содержит ошибки либо имеет правильный формат, но несет в себе информацию, которая находится за пределами ожидаемых параметров для подобных сообщений.

3.5. **функциональная безопасность** (functional safety): Свобода от неприемлемого риска повреждения в результате работы ЭСДЗ/СУАЗ, в том числе в результате:

a) нормальной работы,

b) обоснованно прогнозируемого неправильного применения,

c) неисправности,

d) временных нарушений.

Примечания

1 Часть полной безопасности, связанная с управляемым оборудованием (далее – УО) и системой управления УО, которая зависит от правильного функционирования электрических/электронных /программируемых электронных (далее – Э/Э/ПЭ) систем, связанных с безопасностью, и внешних средств снижения риска [см. ЕН 61508-4:2010, статья 3.1.12].

2 Учтены определения МЭК/ТР 61000-2-1 и МЭК/ТС 61000-1-2.

3.6 **расстояние Хемминга** (hamming distance): Количество битов, в которых соответствующие символы двух слов одинаковой длины различны.

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

Примечание – Физическое повреждение или ущерб, причиняемый здоровью людей, либо ущерб имуществу или окружающей среде. [ЕН 61508-4:2010, статья 3.1.1]

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

[ИСО/МЭК Руководство 51, статья 3.5]

[ЕН 61508-4:2010, статья 3.1.2]

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

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

Примечания

1 Приводит ли опасное событие к нанесению вреда зависит от того, подвергаются ли люди, имущество или окружающая среда последствиям опасного события и, в случае возможного причинения вреда людям, могут ли они избежать последствий этого события после того, как оно произошло

2 Адаптировано из ЕН 61508-4:2010, статья 3.1.4.

3.10 **электронные системы жилых домов и общественных зданий, ЭСДЗ/СУАЗ** (home and building electronic systems, HBES/BACS): Многоцелевая

магистральная система, в которой функции децентрализовано распределены и связаны при помощи общего процесса связи.

Примечание – ЭСДЗ используют в жилых домах и общественных зданиях, в том числе в их окрестностях. Функциями ЭСДЗ могут быть: переключение, регулирование без обратной связи, управление, регулирование с обратной связью, надзор и контроль и др.

3.11 **изделие ЭСДЗ** (HBES product): Изделие, например, аппаратное средство, программно-аппаратное средство, связанное с ними программное обеспечение и средство конфигурации, предназначенное для использования в ЭСДЗ/СУАЗ.

3.12 **изделие** (product): Изделие, например, аппаратное средство, программно-аппаратное средство, связанное с ними программное обеспечение и средство конфигурации.

3.13 **документация на изделие** (product documentation): Документы производителя по установке и эксплуатации такие, как каталог производителя, товарно-маркетинговая и другая информация об изделии на бумажных или электронных носителях.

3.14 **система обеспечения безопасности** (safety related system): Спроектированная система, которая выполняет требуемые функции безопасности, необходимые для достижения или поддержания безопасного состояния УО; а также предназначена для достижения как в отдельности, так и совместно с другими Э/Э/ПЭ системами обеспечения безопасности, а также мерами по снижению риска, основанными на других технологиях, необходимой полноты безопасности для требуемых функций безопасности.

Примечания

1 Термин относится к системам, связанным с безопасностью, которые предназначены совместного с другими средствами снижения риска для достижения необходимого уровня уменьшения риска, чтобы соответствовать необходимому допустимому риску.

2 Системы, связанные с безопасностью, спроектированы так, чтобы защитить УО от перехода в опасное состояние при помощи соответствующих мер по обнаружению условий, которые могут

привести к опасному событию. Отказ системы, связанной с безопасностью, должен быть включен в список событий, ведущих к установленной опасности или рискам. Хотя могут быть другие системы с функциями безопасности, именно системы, связанные с безопасностью, были специально разработаны для достижения необходимого допустимого риска. Системы, связанные с безопасностью, можно разделить на управляющие системы, связанные с безопасностью, и защищающие системы, связанные с безопасностью, и они имеют два режима работы (IEC 61508-4, статья 3.5.12).

3 Системы, связанные с безопасностью, могут являться неотъемлемой частью систем управления УО или могут быть связаны с УО с помощью датчиков и/или исполнительных механизмов. Иначе, необходимый уровень полноты безопасности можно достичь реализацией функций обеспечения безопасности в системе управления УО и, возможно, также с помощью дополнительных отдельных и независимых систем, или функции обеспечения безопасности могут быть реализованы, как отдельные и независимые системы, специализированные на безопасности.

4 Система, связанная с безопасностью, может быть спроектирована для:

a) предотвращения опасных событий (т.е. если системы, связанные с безопасностью, выполняют их функции обеспечения безопасности, то никакое опасное событие не произойдет);

b) ослабления воздействия опасного события, тем самым уменьшая риск с помощью уменьшения последствий;

c) достижения комбинации перечислений a) и b).

5 Человек может стать частью системы, связанной с безопасностью, например, человек может получать информацию от программируемого электронного устройства и выполнять действия по обеспечению безопасности, основанные на данной информации, либо выполнять действия по обеспечению безопасности с помощью данного программируемого электронного устройства.

6 Термин включает в себя все аппаратные средства, программное обеспечение и вспомогательные средства, например, источники электропитания, необходимые для выполнения конкретной функции безопасности (датчики, другие устройства ввода, исполнительные элементы (соленоиды) и другие устройства вывода включены в состав системы, связанной с безопасностью).

7 Система, связанная с безопасностью, может быть основана на широком спектре технологий, в том числе электрических, электронных, программируемых электронных, гидравлических и пневматических технологиях.

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

Примечание – О данном термине см. приложение А ЕН 61508-4:2010.

[ЕН 61508-4:2010, статья 3.1.6]

3.16 **разумно предсказуемое некорректное использование** (reasonably foreseeable misuse): Использование изделия, процесса или услуги в условиях или с целью, не предусмотренной поставщиком, которое может произойти из-за использования изделия, процесса или услуги в сочетании с или в результате легко предсказуемого поведения человека.

[ЕН 61508-4:2010, статья 3.1.14 и ИСО/МЭК Руководство 51:1999, статья 3.14]

3.17 **функция обеспечения безопасности** (safety function): Функция, реализуемая Э/Э/ПЭ системой, связанной с безопасностью либо другими мерами по снижению риска, которая предназначена для достижения и поддержания безопасного состояния УО для конкретного опасного события.

