ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62061— 2015

Безопасность оборудования

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ И ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

IEC 62061:2005+A1:2012
Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems
(IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы» и Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации — «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык 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 от 18 мая 2015 г. № 364-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62061:2005+ A1:2012 «Безопасность оборудования. Функциональная безопасность систем управления электрических, электронных и программируемых электронных, связанных с безопасностью» (IEC 62061:2005+A1:2012 «Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems).

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

5 ВЗАМЕН ГОСТ Р МЭК 62061—2013

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 Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

В результате автоматизации, а также ввиду необходимости роста производства и сокращения физического труда связанные с безопасностью электрические системы управления (СБЭСУ) машин играют все большую роль в достижении безопасности всего оборудования. Кроме того, СБЭСУ в большой степени используют сложную электронную технологию.

Ранее, в отсутствие стандартов СБЭСУ не применялись для выполнения связанных с безопасностью функций, направленных на снижение рисков, вызванных работой машины, из-за отсутствия данных об эффективности такой технологии.

Настоящий стандарт предназначен для использования разработчиками оборудования машин, производителями и интеграторами систем управления и другими специалистами, выполняющими спецификацию, проектирование и подтверждение соответствия СБЭСУ. Стандарт устанавливает подход и требования для достижения необходимой эффективности используемой технологии.

Настоящий стандарт соответствует требованиям МЭК 61508 для области оборудования (машин). Он предназначен для того, чтобы способствовать спецификации характеристик СБЭСУ для основных опасностей (см. 3.8 ИСО 12100-1), вызванных работой машин.

В области оборудования (машин) настоящий стандарт реализует конкретный подход, связанный с обеспечением функциональной безопасности СБЭСУ машин. Стандарт охватывает только те аспекты жизненного цикла системы безопасности, которые связаны с распределением к ней требований, необходимых для подтверждения ее соответствия. Эти требования обеспечивают получение информации о безопасном использовании СБЭСУ машин, которая также может применяться на более поздних стадиях жизненного цикла СБЭСУ.

СБЭСУ часто используют в оборудовании (машинах) в качестве одной из мер по обеспечению безопасности для снижения риска выполнения опасного события. Типичный случай — блокирование доступа, которое предоставляет доступ к опасной зоне и сигнализирует электрической системе управления о необходимости остановить работу машины. Также при автоматизации электрическая система управления, используемая для обеспечения корректного выполнения процессов машины, часто способствует безопасности, смягчая риски, связанные с опасностями, возникающими непосредственно из-за отказов системы управления. В настоящем стандарте представлены методология и требования:

- к определению требуемого уровня полноты безопасности для каждой связанной с безопасностью функции управления, реализуемой СБЭСУ;
- выполнению проекта СБЭСУ для соответствующей(их) определенной(ых) связанной(ых) с безопасностью функции(й) управления;
- интеграции связанных с безопасностью подсистем, разработанных в соответствии с ИСО 13849;
- подтверждению соответствия СБЭСУ.

Настоящий стандарт должны использовать в рамках подхода к систематическому снижению риска, описанного в ИСО 12100-1, и в сочетании с оценкой степени риска согласно принципам, описанным в ИСО 14121 (ЕН 1050). Предлагаемая методология для определения уровня полноты безопасности (УПБ) дана в приложении А.

Представлены меры, координирующие реализацию СБЭСУ с целевым снижением риска, учитывающие вероятности и последствия случайных или систематических ошибок в электрической системе управления.

На рисунке 1 показана связь настоящего стандарта с другими соответствующими стандартами.

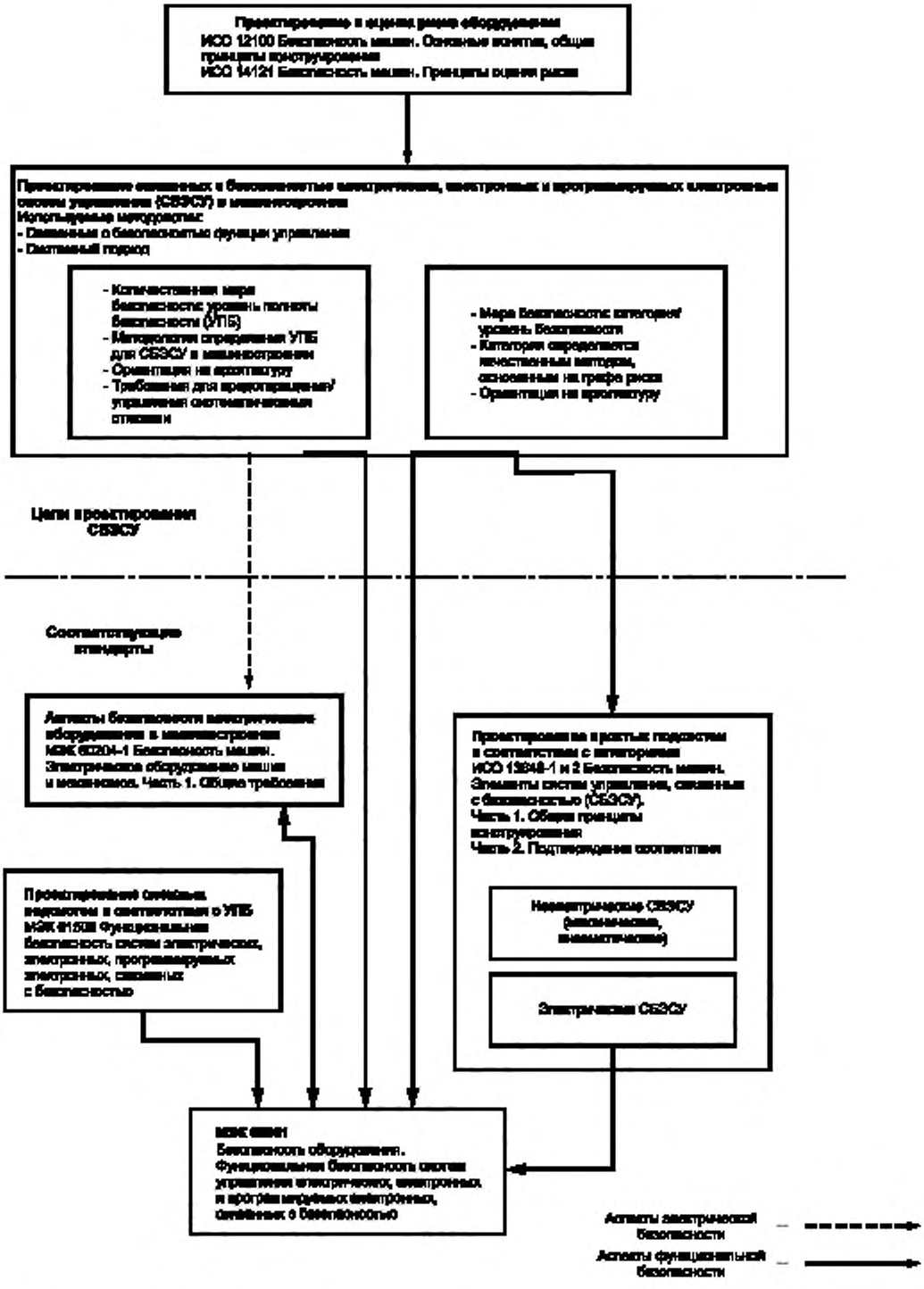


Рисунок 1 — Связь настоящего стандарта с другими соответствующими стандартами

Настоящий стандарт и ИСО 13849-1 определяют требования к проектированию и реализации связанных с безопасностью систем управления оборудованием машин. Использование любого из этих стандартов в соответствии с их областями применения предполагает выполнение соответствующих важных требований к обеспечению безопасности. В МЭК/ТО 62061-1 представлено руководство по применению настоящего стандарта и ИСО 13849-1 при проектировании связанных с безопасностью систем управления в области оборудования (машин).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность оборудования

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ ЭЛЕКТРИЧЕСКИХ, ЭЛЕКТРОННЫХ И ПРОГРАММИРУЕМЫХ ЭЛЕКТРОННЫХ, СВЯЗАННЫХ С БЕЗОПАСНОСТЬЮ

Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems

Дата введения — 2016—05—01

1 Область применения

Настоящий стандарт определяет требования и рекомендации для проектирования, интеграции и подтверждения соответствия связанных с безопасностью электрических, электронных и программируемых электронных систем управления (СБЭСУ) для оборудования (машин) (см. примечания 1 и 2). Настоящий стандарт распространяется на системы управления отдельно или в комбинации, выполняющие связанные с безопасностью функции управления, используемые в стационарно установленных промышленных машинах и механизмах, включая группу машин, работающих вместе в согласованном режиме.

Примечания

1 В настоящем стандарте термин «электрические системы управления» используется вместо «электрические, электронные и программируемые электронные (Э/Э/ПЭ) системы управления», а СБЭСУ — вместо «связанные с безопасностью электрические, электронные и программируемые электронные системы управления».

2 В настоящем стандарте предполагается, что проектирование сложных программируемых электронных подсистем или их элементов удовлетворяет соответствующим требованиям МЭК 61508 и используется способ 1_H (см. 7.4.4.2 МЭК 61508-2). Считается, что способ 2_H (см. 7.4.4.3 МЭК 61508-2) не подходит в общем случае для машинного оборудования, поэтому настоящий стандарт не рассматривает способ 2_H. В настоящем стандарте представлена методология для применения, а не разработки подсистем и их элементов, являющихся частью СБЭСУ.

Настоящий стандарт не предназначен ограничивать или запрещать совершенствование технологии. Он не охватывает все требования (например, защиту, неэлектрическую взаимную блокировку или неэлектрическое управление), которые необходимы и установлены другими стандартами или регламентирующими документами, обеспечивающими безопасность людей. Для того чтобы обеспечить соответствующую безопасность, для каждого типа машины существуют уникальные требования, которые должны быть выполнены.

Настоящий стандарт:

- устанавливает требования только к функциональной безопасности, предназначенные для уменьшения риска травмирования или причинения вреда здоровью людей, находящихся в непосредственной близости от машины и использующих ее;
- рассматривает только риски, возникающие непосредственно из опасностей, связанных с самой машиной или с группой машин, работающих вместе в согласованном режиме.

Примечание — Требования, обеспечивающие смягчение рисков, возникающих в результате других опасностей, приведены в стандартах соответствующих областей. Например, если машина(ы) реализует(ют) промышленный процесс, то кроме требований к функциональной безопасности электрическая система управления машины должна удовлетворять и другим требованиям (например, представленным в МЭК 61511), поскольку связана с безопасностью процесса;

Издание официальное

- не определяет требования к характеристикам неэлектрических (например, гидравлических, пневматических) элементов системы управления машин.

Примечание — Несмотря на то что требования настоящего стандарта определены для электрических систем управления, данный подход и методология могут быть применимы к связанным с безопасностью частям систем управления, использующих другие технологии;

- не охватывает угрозы, связанные с электричеством, возникающие в самом электрическом оборудовании управления (например, поражение электрическим током — см. МЭК 60204-1).

Цели разделов настоящего стандарта представлены в таблице 1.

Таблица 1 — Цели разделов настоящего стандарта

Раздел	Цель
4 Управление функциональной безопасностью	Определить управляющие и технические действия, которые необходимы для достижения требуемой функциональной безопасности СБЭСУ
5 Требования к спецификации связанных с безопасностью функций управления	Установить процедуры для определения требований к связанным с безопасностью функциям управления. Эти требования задаются в виде спецификации функциональных требований и спецификации требований к полноте безопасности
6 Проектирование и интеграция СБЭСУ	Определить критерии выбора и/или методы разработки и реализации СБЭСУ, чтобы выполнить следующие требования функциональной безопасности: к выбору архитектуры системы; выбору связанных с безопасностью аппаратных средств и программного обеспечения; методам проектирования аппаратных средств и программного обеспечения; методам проверки, подтверждающим, что разработанные аппаратные средства и программное обеспечение удовлетворяют требования функциональной безопасности
7 Информация для использования машины	Определить требования к информации по использованию СБЭСУ, которая должна быть поставлена с машиной. Она включает в себя: руководство и описание процедур пользователя; руководство и описание процедур технического обслуживания
8 Подтверждение соответствия СБЭСУ	Определить требования к процессу подтверждения соответствия СБЭСУ. Этот процесс включает контроль и тестирование СБЭСУ, гарантирующие, что СБЭСУ удовлетворяет требования, установленные в спецификации требований к безопасности системы
9 Модификация СБЭСУ	Определить требования для процедуры модификации, которая должна применяться при модификации СБЭСУ. Согласно этим требованиям: модификации к любому СБЭСУ должны быть должным образом запланированы и проверены до внесения изменения; после любой выполненной модификации СБЭСУ должна удовлетворять спецификации требований к безопасности системы

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

МЭК 60204-1 Безопасность машин. Электрооборудование машин и механизмов. Часть 1. Общие требования (IEC 60204-1, Safety of machinery — Electrical equipment of machines — Part 1: General requirements)

МЭК 61000-6-1 Электромагнитная совместимость (ЭМС). Часть 6-1. Общие стандарты. Устойчивость к электромагнитным помехам технических средств, применяемых в жилых, коммерческих зонах и производственных зонах с малым энергопотреблением (IEC 61000-6-1, Electromagnetic compatibility (EMC) — Part 6-1: Generic standards — Immunity for residential, commercial and light-industrial environments)