[ЕН 61508-4:2010, статья 3.5.1]

3.18 **УО** (EUC, Equipment Under Control): Управляемое оборудование.

[ЕН 61508-4:2010, таблица 1]

4 Общие требования

4.1 Основные положения

Требования функциональной безопасности к системе распространяют на работу сети и на работу связываемых этой сетью изделий ЭСДЗ/СУАЗ:

1) отказ любой сети или любой части ЭСДЗ/СУАЗ не должен стать причиной небезопасности системы, изделия или управляемого оборудования;

2) во время эксплуатации безопасная работа отдельных изделий ЭСДЗ/СУАЗ не должна зависеть только от системы;

3) во время эксплуатации системное взаимодействие любого изделия(ий) с любым другим изделием(ями) не должно привести к небезопасной работе системы.

4.2 Метод установления требований

4.2.1 Общие положения

Требования функциональной безопасности приводят в соответствии с жизненным циклом по ЕН 61508-1:

1) стадия формирования концепции изделия;

2) условия эксплуатации;

3) идентификация опасностей и опасных событий;

4) анализ опасности и риска, меры по снижению риска;

5) реализация мер по снижению риска;

6) подтверждение соответствия;

7) техническое обслуживание;

8) установка и пуско-наладочные работы;

9) вывод из эксплуатации.

Технические комитеты по стандартизации и/или разработчики изделий должны использовать требования настоящего стандарта в целях удовлетворения требований безопасности изделия, но нет необходимости включать их в сам процесс ЕН 61508.

4.2.2 Окружающая среда применения ЭСДЗ/СУАЗ

Следует принимать во внимание окружающую среду применения ЭСДЗ/СУАЗ.

4.2.3 Источники опасности

Были рассмотрены следующие источники опасности:

1) материал и конструкция;

2) надежность;

3) нормальная работа;

4) случайное взаимодействие с другими изделиями;

5) взаимодействие с другими изделиями ЭСДЗ/СУАЗ;

6) ненормальные условия;

7) предсказуемое неправильное использование, включая загрузку несанкционированного кода со злым умыслом.

Примечание – В том числе непреднамеренное изменение программного обеспечения;

8) срок службы;

9) окружение.

4.2.4 Опасные события

Для анализа (информационной шины и питающей сети 230 В/400 В) должны быть учтены следующие опасные события:

1) отказ сети питания;

2) замыкание в шине;

3) перенапряжение на линии шины;

4) перенапряжение питающей сети;

5) повреждение изоляции (температурное, импульсное, механическое);

6) неправильное соединение;

7) высокая температура;

8) пожар;

9) механический удар, вибрация;

10) коррозия;

11) электромагнитная помеха;

12) нарушение коммуникации;

13) загрязнение;

14) окончание срока службы компонента/изделий;

15) разумно предсказуемое неправильное использование;

16) отказ программного обеспечения;

17) перегрузка;

18) потеря надежности;

19) поломка материала (механическая);

20) неподходящий проект/конструкция;

21) отключение поврежденного оборудования и подсистем;

22) дистанционное управление;

23) отправка команды от двух источников к одному изделию, например, в исполнительное устройство;

24) отказы системы.

4.2.5 Происхождение требований

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

В любом случае там, где оцененный класс риска указывает на неприемлемый риск, необходимо применение мер по снижению риска, а также определение уровня влияния этого снижения риска и его подтверждение соответствия. Предлагают некоторые меры по снижению риска, а также указывают на область распространения соответствующего стандарта на изделие. Если производители планируют разрабатывать изделия/системы ЭСДЗ/СУАЗ, которые обнаруживают опасные события, не охваченные в 4.2.4, необходимо провести анализ риска в соответствии с ЕН 61508.

5 Требования функциональной безопасности

Примечание – Ссылки на опасные события пункта 4.2.4 приведены ниже в круглых скобках.

5.1 Основные положения

Анализ в соответствии с ЕН 61508 указывает на то, что функциональная безопасность зависит от проектирования и производства изделий, а также от правильного использования изделий в инженерном оборудовании здания.

Подразделы 5.2 – 5.7 содержат требования для изделий ЭСДЗ/СУАЗ и для предоставления информации, необходимой для правильной установки, работы и технического обслуживания данных изделий.

Требования о соответствии являются необходимыми и даны для изделий и для проверки обеспечения необходимой информацией.

Все упомянутые тесты изделий являются типичными тестами.

Основа и причины следующих требований описаны в приложении В.

5.2 Электроснабжение

5.2.1 В случае отказа в системе электроснабжения необходимо провести безопасный запуск изделий после восстановления подачи электропитания. (1)

Примечание – Безопасный запуск можно выполнить с помощью:

– хранения информации о состоянии и использование данной информации для восстановления функционирования после включения питания;

– переключение изделия в определенное состояние в зависимости от области применения изделий;

– расчета безопасного состояния на основе информации, доступной из системы (из контроллера, если имеется, и/или из каждого изделия);

– поддержания достаточного запаса мощности, обеспечивая соответствующее резервное время для изделия и/или блока питания, чтобы подсоединенные к блоку питания изделия могли перейти в безопасное состояние.

5.2.2 Маркировка и инструкции изделий должны быть выполнены так, чтобы избежать риска неправильного подсоединения. (3) (6)

Изделия должны быть промаркированы стойкими чернилами и иметь разборчивое написание.

Соответствие проверяют по документации на изделие и при необходимости при помощи теста на устойчивость и отчетливость маркировки согласно стандарту на конкретное изделие.

5.2.3 Конструкция и проект изделия должны предотвращать неправильное подсоединение. Его можно избежать при соответствующем группировании соединений. (6)

Соответствие параметров проверяют тестированием изделия.

5.3 Окружающая среда

5.3.1 Изделие должно быть спроектировано для рабочей температуры, соответствующей максимальному номинальному значению напряжения, необходимому для условий работы применения, и должен стабильно работать в указанном температурном диапазоне. (7)

Соответствие проверяется тестированием изделия согласно стандарту на конкретное изделие, а в случае отсутствия такового, согласно ЕН 50491-2 и применимым базовым стандартам по безопасности.

5.3.2 Изделия и компоненты должны быть устойчивыми к высоким температурам и не должны служить источником распространения огня. (8)

Соответствие проверяют тестированием изделия согласно стандарту на конкретное изделие, а в случае отсутствия такого стандарта, согласно применимым базовым стандартам по безопасности.