МЭК 61000-6-2 Электромагнитная совместимость (ЭМС). Часть 6-2. Общие стандарты. Устойчивость в промышленных условиях (IEC 61000-6-2, Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments)

МЭК 61000-4 Электромагнитная совместимость (ЭМС). Части 4. Методы испытаний и измерений (IEC 61000-4, Electromagnetic compatibility (EMC) — Parts 4: Testing and measurement techniques)

ИСО/МЭК Руководство 51:1990 Аспекты безопасности. Руководящие указания по включению в стандарты (ISO/IEC Guide 51:1999 Safety aspects — Guidelines for their inclusion in standards)

МЭК 61131-3:2003 Контроллеры программируемые. Часть 3. Языки программирования. (IEC 61131-3:2003, Programmable controllers — Part 3: Programming languages)

МЭК 61310 (все части) Безопасность машин. Индикация, маркирование и запуск (IEC 61310 (all parts), Safety of machinery — Indication, marking and actuation)

МЭК 61326-1:2005 Совместимость технических средств электромагнитная. Электрическое оборудование для измерения, управления и лабораторного применения. Часть 1. Общие требования и методы испытаний (IEC 61326-1:2005, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 1: General requirements) (MOD)

МЭК 61508-1:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования (IEC 61508-1:2010, Functional safety of electrical/electronic /programmable electronic safety-related systems — Part 1: General requirements)

МЭК 61508-2:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам электрическим/электронным/программируемым электронным, связанным с безопасностью (IEC 61508-4:2010, Functional safety of electrical/electronic/ programmable electronic safety-related systems — Part 2. Requirements for electrical / electronic / programmable electronic safety-related systems)

МЭК 61508-3:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению (IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements)

МЭК 61508-4:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения (ISO/IEC 61508-4:2010, Functional safety of electrical/electronic /programmable electronic safety-related systems — Part 4. Definitions and abbreviations)

МЭК 61508-5:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности (IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels)

МЭК 61508-7:2010 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Анализ методов и средств (IEC 61508-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures)

МЭК 61511-1:2003 Безопасность функциональная. Приборные системы безопасности, для технологических процессов в промышленности. Часть 1. Термины, определения и технические требования (IEC 61511-1:2003, Functional safety — Safety instrumented systems for process industry sector — Part 1: Framework, definitions, system, hardware and software requirements)

МЭК 61784-3-3:2007 Промышленные сети связи. Профили. Часть 3-3. Функциональная безопасность полевых (магистральных) шин. Дополнительные спецификации для CPF 3 (IEC 61784-3-3:2007, Industrial communication networks — Profiles — Part 3-3: Functional safety fieldbuses — Additional specifications for CPF 3)

ИСО 12100:2010 Безопасность машин и оборудования. Принципы обеспечения безопасности при проектировании (ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction)

ИСО 13849-1:2006 Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования (ISO 13849-1:1999, Safety of machinery — Safety related parts of control systems — Part 1: General principles for design)

ИСО 13849-2:2003[1)] Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 2. Подтверждение соответствия (ISO 13849-2:2003, Safety of machinery — Safety-related parts of control systems — Part 2: Validation)

ИСО 14121 Безопасность оборудования. Принципы оценки риска (ISO 14121, Safety of machinery — Principles of risk assessment)

[1)] Отменен. Действует ИСО 13849-2:2012 Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 2. Подтверждение соответствия.

3 Термины и определения

3.1 Алфавитный список определений

Таблица

Термин	Пункт раздела 3
архитектура	3.2.35
архитектурное ограничение	3.2.36
безопасный отказ	3.2.41
верификация	3.2.51
вероятность опасного отказа в час; PFH_D	3.2.28
встроенное программное обеспечение	3.2.47
доля безопасных отказов; ДБО	3.2.42
запрос	3.2.25
компонент низкой сложности	3.2.7
контрольная проверка	3.2.37
мера защиты	3.2.12
механизмы	3.2.1
опасность	3.2.10
опасная ситуация	3.2.11
опасный отказ	3.2.40
отказ	3.2.39
отказ по общей причине	3.2.43
охват диагностикой	3.2.38
подсистема	3.2.5
подтверждение соответствия	3.2.52
полнота безопасности	3.2.19
полнота безопасности аппаратных средств	3.2.20
полнота безопасности, касающаяся систематических отказов	3.2.22
полнота безопасности программного обеспечения	3.2.21
предельное требование к УПБ (для подсистемы); ПТУПБ	3.2.24
прикладное программное обеспечение	3.2.46
программное обеспечение, связанное с безопасностью	3.2.50
режим с высокой частотой запросов или непрерывный режим	3.2.27
режим с низкой частотой запросов	3.2.26
риск	3.2.13
сбой	3.2.30
связанная с безопасностью функция управления; СБФУ	3.2.16

Окончание таблицы

Термин	Пункт раздела 3
связанные с безопасностью электрические системы управления; СБЭСУ	3.2.4
система управления машиной	3.2.2
систематический отказ	3.2.45
сложный компонент	3.2.8
случайный отказ аппаратных средств	3.2.44
среднее время до отказа; *MTTF*	3.2.34
уровень полноты безопасности; УПБ	3.2.23
устойчивость к отказам	3.2.31
функциональная безопасность	3.2.9
функциональный блок	3.2.32
функция безопасности	3.2.15
функция диагностики	3.2.17
функция реакции на отказ СБЭСУ	3.2.18
функция управления	3.2.14
целевая величина отказов	3.2.29
электрическая система управления	3.2.3
элемент подсистемы	3.2.6
элемент функционального блока	3.2.33
язык программирования с ограниченной изменчивостью; ЯОИ	3.2.49
язык программирования с полной изменчивостью; ЯПИ	3.2.48

3.2 Термины и определения

В настоящем стандарте применены следующие термины и определения:

3.2.1 **механизмы** (machinery): Совокупность связанных между собой деталей и устройств, как минимум одно из которых движется, имеет соответствующий привод, органы управления и сети электропитания, соединенные вместе для конкретного применения, например для обработки, переработки, производства, транспортирования или упаковки материалов.

Термины «машина» и «механизм» также распространяются на совокупность машин, которые размещаются и управляются таким образом, чтобы функционировать как единое целое.

[ИСО 12100, п. 3.1]

3.2.2 **система управления машиной** (machine control system): Система, которая реагирует на входной сигнал, например от процесса, других элементов машины, оператора, внешнего управляемого оборудования, и генерирует выходной(ые) сигнал(ы), заставляющий(ие) машину вести себя предназначенным способом.

3.2.3 **электрическая система управления** (electrical control system): Система управления машины, выполняющая, например, операционное управление, контроль, взаимную блокировку, связь, защиту и связанные с безопасностью функции управления и использующая только электрические, электронные и программируемые электронные компоненты.

Примечание — Связанные с безопасностью функции управления могут быть реализованы с помощью электрической системы управления, которая является либо неотъемлемой составной частью, либо независимой от тех частей системы управления машины, которые выполняют функции, не связанные с безопасностью.

3.2.4 **связанные с безопасностью электрические системы управления**; СБЭСУ (Safety-Related Electrical Control System, SRECS): Электрическая система управления, отказ которой может непосредственно привести к увеличению риска(ов).

Примечание — СБЭСУ включает в себя все элементы электрической системы управления, отказ которых может привести к снижению или потере функциональной безопасности, а также может включать в себя цепи электропитания и управления.

3.2.5 **подсистема** (subsystem): Объект проекта архитектуры верхнего уровня СБЭСУ, в которой опасный отказ любой подсистемы приведет к опасному отказу связанной с безопасностью функции управления.

[МЭК 61508-4, п. 3.4.4 модифицирован]

Примечания

1 Полная подсистема может быть составлена из большого количества идентифицируемых и отдельных элементов, которые, когда соединяются вместе, реализуют функциональные блоки, выделенные в подсистеме.

2 Данное определение отличается от обычно используемого, где «подсистема» может означать любую подразделяемую часть объекта, в настоящем стандарте термин «подсистема» использован в строго определенной терминологической иерархии: «подсистема» — первый уровень декомпозиции системы. Компоненты последующей декомпозиции называют «элементы подсистемы».

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

3.2.7 **компонент низкой сложности** (low complexity component): Компонент, для которого:

- строго определены режимы отказов;
- может быть полностью определено поведение в условиях отказа.

[МЭК 61508-4, п. 3.4.3 модифицирован]

Примечания

1 Поведение компонента низкой сложности в условиях отказа может быть определено либо аналитическими методами, либо методами испытаний.

2 Подсистема или элемент, включающие один или более концевых выключателей, работающих, возможно, через промежуточные электромеханические реле, один или более контакторов, используемых для отключения питания электродвигателя, является примером компонента низкой сложности.

3.2.8 **сложный компонент** (complex component): Компонент, для которого:

- плохо определены режимы отказов;
- не может быть полностью определено поведение в условиях отказа.

3.2.9 **функциональная безопасность** (functional safety): Часть безопасности машины и системы управления машины, которая зависит от корректного функционирования СБЭСУ, систем, связанных с безопасностью, основанных на других технологиях и внешних средствах снижения риска.

[МЭК 61508-4, п. 3.1.12 модифицирован]

Примечания

1 Настоящий стандарт рассматривает только функциональную безопасность, которая зависит от корректного функционирования СБЭСУ в применениях для оборудования машин.

2 В ИСО/МЭК Руководство 51 безопасность определена как отсутствие неприемлемого риска.

3.2.10 **опасность** (hazard): Потенциальный источник телесного повреждения или причинения вреда здоровью.

[ИСО 12100, п. 3.6 модифицирован]

Примечание — Термин «опасность» может быть квалифицирован, чтобы определить ее источник или природу ожидаемого вреда (например, опасность удара током, опасность разрушения, опасность резки, токсичная опасность, пожароопасность).

3.2.11 **опасная ситуация** (hazardous situation): Обстоятельства, при которых человек подвергается одной или нескольким опасностям.

[ИСО 12100, п. 3.10 модифицирован]

3.2.12 **мера защиты** (protective measure): Мера, направленная на достижение снижения риска.

[ИСО 12100, п. 3.19 модифицирован]

3.2.13 **риск** (risk): Сочетание вероятности причинения вреда и его тяжести.

[ИСО 12100, п. 3.12]

3.2.14 **функция управления** (control function): Функция, которая оценивает входную информацию или сигналы и формирует выходную информацию или действия.

3.2.15 **функция безопасности** (safety function): Функция машины, отказ которой может привести к непосредственному увеличению риска(ов).

[ISO 12100, п. 3.30]

Примечание — Данное определение отличается от определений в МЭК 61508-4 и ИСО 13849-1.

3.2.16 **связанная с безопасностью функция управления**, СБФУ (Safety-Related Control Function, SRCF): Функция управления, реализованная СБЭСУ с заданным уровнем полноты и предназначенная для поддержки безопасных условий работы машины или предотвращения увеличения риска(ов).

3.2.17 **функция диагностики СБЭСУ** (SRECS diagnostic function): Функция, предназначенная для обнаружения отказов в СБЭСУ и формирования заданной выходной информации или действия при обнаружении отказа.

Примечание — Данная функция предназначена для обнаружения отказов, которые могут привести к опасному отказу СБФУ, и запуска заданной функции реакции на отказ.

3.2.18 **функция реакции на отказ СБЭСУ** (SRECS fault reaction function): Функция, которая запускается, когда в СБЭСУ обнаружен отказ с помощью функции диагностики СБЭСУ.

3.2.19 **полнота безопасности** (safety integrity): Вероятность того, что СБЭСУ или ее подсистема будет удовлетворительно выполнять требуемые, связанные с безопасностью функции управления при всех указанных условиях.

[МЭК 61508-4, п. 3.5.4 модифицирован]

Примечания

1 Чем выше уровень полноты безопасности элемента, тем ниже вероятность, что элемент не выполнит требуемую, связанную с безопасностью функцию управления.

2 Полнота безопасности включает полноту безопасности аппаратных средств (см. 3.2.20) и систематическую полноту безопасности (см. 3.2.22).

3.2.20 **полнота безопасности аппаратных средств** (hardware safety integrity): Составляющая полноты безопасности СБЭСУ или ее подсистем, включающая требования к вероятности опасных случайных отказов технических средств и к архитектурным ограничениям.

[МЭК 61508-4, п. 3.5.7 модифицирован]

3.2.21 **полнота безопасности программного обеспечения** (software safety integrity): Составляющая систематической полноты безопасности СБЭСУ или ее подсистем, связанная с возможностью программного обеспечения в программируемой электронной системе выполнять в ней связанные с безопасностью функции управления при всех заданных условиях в течение установленного промежутка времени.

[МЭК 61508-4, п. 3.5.5 модифицирован]

Примечание — Обычно полнота безопасности программного обеспечения не может быть охарактеризована количественно.

3.2.22 **систематическая полнота безопасности** (systematic safety integrity): Составляющая полноты безопасности СБЭСУ или ее подсистем, касающаяся ее противодействия систематическим отказам (см. 3.2.45), проявляющимся в опасном режиме.

[МЭК 61508-4, п. 3.5.6 модифицирован]

Примечания

1 Обычно полнота безопасности, касающаяся систематических отказов, не может быть охарактеризована количественно.