5.3.3 Изделия должны быть устойчивыми к механическим нагрузкам, соответствующим применению(-ям). (9)

Соответствие проверяют тестированием изделия согласно стандарту на конкретное изделие, а в случае отсутствия такого стандарта, согласно ЕН 50491-2 и применимым базовым стандартам по безопасности.

5.4 Срок службы

Изделия должны быть спроектированы на указанный срок эксплуатации согласно МЭК 61709:1996 подраздел 5.2 и приложению А или на указанное число циклов включений при нормальных условиях.

Паспорт изделия должен содержать инструкции по его эксплуатации и техническому обслуживанию в целях обеспечения срока эксплуатации. (14)

Соответствие проверяют в ходе инспекции документации.

5.5 Разумно предсказуемое некорректное использование

5.5.1 Риск нежелательного скачивания неверного прикладного программного обеспечения или параметров в данное изделие должен быть минимизирован. (15)

Примечание – Следует применять следующие меры:

– разработать средства конфигурации;

– использовать идентификацию изделий и сравнение их профайлов на уровне сетевого управления;

– устанавливать пароль;

– использовать проверку подлинности;

– следовать документации на изделие;

– обучить специалиста по установке или оператора правильной работе изделием.

Соответствие проверяют тестированием изделия и/или в ходе инспекции документации на изделие.

5.5.2 Необходимо убедиться в установке верных конфигураций и соответствующих параметров. (15)

Примечание – Следует применять следующие меры:

– строго специфицировать диапазоны параметров;

– ограничить возможности по конфигурированию для конечного пользователя;

– допускать к конфигурации только опытных сотрудников (см. ЕН 50090-2-1);

– провести проверку на совместимость установщиком или с помощью инструментальных средств;

– проверить на соответствие конфигурациям.

Соответствие проверяют проверкой действительных конфигураций с запланированными (рекомендуемыми).

6.5.3 Необходимо принимать меры для обнаружения и/или отображения отсутствующих или не полностью сконфигурированных изделий в процессе конфигурации. (15)

Примечание – Возможны следующие меры:

– разработать средства конфигурации;

– следовать рекомендуемым процедурам установки.

Соответствие проверяют тестированием изделия и/или в ходе инспекции документации на изделие.

5.6 Программное обеспечение и передача данных

5.6.1 Процесс разработки программного обеспечения должен соответствовать ЕН ИСО 9000 или применимым стандартам. (16)

Соответствие проверяют в ходе инспекции документации на процессы или применимых сертификатов.

5.6.2 Необходимо принимать меры по проверке на корректность работы программного обеспечения и на верность конфигураций. Если обнаруживают неправильную работу, изделие должно восстановить корректные значения или вернуться к определенному состоянию. (16)

Соответствие проверяют в ходе инспекции технологической документации программного обеспечения продукта.

5.6.3 При необходимости, учитывая применение, могут быть приняты меры внутри изделий по ограничению нагрузки трафика на канал передачи данных. (12)(17)

Примечание – Возможны следующие меры:

– ограничить цикл передачи данных;

– ограничить число сообщений в единицу времени для изделия;

– ограничить цикл опроса.

Соответствие проверяют в ходе инспекции документации на изделие и, если это возможно, тестированием изделия.

5.6.4 Прием сообщений от нескольких источников не должен влиять на правильную работу изделия и вызывать какие-либо опасности. (23)

Примечание – Возможны следующие меры:

– проверить адрес источника, если существует иерархия источников;

– использовать правило: обработка в порядке поступления;

– руководствоваться правилом: последнее сообщение - решающее;

– защитить процесс, завершив его до того, как поступят новые сообщения, которые могут повлиять на его протекание;

– защитить процесс, прервав и перезапустив его;

– защитить процесс, отключив и включив его;

Соответствие проверяют в ходе инспекции документации на изделие и, если это возможно, тестированием изделия.

5.6.5 Изделия должны реагировать на сброс системы (если он происходит), переходя в определенное состояние. (24)

Соответствие проверяют в ходе инспекции документации на изделие и, если это возможно, тестированием изделия.

5.6.6 Доступ к ручному конфигурированию параметров системы должен быть ограничен. (24)

Примечание – Возможны следующие меры:

– использовать инструмент конфигурирования (аппаратный или программный);

– использовать пароль и/или удостоверение подлинности;

– установить защиту от несанкционированного доступа;

– выполнять комбинацию или последовательность действий;

– использовать скрытые средства конфигурации;

– убрать все прямые детальные описания ручной конфигурации в руководстве по эксплуатации изделия (то же самое применительно к автоматической конфигурации).

Соответствие проверяют в ходе инспекции документации на изделие и, если это возможно, тестированием изделия.

5.6.7 Прерванная связь

5.6.7.1 Безопасная работа изделия не должна зависеть от работы других изделий в системе или применении. (12)

Примечание – Возможны следующие меры:

– использовать циклическую передачу данных;

– выполнять проверку диапазона полученных значений.

Соответствие проверяют в ходе инспекции результатов тестирования изделия либо в ходе инспекции документации на изделие.

5.6.7.2 Прерванные сообщения должны быть успешно идентифицированы. В случае обнаружения прерванных сообщений, следует предпринять определенные меры по обеспечению безопасной работы. Значение расстояния Хемминга должно быть не менее 2. (11) (12)

Примечание – Возможны следующие меры:

– принимающее изделие может отклонить или изменить сообщение;

– отправитель может повторить свое сообщение.

Соответствие проверяют в ходе инспекции результатов тестирования изделия либо в ходе инспекции документации на изделие.

5.6.7.3 Необходимо предотвращать рассылку ложных, но формально правильных сообщений.

Соответствие проверяют в ходе применимого теста на электромагнитную совместимость по ЕН 50491-5 (все части).

5.6.7.4 Если сообщения потеряны, необходимо, чтобы они были отображены и высланы повторно. (12) (17)

Примечание – Возможны следующие меры:

– использовать механизмы подтверждения приема сообщений в коммуникационных системах, а также в применяемых системах;

– включить отображение или визуализацию статуса обратной связи;

– в случае использования однонаправленных изделий, использовать подходящий систематический повтор.

Соответствие проверяют в ходе инспекции результатов тестирования изделия либо в ходе инспекции документации на изделие.