2 Требования к полноте безопасности, касающейся систематических отказов, применяются как к аппаратным средствам, так и к аспектам программного обеспечения СБЭСУ или ее подсистем.

3.2.23 **уровень полноты безопасности**; УПБ (safety integrity level (SIL)): Дискретный уровень (принимающий одно из трех возможных значений), устанавливающий требования к полноте безопасности связанных с ней функций управления, которые были определены для СБЭСУ, при этом уровень 3 является высшим уровнем полноты безопасности, а уровень 1 — самым низшим.

[МЭК 61508-4, п. 3.5.8 модифицирован]

Примечание — УПБ 4 в настоящем стандарте не рассматривается, поскольку такие требования к снижению риска обычно не используют для машинного оборудования. О требованиях при применении УПБ 4 см. МЭК 61508-1 и МЭК 61508-2.

3.2.24 **предельное требование к УПБ (для подсистемы); ПТУПБ** (SIL Claim Limit (for a subsystem), SILCL): Максимальное значение УПБ, которое может быть заявлено для подсистемы СБЭСУ относительно архитектурных ограничений и систематической полноты безопасности.

3.2.25 **запрос** (demand): Событие, которое инициирует СБЭСУ выполнять свою СБФУ.

3.2.26 **режим с низкой частотой запросов** (low demand mode): Режим работы, в котором частота запросов к СБЭСУ не больше чем один раз в год.

Примечание — Оборудование, которое в соответствии с требованиями спроектировано для работы только в режиме с низкой частотой запросов, описанном в МЭК 61508-1 и МЭК 61508-2, может быть непригодно для применения в качестве элемента СБЭСУ, соответствующей настоящему стандарту. Режим работы с низкой частотой запросов не используют для применения СБЭСУ в оборудовании машин.

3.2.27 **режим с высокой частотой запросов или непрерывный режим** (high demand or continuous mode): Режим работы, в котором частота запросов к СБЭСУ больше, чем один раз в год, либо СБФУ поддерживает машину в безопасном состоянии, являющемся одним из режимов нормального функционирования.

[МЭК 61508-4, п. 3.5.16 модифицирован]

Примечания

1 Режим работы с низкой частотой запросов, как полагают, неважен для применений СБЭСУ в машинном оборудовании. Поэтому в настоящем стандарте предполагается, что СБЭСУ работают только в режиме с высокой частотой запросов или в непрерывном режиме.

2 Режим запроса означает, что связанная с безопасностью функция управления выполняется только по запросу (требованию), чтобы перевести машину в указанное состояние. СБЭСУ не влияет на машину, пока нет требований к связанной с безопасностью функции управления.

3 Непрерывный режим подразумевает стабильное выполнение связанной с безопасностью функции управления, т.е. СБЭСУ постоянно управляет машиной и (опасный) отказ ее функции может привести к опасному событию.

3.2.28 **вероятность опасного отказа в час**; PFH_D (probability of a dangerous failure per hour, *PFH*): Средняя вероятность опасного отказа в час связанной с безопасностью системы или подсистемы, выполняющей конкретную функцию безопасности в течение установленного периода времени.

Примечание — PFH_D не надо путать с вероятностью опасного отказа по запросу (*PFD*).

3.2.29 **целевая величина отказов** (target failure value): Заданное значение PFH_D, которое должно быть достигнуто, чтобы удовлетворить конкретное требование полноты безопасности.

Примечание — Целевая величина отказов задается в терминах вероятности опасного отказа в час.

[МЭК 61508-4, п. 3.5.17 модифицирован]

3.2.30 **сбой** (fault): Ненормальный режим, способный вызвать снижение или потерю способности СБЭСУ, подсистемы или элемента подсистемы выполнять требуемую функцию.

[МЭК 61508-4, п. 3.6.1 модифицирован]

3.2.31 **устойчивость к сбоям** (fault tolerance): Способность СБЭСУ, подсистемы или элемента подсистемы продолжать выполнять необходимую функцию при наличии сбоев или ошибок.

[МЭК 61508-4, п. 3.6.3 модифицирован]

3.2.32 **функциональный блок** (functional block): Наименьший элемент СБФУ, отказ которого может привести к отказу СБФУ.

Примечания

1 В настоящем стандарте СБФУ можно рассматривать как логическую функцию Ф из функциональных блоков (ФБ), то есть $Ф = ФБ_1 \,\&\, ФБ_2 \,\&\, ФБ_n$.

2 Это определение функционального блока отличается от используемого в МЭК 61131-3 и других стандартах.

3.2.33 **элемент функционального блока** (function block element): Часть функционального блока.

3.2.34 **среднее время до отказа** (Mean Time To Failure, MTTF): Ожидание среднего времени наработки на отказ.

[МЭС 191-12-07 модифицирован]

Примечание — MTTF обычно выражается как среднее значение ожидания времени безотказной работы.

3.2.35 **архитектура** (architecture): Конкретная конфигурация элементов аппаратных средств и программного обеспечения СБЭСУ.

[МЭК 61508-4, п. 3.3.4 модифицирован]

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

Примечание — Требования к архитектурным ограничениям представлены в 6.7.6.

3.2.37 **контрольная проверка** (proof test): Периодическая проверка, выполняемая для того, чтобы обнаружить опасные скрытые отказы и ухудшение функционирования СБЭСУ и ее подсистем с тем, чтобы при необходимости СБЭСУ и ее подсистемы могли быть восстановлены настолько близко к «исходному» состоянию, насколько это возможно в данных условиях.

[МЭК 61508-4, п. 3.8.5 модифицирован]

Примечание — Контрольная проверка предназначена для того, чтобы подтвердить, что СБЭСУ находится в состоянии, которое обеспечивает заданную полноту безопасности.

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

[МЭК 61508-4, п. 3.8.6 модифицирован]

Примечания

1 Охват диагностикой опасных отказов определяют с помощью следующего выражения, где DC — охват диагностикой, λ_{DD} — интенсивности выявленных опасных отказов, λ_{total} — общая интенсивность опасных отказов:

$$DC \quad \frac{\sum \quad DD}{\sum \quad total}$$

2 Доля выявляемых опасных отказов, вычисляемая как отношение интенсивности опасных отказов, выявляемых автоматическими диагностическими проверками в неавтономном режиме, к общей интенсивность опасных отказов.

3.2.39 **отказ** (failure): Прекращение способности СБЭСУ, подсистемы или элемента подсистемы выполнять требуемую функцию.

[МЭК 61508-4, п. 3.6.4 модифицирован и ИСО 12100-1:2003, п. 3.32]

Примечание — Отказы могут быть случайными (в аппаратных средствах) или систематическими (в аппаратных средствах или в программном обеспечении).

3.2.40 **опасный отказ** (dangerous failure): Отказ СБЭСУ, подсистемы или элемента подсистемы, который может привести к опасному состоянию или ошибке при выполнении функции.

Примечания

1 Будут или нет реализованы опасные последствия отказа, зависит от канальной архитектуры системы; например, в многоканальных системах, повышающих уровень безопасности, опасный отказ технического средства с меньшей вероятностью приведет к итоговому опасному состоянию или отказу при выполнении функции.

2 В многоканальной подсистеме вероятность опасного отказа может быть меньше, чем интенсивность опасного отказа канала, который включен в подсистему. Вероятность же опасного отказа СБЭСУ не может быть меньшей, чем вероятность опасного отказа любой из подсистем, составляющей СБЭСУ (это следует из определения «подсистемы», данного в настоящем стандарте).

3 Опасный отказ обычно приводит к отказу или возможному отказу выполнения СБФУ.

3.2.41 **безопасный отказ** (safe failure): Отказ СБЭСУ, подсистемы или ее элемента, не вызывающий опасность.

Примечание — Безопасный отказ не приводит к отказу или возможному отказу выполнения СБФУ.

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

Примечание — Значение ДБО может быть вычислено по следующей формуле:

$$\text{ДБО} = \left(\sum \lambda_S + \sum \lambda_{DD}\right) / \left(\sum \lambda_S + \sum \lambda_D\right),$$

где:

λ_S — интенсивность безопасных отказов;

$\sum \lambda_S + \sum \lambda_D$ — общая интенсивность отказов;

λ_{DD} — интенсивность опасных отказов, выявляемых диагностикой;

λ_D — интенсивность опасных отказов.

Диагностический охват (если таковой имеется) каждой подсистемы в СБЭСУ учитывается при вычислении вероятности случайных отказов аппаратных средств. ДБО — при определении архитектурных ограничений на полноту безопасности аппаратных средств (см. 6.7.7).

3.2.43 **отказ по общей причине** (common cause failure): Отказ, который является результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной подсистеме (с архитектурой с резервированием), ведущий к отказу СБЭСУ.

[МЭК 61508-4, п. 3.6.10 модифицирован]

Примечание — Данное определение отличается от представленного в ИСО 12100-1 и МЭС 191-04-23.

3.2.44 **случайный отказ аппаратных средств** (random hardware failure): Отказ, возникающий в случайный момент времени и являющийся результатом одного или нескольких возможных механизмов ухудшения характеристик аппаратных средств.

[МЭК 61508-4, п. 3.6.5]

3.2.45 **систематический отказ** (systematic failure): Отказ, обусловленный определенной причиной, которая может быть исключена только путем модификации проекта, производственного процесса, операций, документации или других факторов.

[МЭК 61508-4, п. 3.6.6]

Примечания

1 Корректирующее действие без модификации обычно не устраняет причину отказа.

2 Систематический отказ может быть вызван имитацией причины отказа.

3 Примерами причин систематических отказов являются ошибки человека:

- в спецификации требований к безопасности;
- проекте, при изготовлении, вводе в эксплуатацию или работе аппаратных средств;
- при проектировании, реализации и т. п. программного обеспечения.

3.2.46 **прикладное программное обеспечение** (application software): Определенное для применения программное обеспечение, реализованное разработчиком СБЭСУ, обычно содержащее последовательность логических операций, ограничения и выражения и управляющее соответствующей входящей и выходящей информацией, вычислениями и решениями, удовлетворяющими функциональные требования СБЭСУ.

3.2.47 **встроенное программное обеспечение** (embedded software): Программное обеспечение, поставленное производителем, которое является частью СБЭСУ и, как правило, недоступное для модификации.

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

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

[МЭК 61511-1, п. 3.2.81.1.3 модифицирован]

Примечания

1 Типичными примерами систем, применяющих ЯПИ, являются системы, широко используемые компьютерами.

2 Обычно ЯПИ применяют во встроенном программном обеспечении и реже — в прикладном.

3 Примерами ЯПИ являются Ada, C, Pascal, языки ассемблера, C++, Java, SQL.

3.2.49 **язык программирования с ограниченной изменчивостью**; ЯОИ (limited variability language, LVL): Тип языка программирования, который позволяет объединять предварительно определенные, специфические для предметной области библиотечные функции для выполнения спецификаций требований к системе безопасности.

[МЭК 61511-1, п. 3.2.81.1.2 модифицирован]

Примечания

1 ЯОИ обеспечивает близкое соответствие функциям, необходимым для реализации применения.

2 Типичные примеры ЯОИ приведены в МЭК 61131-3 и включают языки многоступенчатых диаграмм, функциональных блок-диаграмм, последовательностных функциональных схем.

3 Типичными примерами систем, использующих ЯОИ, являются программируемые логические контроллеры (ПЛК), сконфигурированные для управления оборудованием машин.

3.2.50 **программное обеспечение, связанное с безопасностью** (safety-related software): Программное обеспечение, которое используется для реализации СБФУ в системах, связанных с безопасностью.

3.2.51 **верификация** (verification): Подтверждение проверкой (например, тестами, анализом), что СБЭСУ, ее подсистемы или элементы подсистемы удовлетворяют требования, установленные соответствующей спецификацией.

[МЭК 61508-4, п. 3.8.1 модифицирован и МЭК 61511-1, п. 3.2.92 модифицирован]

Примечание — Результаты верификации должны быть представлены в виде документально оформленных объективных доказательств.

Пример — Процессы верификации включают:

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

- просмотр проектов;

- тестирование, выполняемое на проектируемых изделиях для того, чтобы убедиться, что они работают в соответствии с их спецификациями;

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

3.2.52 **подтверждение соответствия** (validation): Подтверждение проверкой (например, тестами, анализом), что СБЭСУ соответствует требованиям функциональной безопасности для конкретного применения.

[МЭК 61508-4, п. 3.8.2 модифицирован]

3.3 Сокращения

В настоящем стандарте использованы следующие сокращения.

Сокращение	Полное выражение
ООП	Отказ по общей причине
DC	Охват диагностикой
ЭМС	Электромагнитная совместимость
ФБ	Функциональный блок
ЯПИ	Язык программирования с полной изменчивостью
Вх/Вых	Вход/Выход
ЯОИ	Язык программирования с ограниченной изменчивостью
PFH_D	Вероятность опасного отказа в час
MTTF	Среднее время до отказа
MTTR	Среднее время восстановления
P_{TE}	Вероятность опасности ошибки передачи
ДБО	Доля безопасных отказов
УПБ	Уровень полноты безопасности
ПТУПБ	Предельное требование к УПБ (для подсистем): ПТУПБ
СБ	Связанный с безопасностью
СБЭСУ	Связанная с безопасностью электрическая система управления
СБФУ	Связанная с безопасностью функция управления
СТСБ	Спецификация требований к системе безопасности
СИС	Система

4 Управление функциональной безопасностью

4.1 Цель

Данный раздел определяет управление и технические действия, необходимые для достижения требуемой функциональной безопасности СБЭСУ.