5.7 Дистанционное управление

5.7.1 Основные рекомендации

Предыдущие требования распространяют также и на дистанционное управление в помещении.

Сетевые розетки, находящиеся под дистанционным управлением, должны быть промаркированы так, чтобы их можно было визуально отличать от других розеток, используемых пользователем. Либо эти розетки должны быть устроены так, чтобы исключить возможность использования обычных вилок к розеткам, не предназначенным для дистанционного управления. (22)

5.7.2 Управление внутри одного здания или в его непосредственной близости

Изделия или подсистема, связанная с изделием, которое может быть источником вреда, а также обладающие дистанционным управлением внутри одного помещения или в его непосредственной близости, должны предусматривать автономные средства управления или выполнения/отмены дистанционных операций.

Примечание – Возможны следующие меры:

– использовать автономные средства управления потенциально вредоносными изделиями;

– применять автономные средства управления на соседних потенциально вредоносных изделиях;

– использовать коммуникационные входы, обеспечивающие автономное управление.

Соответствие проверяют в ходе инспекции изделия либо документации на изделие.

5.7.3 Управление за пределами здания

5.7.3.1 Потенциально вредоносные изделия или подсистемы, обладающие дистанционным управлением, находящиеся вне помещения, должны отвечать

условиям для их автономных средств по обязательному выполнению дистанционных операций.

Примечание – Возможны следующие меры:

– использовать автономные средства управления потенциально вредоносными изделиями;

– применять автономные средства управления на соседних потенциально вредоносных изделиях;

- использовать коммуникационные входы, обеспечивающие автономное управление;

- использовать автономные средства отключающие межсетевой шлюз или другое изделие удаленного доступа.

Соответствие проверяют в ходе инспекции изделия либо документации на изделие.

5.7.3.2 Следует использовать особый механизм авторизации или удостоверения подлинности дистанционного контроля, осуществляемого за пределами здания (см. таблицу 1). Такой механизм может быть применен в системе (брандмауэр или межсетевой шлюз) либо на уровне изделия. (22)

Примечание – Авторизация может быть следующих видов:

- с использованием пароля для удостоверения подлинности или авторизации;

- с доступом по выделенному каналу.

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

Требования	Рекомендации по выполнению
Предотвращение непреднамеренных операций	Ограничить внешние операции - оставив лишь авторизованные напрямую владельцем, например, с задержкой по времени; - оставив, лишь те, которые были созданы внутри шлюза
Непреднамеренные операции по управлению сетью недопустимы	Необходимо использовать инструментальные средства (физические или на основе программного обеспечения) либо следующие коды доступа: - простой код, 4 символа; - более длинный код. (простой и более длинный коды используют в закрытой среде передачи данных, но они не подходят для открытой среды, поскольку являются передаваемыми);

	- шифрование и/или проверка подлинности
Необходимо проверить подлинность целевого изделия и «загрузчика»	Например «сертифицированный компонент программного обеспечения»

Соответствие проверяют в ходе инспекции изделия либо документации на изделие.

5.7.4 Управление

5.7.4.1 Следует использовать особый механизм авторизации или проверки подлинности дистанционного управления, включая конфигурацию и загрузку данных из источников за пределами здания (см. таблицу 1). Такой механизм может быть применен в системе (брандмауэр или межсетевой шлюз) либо на уровне изделия. (22)

Примечание – Авторизация может быть следующих видов:

- с использованием пароля для проверки подлинности или авторизации,

- с доступом по выделенному каналу.

Соответствие проверяют в ходе инспекции изделия либо документации на изделие.

5.7.4.2 Следует предпринять соответствующие меры для точного соответствия реальной сети изображению этой дистанционной сети. (22)

Примечание – Возможны следующие меры:

- обеспечить существование единственной точной копии базы данных системы;

- использовать механизмы проверки базы данных дистанционной системы на соответствие реальной сети;

- система должна иметь функцию самодокументирования (центральную или распределенную).

Соответствие проверяют в ходе инспекции изделия либо документации на изделие.

Приложение А
(справочное)

Пример метода определения уровней полноты безопасности

А.1 Общие положения

При помощи рассматриваемого метода описывают допустимый риск:

– Э/Э/ПЭ систем обеспечения безопасности,

– систем обеспечения безопасности, основанных на других технологиях,

– внешних средств уменьшения риска, которые будут определены.

На рисунке А.1 показана общая концепция снижения риска, см. рисунок А.1 ЕН 61508-5.

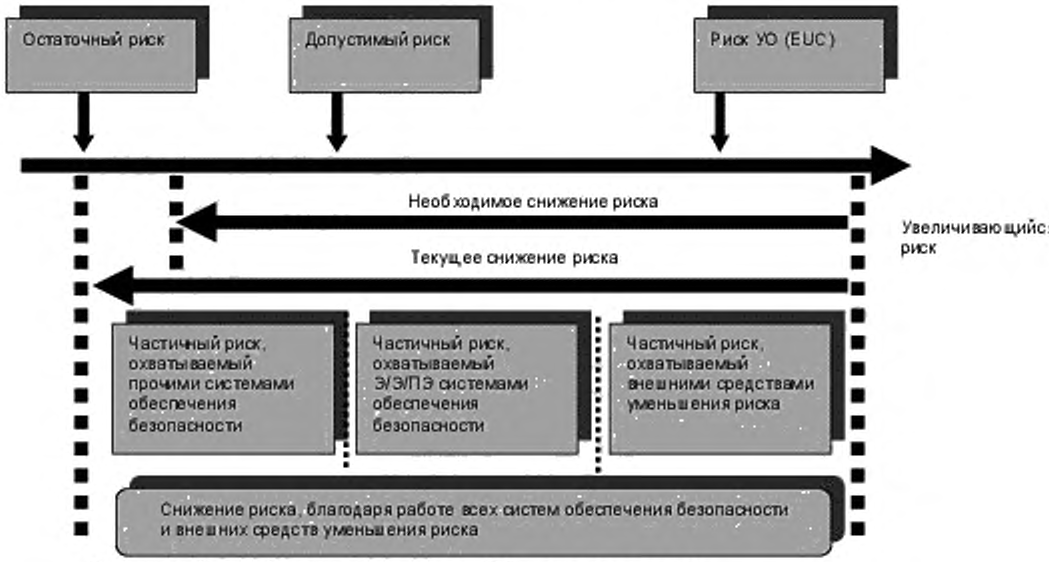

Рисунок А.1 – Снижение риска. Общая концепция

А.2 Термины и определения

В данном приложении использованы 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 оговоренных условиях в течение заданного периода.