4.2 Требования

4.2.1 План обеспечения функциональной безопасности должен быть составлен и документально оформлен для каждого проекта СБЭСУ и обновляться по мере необходимости. Он должен включать процедуры по управлению действиями, определенными в разделах 5–9.

Примечание — Содержание плана обеспечения функциональной безопасности должно зависеть от следующих конкретных характеристик проекта:

- размер;
- степень сложности;
- степень новизны и используемых технологий;
- уровень стандартизации характеристик;
- возможное(ые) последствие(я) в случае отказа.

В частности план должен содержать:

a) идентификацию соответствующих действий, заданных в разделах 5–9;

b) описание политики и стратегии для выполнения заданных требований к функциональной безопасности;

c) описание стратегии обеспечения функциональной безопасности для прикладного программного обеспечения, разработки, интеграции, верификации и подтверждения соответствия СБЭСУ;

d) идентификацию лиц, департаментов или других подразделений и ресурсов, которые отвечают за проведение и рассмотрение каждого из мероприятий, указанных в разделах 5–9;

e) определение или формирование процедуры и ресурсов для записи и сохранения информации, относящейся к функциональной безопасности СБЭСУ.

Примечание — Необходимо рассмотреть следующее:

- результаты идентификации опасностей и оценки рисков;
- оборудование, используемое для связанных с безопасностью функций, с требованиями к системе безопасности;
- организацию, ответственную за поддержание функциональной безопасности;
- процедуры, необходимые для достижения и поддержания функциональной безопасности (в том числе модификаций СБЭСУ);

f) описание стратегии управления конфигурацией (см. 9.3), учитывающей соответствующие организационные проблемы, такие как наличие уполномоченных лиц и внутренней структуры организации;

g) созданный план верификации, включающий:

- подробную информацию о том, когда проводят верификацию;
- подробную информацию о лицах, отделах или подразделениях, которые осуществляют верификацию;
- информацию о выборе стратегий и методов верификации;
- информацию о выборе и использовании контрольно-измерительного оборудования;
- информацию о выборе действий по верификации;
- критерии приемки;
- информацию о средствах, которые будут использовать для оценки результатов верификации;

h) созданный план подтверждения соответствия, включающий:

- подробную информацию о том, когда проводят подтверждение соответствия;
- информацию об определении соответствующих режимов работы машины (например, нормальная работа, установка);
- требования, в соответствии с которыми следует проводить подтверждение соответствия СБЭСУ;
- описание технической стратегии для подтверждения соответствия, например аналитические методы или статистические тесты;
- критерии приемки;
- описание предпринимаемых действий в случае невыполнения критериев приемки.

Примечание — Необходимо, чтобы план подтверждения соответствия указывал, должны ли СБЭСУ и ее подсистемы быть предметом для обычного тестирования, типовых испытаний и/или выборочного тестирования.

4.2.2 План обеспечения функциональной безопасности должен быть реализован для оперативного наблюдения и удовлетворительного решения вопросов, связанных с СБЭСУ и вытекающих из:

- действий, указанных в разделах 5–9;
- действий по верификации;
- действий по подтверждению соответствия.

5 Требования к спецификации связанных с безопасностью функций управления

5.1 Цель

Данный раздел устанавливает процедуры для определения требований к СБФУ, реализуемых СБЭСУ.

5.2 Спецификация требований к СБФУ

5.2.1 Общие положения

5.2.1.1 Как указано в ИСО 12100-1, ИСО 12100-2 и ИСО 14121, необходимость в функциях безопасности определяется исходя из стратегии по снижению риска.

5.2.1.2 Если функции безопасности выбраны для реализации (полностью или частично) СБЭСУ, то СБФУ должны быть специфицированы (см. 3.2.16).

5.2.1.3 Спецификация каждой СБФУ должна включать спецификацию:

- функциональных требований (см. 5.2.3);
- требований к полноте безопасности (см. 5.2.4).

Они должны быть документально оформлены в спецификации требований к системе безопасности (СТСБ).

Примечания

1 Если для выполнения функции безопасности используют неэлектрическое оборудование совместно с электрическими средствами, то целевые значения отказов, применимые к неэлектрическому оборудованию, в настоящем стандарте не рассматривают. Электрические средства — любые устройства или системы, работающие на электрических принципах, в том числе:

- электромеханические устройства;
- непрограммируемые электронные устройства;
- программируемые электронные устройства.

2 Необходимо обеспечить управление версиями СТСБ, которое должно быть одной из процедур управления конфигурацией (см. 9.3).

5.2.1.4 СТСБ должна быть проверена, чтобы обеспечить согласованность и полноту для предназначенного использования.

Примечание — Например, это может быть достигнуто путем осмотра, анализа, применения метода таблицы контрольных проверок (см. также В.2.6 МЭК 61508-7).

5.2.2 Необходимая информация

Для формирования спецификации функциональных требований и спецификации требований к функциональной безопасности для каждой СБФУ необходима следующая информация:

- для каждой конкретной опасности результаты оценки риска для машины, в том числе все функции безопасности, которые определены как необходимые для снижения риска;
- эксплуатационные характеристики машины, в том числе:
  - режимы работ,
  - время цикла,
  - характеристика времени отклика,
  - условия окружающей среды,
  - взаимодействие персонала с машиной (например, при ремонте, установке, уборке);
- вся информация, относящаяся к СБФУ, которая может повлиять на проектирование СБЭСУ, например:
  - описание поведения машины, которое СБФУ должна обеспечить или предотвратить,
  - все интерфейсы между СБФУ, а также между СБФУ и любыми другими функциями (внутри или вне машины),
  - требуемая функциональная реакция на отказ для СБФУ.

Примечание — Некоторая информация может быть недоступна или полностью не определена перед началом итерационного процесса проектирования СБЭСУ, поэтому в процессе проектирования необходимо обновлять спецификации требований к безопасности СБЭСУ.

5.2.3 Спецификация функциональных требований к СБФУ

Спецификация функциональных требований к СБФУ должна содержать подробное описание каждой реализуемой СБФУ, включая в соответствующих случаях:

- условие(я) (например, режим работы) машины, при котором(ых) СБФУ должна быть активна или заблокирована;
- приоритет тех функций, которые могут быть одновременно активны и вызвать конфликтную ситуацию;
- частоту работы каждой СБФУ;
- требуемое время реакции каждой СБФУ;
- интерфейс(ы) СБФУ с другими функциями машины;
- требуемое время отклика (например, устройства ввода и вывода);
- описание каждой СБФУ;
- описание функции(й) реакции на отказ и любых ограничений, например на повторный запуск или продолжение работы машины в тех случаях, когда первоначальная реакция на отказ — остановка машины;
- описание окружающих условий (например, температуры, влажности, пыли, химических веществ, механических вибраций и ударов);
- испытания и любые необходимые для этого средства (например, испытательное оборудование, порты доступа тестов);
- частоту циклов выполнения операций, рабочий цикл и/или категории применения для электромеханических устройств, предназначенных для использования в СБФУ.