[ЕН 61508-4, статья 3.5.4]

Примечания

1 Чем выше уровень полноты безопасности, тем ниже вероятность того, что система, связанная с безопасностью, не сможет выполнить указанные функции безопасности или будет не в состоянии принять указанное состояние, когда это потребуется.

2 Имеется четыре уровня полноты безопасности для систем (см. ЕН 61508-4, пункт 3.5.8).

3 При определении полноты безопасности следует учитывать все причины отказов (и случайных отказов аппаратных средств, и систематических отказов), которые ведут к небезопасному состоянию, например, отказы аппаратных средств, отказы, вызванные программным обеспечением и отказы, вызванные электрическими помехами. Некоторые из этих типов отказов, например, случайные отказы аппаратных средств, могут быть охарактеризованы количественно, с использованием таких параметров, как интенсивность отказов в опасном режиме или вероятность того, что система защиты, связанная с безопасностью, не сможет выполнить запрос. Однако полнота безопасности системы также зависит и от многих факторов, которым нельзя дать точную количественную оценку и которые могут быть оценены только качественно.

4 Полнота безопасности включает полноту безопасности аппаратных средств и полноту безопасности по отношению к систематическим отказам.

5 Данное определение основано на определении безотказности (надежности) систем, связанных с безопасностью, при выполнении ими функций безопасности (определение надежности - см. 191-12-01 в Международном электротехническом словаре).

А.2.2 **уровень полноты безопасности; УПБ** (safety integrity level): Дискретный уровень (принимающий одно из четырех возможных значений), определяющий требования к полноте безопасности для функций безопасности, который ставится в соответствие Э/Э/ПЭ системам обеспечения безопасности: УПБ, равный 4, характеризует наибольшую полноту безопасности, УПБ, равный 1, отвечает наименьшей полноте безопасности.

Примечания

1 Целевые величины отказов (см. ЕН 61508-4, пункт 3.5.17) для четырех уровней полноты безопасности указаны в таблицах 2 и 3 ЕН 61508-1.

2 УПБ используются при определении требований полноты безопасности для функций

безопасности, которые должны быть распределены по Э/Э/ПЭ системам, связанным с безопасностью.

3 УПБ не является свойством системы, подсистемы, элемента или компонента. Правильная интерпретация фразы: «УПБ системы, связанной с безопасностью, равен *n*, где *n* = 1, 2, 3 или 4» – система потенциально способна к реализации функций безопасности с уровнем полноты безопасности до *n*.

[ЕН 61508-4, статья 3.5.8]

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

Применяют приложение В ЕН 61508-5. Для удобства пользователя здесь приведены некоторые из сведений, указанных в приложении В ЕН 61508-5.

В таблице А.1 показана взаимосвязь вероятности (частоты) риска, его последствий и классов, а в таблице А.2 отражена классификация классов риска при помощи 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
Вероятные	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
Невероятные	Класс III	Класс III	Класс VI	Класс VI
Немыслимые	Класс VI	Класс VI	Класс VI	Класс VI
Примечание – Фактическое распределение [заполнение] риска по классам I, II, III и IV должно быть секториально зависимым и также должно зависеть от того, какие частоты, вероятности и т.д. являются реальными, поэтому 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	Нежелательный риска и допустимой только, 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 показана разработка необходимых методов снижения риска в случае опасных ситуаций, упомянутых в пункте 4.2.4 и соответствующих элементов событий. В ходе анализа были разработаны требования, изложенные в разделе 5.

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

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

Таблица В.1 – Требования к безопасности и снижение риска

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
1 Отказ сети питания	1-1 Отключение питания шины	Только в шине	Изделие должно сохранять всю информацию состояния, необходимую во избежание риска в случае включения питания и/или в случае необходимости перевести систему/изделие в безопасный режим
	1-2 Питание в шине отсутствует		
	1-3 Возобновление питания в шине		См. 1-1
	1-4 Отключение питания шины от сети 220 В		См. 1-1. Блок питания должен работать до 80 мсек
	1-5 Питание в шине от сети 220 В отсутствует		
	1-6 Отключение резервного питания продукта		
	1-7 Резервное питание продукта отсутствует		
	1-8 Возобновление питания только в сети		См. 1-1
	1-9 Возобновление питания в сети и в шине		См. 1-1

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
2 Короткое замыкание линии шины	2-1 Полное короткое замыкание	Изделия с питанием 220 В и/или с дополнительными источниками питания более не контролируют через шину, хотя на них подано питание	См. 1-1. Сеть шины должна быть защищена от перегрузки, см. ЕН 50491-3
	2-2 Неполное короткое замыкание	Некоторая часть линий шины еще может функционировать. Нет индикации в блоке питания	См. 12 для устройств без связи. См. 1-1 для изделий без питания в шине
	2-3 Повышенный ток в шине	Шина прекращает сообщать об отключении подачи питания устройством защиты	См. 12. Другой вариант: отключается блок питания и/или выдает специальный сигнал. Другой вариант решения проблемы: разделить независимые линии и разные блоки питания и оставить неисправность локальной
3 Перенапряжение на шине	3-1 Нет последствий		Выполняют требования ЕН 50491-3. Электростатический и индукционный заряд: - линия шины с безопасным сверхнизким напряжением (SELV[1]) с защитным полным сопротивлением относительно земли для временных перенапряжений; - постоянные опасные перенапряжения вряд ли возможны из-за применения безопасного сверхнизкого напряжения (SELV). Повреждение изоляции: - изоляция ЭСДЗ/СУАЗ и изделий ЭСДЗ/СУАЗ от других сетей с U_R не менее 250 В и следовательно с U_R не менее 80 В переменного тока для PELV[2]/SELV, в соответствии с ЕН 50491-3; - опционально: защита устройства защитного отключения (на стороне сети)
	3-2 Автоматический сброс		Опционально, нет требований
	3-3 Ручной сброс		Опционально, нет требований
	3-4 Неисправность изделия		Даже есть изделие ЭСДЗ/СУАЗ подключено к сети с напряжением 230 В, оно не должно наносить вред (или вред должен быть маловероятен, из-за оригинального соединения для SELV)

[1] SELV – безопасное сверхнизкое напряжение.
[2] PELV – заземлённая система безопасного сверхнизкого напряжения.

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
4 Перенапряжение питающей сети	4-1 Нет воздействия на блок питания		Сеть 220/400 В: Изделия должны соответствовать требованиям ЕН 50491-3. Тестовое напряжение для массивного изолятора или герметизированнных компонентов при проверке изоляции между сетью и ЭСДЗ/СУАЗ равно 4 кВ переменного тока (тестирование проводят в соответствии с ЕН 60664-1:2007)
	4-2 автоматический сброс блока питания		Опционально, нет требований
	4-3 ручной сброс блока питания		Опционально, нет требований
	4-4 Неисправность блока питания		Следите за тем, чтобы из-за неисправности блока питания не начался пожар или не произошел взрыв
5 Повреждение изоляции (температурное, импульсное, механическое)	5-1 Короткое замыкание		Должны быть установлены: - в сети – защита от избыточного тока, в соответствии с [12]; - в шине – ограничение тока (см. ЕН 50491-3)
	5-2 Поступает опасное напряжение		Следует соблюдать: - для изделий и сетевых кабелей – правила установки по [12]; - для изделий и кабелей шин – требования к SELV
	5-3 Открыты токоведущие части		См. ЕН 50491-3. Комитеты по разработке изделия должны выработать специальную защиту от механического воздействия, с учетом окружающей среды и, при необходимости, добавить дополнительную внешнюю защиту
6 Неправильное подключение	6-1 На стороне шины	Неправильная полярность	Конструкция и проект изделия должны защищать от неправильных подключений. Маркирование и соответствующие описания помогут избежать неправильных подключений. Если изделие подключено неправильно – оно не должно работать. Изделие не должно вызывать возгораний или взрывов или отрицательно влиять на электрическую безопасность
	6-2 На стороне сети	Соединение клемника с сетью питания	См. 3-4 и 6-1. Разъемы шины и сети не должны быть взаимозаменяемыми. Конструкция и проект изделия должны защищать от неправильных подключений. Маркирование и соответствующие описания помогут избежать неправильных подключений. Изделие не должно вызывать возгораний или взрывов или отрицательно влиять на электрическую безопасность
	6-3 Соединение изделий с разными физическими слоями/магистральными системами в разных SELV		Конструкция и проект изделия должны защищать от неправильных подключений. Маркирование и соответствующие описания помогут избежать неправильных подключений. Изделие не должно вызывать возгораний или взрывов или отрицательно влиять на электрическую безопасность

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
7 Перегрев	7-1 Нарушение функционирования		Исправная работа изделия возможна только в определенном температурном диапазоне ЕН 50491-2
	7-2 Внешняя среда		Управление подсистемой, работающей при температуре (внешней среды и/или поверхности) более 60 °С: - изделие рассчитано на более высокую температуру внешней среды; - в случае отказа шины подсистема должна перейти в безопасный режим, который, может потребовать ручного управления
8 Возгорание			В стандарты изделия должны быть включены требования к пожарной безопасности
9 Механический удар, вибрация			Изделия ЭСДЗ должны соответствовать ЕН 50491-2. Комитет по разработке изделия может добавить дополнительные требования
10 Коррозия			В стандарты изделия должны быть включены соответствующие требования
11 Электромагнитная совместимость			В ходе тестов на электромагнитную совместимость по ЕН 50491-5: - должна быть обеспечена идентификация прерванных сообщений; - не должны возникать ложные, но формально правильные сообщения
12 Прерванная связь	12-1 Сигнал прерван		Должна быть обеспечена идентификация прерванных сообщений. Расстояние Хемминга, зависимая от среды частота повторения. Необходимое расстояние Хемминга должно быть более 2. Получение надлежащих сообщений должно быть обеспечено также в случае конфликтов (предотвращение конфликтов, обнаружение конфликтов, повтор, подтверждение сообщений и т.д.)
	12-2 Отсутствует часть шины	Например, датчик грозы	Необходимо управлять постоянными/циклическими передатчиками. Безопасная работа изделия должна быть осуществлена независимо от других изделий
13 Загрязнение			Руководствуются ЕН 50491-2

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
14 Конец срока службы компонента/ изделия	Общее		Комитеты по разработке изделий должны установить требования к минимальному сроку службы (надежность, циклы проверки и т. д.) и/или при необходимости разработать руководства по правилам эксплуатации изделия, например, указать дату разработки.
	14-1 Перегрев или возгорание	Неправильное функционирование	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 неправильно, либо наблюдается перегрев или возгорание	См. 7, 10 и 12
	14-4 Потеря или изменение памяти	Устройство не работает или связь установлена неправильно	См. 16
	14-5 Разрыв связи	Не удается установить связь	См. 12
	14-6 Внутреннее отключение питания	Устройство не работает	См. 12-2
	14-7 Отказ технических средств локальной функции управления	Невозможно произвести внешние операции	Устранимо, нет дополнительного риска
	14-8 Отказ технических средств, влияющий на связь		См. 12
	14-9 Ошибка прошивки		См. 16
	14-10 Кроткое замыкание в шине		См. 2

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
15 Разумно предсказуемое некорректное использование. Диверсия не относится к изделию ЭСДЗ/СУАЗ	15-1 Загрузка неправильного программного обеспечения	Стабилизация программного обеспечения	Избегать загрузки неправильного программного обеспечения, например: - используя инструмент; - применяя идентификацию изделия и его возможностей с помощью сетевого управления; - используя пароль; - обучив оператора работе с устройством
	15-2 Неправильная конфигурация или параметры		В зависимости от применения, комитет по разработке изделия должен установить предельные значения параметров. Конечный пользователь должен обладать ограниченными возможностями конфигурирования. Только профессионалы могут иметь доступ к конфигурированию изделия. Выполнить проверку непротиворечивости, например, с помощью инструментальных средств, средств конфигурации и т. д. Проверка непротиворечивости может быть произведена средством инсталяции
	15-3 Незавершенная конфигурации	Отсутствие изделия	См.12. Средства конфигурации должны оповещать об отсутствии изделия в процессе конфигурации
	15-4 Неправильное использование типов переменных или команд		Только профессионалы могут иметь доступ к конфигурации изделия. Средства конфигурации должны проверять правила взаимодействия. Изделия/системы/ приложения ЭСДЗ/СУАЗ должны соблюдать правила взаимодействия
16 Ошибка программного обеспечения	16-1 Ошибка программного обеспечения		Процесс разработки должен соответствовать стандартам серии ISO 9000 или подобным
	16-2 Ошибка памяти		Постоянно выполняйте проверку памяти и принимайте соответствующие меры
17 Перегрузка	17-1 Перегрузка трафика шины	Задержка подачи сигналов	Необходимо управлять постоянными/циклическими передатчиками. Необходимо рассмотреть оптимальный/максимальный загружаемый трафик в каждой среде передачи данных. Проект приложения должен оптимизировать трафик шины
		Потерянные сообщения	С помощью протокола можно разобраться с потерями сообщений (например, через повторную передачу). Отображение статуса
18 Надежность			Это не опасность, а только мера ее частоты
19 Повреждение материала (механическое)	19-1 Отказ в результате износа	Открыты токоведущие части	Для соблюдения электрической безопасности следует: - руководствоваться стандартами изделия или общим стандартом ЕН 50491-3; - проверить включены ли в инструкцию указания по правильной установке оборудования
	19-2 Использование недопустимо	Открыты токоведущие части	
	19-3 Неправильная установка оборудования	Открыты токоведущие части	
	19-4 Неверный тип материала	Открыты токоведущие части	

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
20 Неправильный проект/конструкция	20-1 Срок службы существенно сокращается		См. 14
	20-2 Возгорание/взрыв из-за перегрузки		Меры изложены в стандартах изделия
	20-3 Перегрев из-за перегрузки		
	20-4 Разрыв соединительных кабелей		
	20-5 Механическая блокировка механизма переключения из-за деформации корпуса		
	20-6 Механическая блокировка из-за коррозии		
	20-7 Повреждение/вред от краев корпуса		
	20-8 Открыты опасные токоведущие части		
	20-9 Выход из строя из-за перегрузки		
	20-10 Выход из строя из-за недостаточной электромагнитной совместимости		
21 Отключение поврежденного оборудования и подсистем	21-1 Разрушение корпуса	Возгорание, взрыв. Нет гашения дуги. Короткое замыкание. Открыты токоведущие части	Стандарты оборудования должны также учитывать правила функциональной безопасности
	21-2 Блокировка техники	Устройство не функционирует. Перегрузка => дальнейшие повреждения	
	21-3 Разрушение разъема или кабеля, находящегося под напряжением => дуга		
	21-4 Повреждение электронных схем	Устройство не функционирует. Выход из строя. Короткое замыкание => перегрев	
22a Дистанционное управление внутри одного помещения			Нет дополнительных опасностей

Продолжение таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
22b Дистанционное управление внутри здания	22b-1 Машина начинает вращаться	Движение не контролирует оператор	Прекратить функционирование. Стандарты на приборы. Внешние меры, например аварийная кнопка. Автономные средства
	22b-2 Нагрев изделия возрастает из-за огнеопасного окружения нагревателя		Внешнее средство, например биметалл. Дистанционный контроль включен, если авторизация была проведена заблаговременно или любым другим способом. Удостоверение подлинности личности. Автономные средства/меры
	22b-3 Функционирование оборудования прекращено	Выполняемый процесс становится неконтролируемым	Отключить дистанционную остановку оборудования во время выполнения процесса или принять внешние меры
	22b-4 Дистанционный контроль сетевых розеток	Например, индикатора	Сетевые розетки с дистанционным управлением должны быть маркированы
	22b-5 Дистанционная переконфигурация		Возможно только внутри зданий
Дистанционное управление вне здания	22c-1 Машина начинает вращаться	Движение не контролирует оператор	Внешние средства, например, аварийная кнопка. Автономные средства. Удостоверение подлинности личности
	22c-2 Нагрев изделия возрастает из-за огнеопасного окружения нагревателя		Внешнее средство, например биметалл. Дистанционный контроль включен, если авторизация была проведена заблаговременно или любым другим способом. Удостоверение подлинности личности
	22c-3 Функционирование оборудования прекращено	Выполняемый процесс становится неконтролируемым	Отключить дистанционную остановку оборудования во время выполнения процесса или принять внешние меры. Удостоверение подлинности личности
	22c-4 Дистанционный контроль сетевых розеток	Индикатор	Сетевые розетки с дистанционным управлением должны быть маркированы. Авторизованные лица
	22c-5 Дистанционная переконфигурация		Удостоверение подлинности личности

Окончание таблицы В.1

Опасное событие (п. 4.2.4)	Элементы события	Детали	Требования/меры по снижению риска
23 Из двух источников поступает команда одному изделию (привод)	23-1 Несанкционированный доступ из разных источников		Конфигурационные решения, например: - доступ открыт только для источников с иерархией, проверяется адрес источника; - правило живой очереди
	23-2 Команда встает в очередь	Непредсказуемые результаты	Защитите изделия. Изделие / блокировка функционирования / отключение / приоритет. Разделяемые переменные. «Герметизация» процесса
24 Ошибки системы	24-1 Нет ответа системы	Устройство не функционирует	Выполните сброс системы и переведите ее в заданное состояние
	24-2 Поврежденное сообщение	Электромагнитная совместимость	См. 12
	24-3 Ложное сообщение	Изредка может привести к неправильной работе	См. 12
	24-4 Непреднамеренное изменение изделий шины	Неверная конфигурация или параметры. Самоконфигурирование	См. 15-4. Авторизация доступа по идентификационному номеру производителя или удостоверение подлинности для конфигурирования программного обеспечения
	24.5 Система занята	Устройство не функционирует	См. 17
Примечание – Настоящий стандарт не содержит связанные с рисками требования для опасных событий 4, 5, 8, 10, 13, 18, 19, 20, 21, которые должны быть рассмотрены в других стандартах.			

Приложение С
(справочное)

Примеры применения ЭСДЗ/СУАЗ, не связанных с обеспечением безопасности

С.1 Общие положения

Ниже приведены примеры из различных сфер деятельности, а также возможные проблемы и способы их решения. Эти примеры могут послужить источником вдохновения для разработчиков различных изделий. Примеры не были проверены или одобрены каким-либо комитетом по разработке изделий, у которого могут быть другие рекомендации относительно их конкретных изделий.

В настоящем приложении применены следующие сокращения:

В. – Вопрос;

О. – Ответ.

С.2 Пример 1. Печь

В. Можно ли с помощью ЭСДЗ/СУАЗ 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? Что если я управляю печью с помощью телефона? Это не запрещено?

О. На протяжении многих лет многие печи оборудованы таймерами – между ними и дистанционным управлением нет никакой разницы.

В. Но когда мы устанавливаем таймер, мы делаем это вручную, стоя напротив печи и отдаем себе отчет в своих действиях.

О. Печь оборудована кнопкой включения дистанционного управления Ее следует нажать прежде чем печь можно будет включить на расстоянии. Не нужно снова нажимать эту кнопку, если вы хотите выключить устройство на расстоянии. Печь должна соответствовать стандартам всех обычных печей.

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 применение или измерить потребление энергии).

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

Некоторые устройства, отмечены их производителями, как обладающие высоким риском возникновения опасности. Работа с такими устройствами предполагает присутствие локального оператора.

В. Такие устройства могут быть запущены, только если точка запуска непосредственно видна из устройства?

О. Да, если таково требование производителей.

В. Значит ли это, что использование доступа ЭСДЗ/СУАЗ к таким изделиям невозможно?

В. Необязательно. Инфракрасное излучение, осуществляющее доступ ЭСДЗ/СУАЗ требует, чтобы устройство находилось в пределах видимости оператора.

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

О. Команды, которые передают через шлюз от другой информационной среды к инфракрасному датчику, должны быть распознаны, как исходящие извне либо вообще не должны быть переданы. Так можно избежать определенных проблем.

С.4 Пример 3. Сетевые розетки, выходные гнезда и цепи

Сетевые розетки, выходные гнезда и магистральные цепи, управляемые с помощью ЭСДЗ/СУАЗ на распределительном щите являются:

- полезными, поскольку благодаря им можно подключить классические устройства к сетевые розеткам, выходным гнездам и магистральным цепям, управляемым с помощью ЭСДЗ/СУАЗ, а ни один из производителей крупных бытовых приборов и электротехники не может предложить полный ряд продуктов ЭСДЗ/СУАЗ на первой фазе,

- потенциально опасными, поскольку с их помощью можно подключить устройства любого типа, которые могут выполнять действия, ранее непредусмотренные производителем или установщиком розетки (гнезда или магистральной цепи).

Обычно, правилами установки разрешено, чтобы дистанционные устройства контролировали штепсельные розетки, расположенные внутри того же помещения. «Дополнительные устройства» для выходных гнезд, а именно таймерные выключатели или пульты дистанционного управления (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/СУАЗ.

За все несут ответственность установщик и пользователь. Можно использовать инструмент настройки и запуска, четко разграничивающий разные магистральные

цепи (освещения, обогрева и т. п.). Также можно создать стандарт для новых розеток и гнезд, используемых в приборах с дистанционным управлением. Гнездо такого типа не будет подходить для обычных розеток, а новая розетка будет подходить как для старых, так и новых разъемов. Новую розетку можно использовать только для приборов, которые можно безопасно использовать на расстоянии и которые могут быть подсоединены к старым или новым гнездам, в зависимости от того, будет ли пользователь пользоваться прибором напрямую или дистанционно.

С.5 Пример 4. Регулировка температуры воды

В. Какие механизмы следует задействовать, чтобы установщик мог настроить верхний предел установки и при этом сделать так, чтобы пользователь не мог изменить этот предел? 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 официально не установлено?

О. Обычно максимальная температура домашнего резервуара для воды не должна превышать определенный предел (около 60 °С), чтобы не допустить получение ожогов. Конечно, возможно пользователь захочет понизить этот предел и он сможет сделать это. В обогреватель может быть встроено программное обеспечение или специальный регулятор, не позволяющий пользователю установить предел температуры выше 60 °С. Однако, такие меры могут быть недопустимыми в некоторых случаях, например на производстве, где нужен более высокий предел, либо в частных случаях, когда в устройстве есть механизмы защиты от ожогов – например, терморегулирующие смесители в кранах или насадках душа.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ЕН 50491-2	–	*
ЕН 50491-3	–	*
ЕН 50491-5 (все части)	–	*
ЕН 61508 (все части)	–	*
ЕН 61709:1998	–	*
ИСО 9000	IDT	ГОСТ Р ИСО 9000–2008 «Системы менеджмента качества. Основные положения и словарь»

* 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] EN 41003 Particular safety requirements for equipment to be connected to telecommunication networks and/or a cable distribution system

[2] EN 60664-1:2007 Insulation coordination for equipment within low-voltage systems – Part 1: Principles, requirements and tests (IEC 60664-1:2007)

[3] EN 60950-1 Information technology equipment – Safety – Part 1: General requirements (IEC 60950-1)

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

[5] EN 61000-6-2 Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments (IEC 61000-6-2)

[7] EN 61000-6-3 Electromagnetic compatibility (EMC) – Part 6-3: Generic standards – Emission standard for residential, commercial and light-industrial environments (IEC 61000-6-3)

[8] EN 61000-6-4 Electromagnetic compatibility (EMC) – Part 6-4: Generic standards – Emission standard for industrial environments (IEC 61000-6-4)

[9] EN 61508-1 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements (IEC 61508-1)

[10] EN 61508-2 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2)

[11] EN 61508-3 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements (IEC 61508-3)

[12] HD 384 series Electrical installations of building (IEC 60364 series, modified)

[13] CEN/CLC Guide 9 Guidelines for the inclusion of safety aspects in standards (ISO/IEC Guide 51)

[14] IEC/TS 61000-1-2 Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena

[15] IEC/TR 61000-2-1 Electromagnetic compatibility (EMC) – Part 2: Environment – Section 1: Description of the environment – Electromagnetic environment

for low-frequency conducted disturbances and signalling in public power supply systems

[16] IEC Guide 104 The preparation of safety publications and the use of basic safety publications and group safety publications

[17] IEC Guide 110 Home control systems–guidelines relating to safety

УДК 62-783:614.8:331.454:006.354 ОКС 13.110, 13.120, 35.240.99 Группа Т51

Ключевые слова: безопасность функциональная; электронные системы; жилые дома и общественные здания; системы управления и автоматизации; общие требования к функциональной безопасности

Руководитель организации-разработчика

Общество с ограниченной ответственностью «Корпоративные электронные системы»

Генеральный директор С.В. Сумароков

Руководитель разработки,

Заместитель генерального директора А.Ф. Колчин