Примечания

1 Кроме требований МЭК 61000-6-2 к СБЭСУ, предназначенных для использования в промышленных условиях, следует выполнять требования к уровням электромагнитной (ЭМ) устойчивости, приведенные в МЭК 61236-2-1. СБЭСУ для использования в другой ЭМ среде (например, жилые помещения), должны иметь уровни устойчивости в соответствии с указанными в различных стандартах по электромагнитной совместимости (например, для жилых помещений по МЭК 61000-6-1).

2 При определении уровней электромагнитной устойчивости необходимо рассмотреть вопрос о целесообразности применения используемых в различных стандартах уровней электромагнитной совместимости для случаев, которые могут возникнуть в применении СБЭСУ, даже с низкой вероятностью их возникновения.

3 Критерий электромагнитной устойчивости для функциональной безопасности СБЭСУ приведен в 6.4.3.

5.2.4 Спецификация требований к полноте безопасности для СБФУ

5.2.4.1 Требования к полноте безопасности для каждой СБФУ должны определяться исходя из оценки возможного риска, чтобы обеспечить его необходимое снижение. В настоящем стандарте требование к полноте безопасности выражается в виде целевой величины отказов для вероятности опасных отказов в час для каждой СБФУ.

5.2.4.2 Требования к полноте безопасности для каждой СБФУ должны задаваться в терминах УПБ в соответствии с таблицей 2 и документально оформляться. Пример метода определения УПБ приведен в приложении А.

Таблица 2 — Уровни полноты безопасности. Целевые величины отказов

Уровень полноты безопасности (УБП)	Вероятность опасных отказов в час (PFH_D)
3	$\geq 10^{-8}$ — $< 10^{-7}$
2	$\geq 10^{-7}$ — $< 10^{-6}$
1	$\geq 10^{-6}$ — $< 10^{-5}$

Примечание — Если требуемая полнота безопасности СБФУ меньше, чем УПБ 1, то как минимум требования категории B ИСО 13849-1 должны быть удовлетворены.

5.2.4.3 Если в стандарте на изделие определен УПБ для СБФУ, то он должен иметь приоритет над приложением А.

6 Проектирование и интеграция связанной с безопасностью электрической системы управления (СБЭСУ)

6.1 Цель

Данный раздел устанавливает требования к выбору или проектированию СБЭСУ, удовлетворяющей функциональные требования и требования к полноте безопасности, указанные в спецификации требований к системе безопасности (см. 5.2).

6.2 Общие требования

6.2.1 СБЭСУ должна быть выбрана или разработана с учетом спецификации требований к системе безопасности (см. 5.2) и, где это необходимо, с учетом спецификации требований к программному обеспечению системы безопасности (см. 6.10) в соответствии с требованиями настоящего стандарта.

6.2.2 Методы выбора или проектирования СБЭСУ (в том числе общей архитектуры аппаратных средств и программного обеспечения, датчиков, приводов, программируемой электроники, встроенного и прикладного программного обеспечения и т. п.) должны соответствовать 6.5 или 6.6. Какой бы метод ни использовался, СБЭСУ должна соответствовать следующим требованиям:

a) к полноте безопасности аппаратных средств, включая:
- ограничения архитектуры на полноту безопасности аппаратных средств (см. 6.6.3.3),
- требования к вероятности опасных случайных отказов аппаратных средств (см. 6.6.3.2);

b) к систематической полноте безопасности, включая:
- требования к возможности избежать отказы,
- требования к управлению систематическими ошибками;

c) к поведению СБЭСУ при выявлении ошибки (см. 6.3);

d) к проектированию и разработке связанного с безопасностью программного обеспечения (см. 6.10 и 6.11).

6.2.3 Проект СБЭСУ должен учитывать возможности и ограничения человека (в том числе разумно предсказуемое неправильное использование) и быть пригодным для действий, выполняемых операторами, обслуживающим персоналом и другими, кто может взаимодействовать с СБЭСУ. Необходимо, чтобы проектирование всех интерфейсов оператором следовало «хорошим практикам» учета человеческого фактора (см. МЭК 61310), а также учитывало вероятный уровень подготовки или осведомленности операторов, в частности при массовом производстве подсистем, где оператором может быть любой человек.

Примечание — Цель проекта должна состоять в том, чтобы разумно предсказуемые ошибки, сделанные операторами или обслуживающим персоналом, были предотвращены или устранены при проектировании. Если это невозможно, то, чтобы минимизировать возможность ошибок оператора и удостовериться в том, что предсказуемые ошибки не приводят к увеличению риска, должны быть также применены другие средства (например, реализация действия вручную с дополнительным подтверждением перед его выполнением).

6.2.4 В целях содействия реализации этих свойств в ходе разработки и интеграции СБЭСУ должны быть рассмотрены ремонтопригодность и тестируемость СБЭСУ.

6.2.5 Необходимо, чтобы проект СБЭСУ, его диагностические функции и функции реакции на отказ были документально оформлены. Эта документация должна:
- быть точной, полной и краткой;
- соответствовать предназначенной цели;
- быть доступной и поддерживаемой;
- быть обеспечена управлением версиями.

6.2.6 Данные, полученные в результате проектирования, разработки и реализации СБЭСУ, должны быть верифицированы на соответствующих этапах.

6.3 Требования к поведению СБЭСУ при обнаружении в ней сбоя

6.3.1 Обнаружение опасного сбоя в любой из подсистем, которая имеет значение устойчивости к сбоям аппаратных средств больше чем ноль, влечет за собой выполнение специфицированной функции реакции на отказ.

Такая спецификация может содержать действия по изоляции неисправных частей подсистемы для продолжения безопасной эксплуатации машины в то время, как происходит ремонт неисправных частей. Если неисправная деталь не будет восстановлена в течение максимального времени, оцененного, как принято из расчета вероятности случайного сбоя в технических средствах (см. 6.7.8), то для поддержки безопасного состояния должна быть выполнена реакция на второй сбой.

Если для СБЭСУ предусмотрен ремонт в неавтономном режиме, то изоляцию неисправного элемента применяют только тогда, когда это не приводит к увеличению вероятности опасных случайных сбоев аппаратных средств СБЭСУ, указанной выше в спецификации требований к системе безопасности.

После появления неисправностей, снижающих устойчивость к сбоям аппаратных средств до нуля, применяют требования 6.3.2.

Примечание — При определении среднего времени восстановления (см. МЭС 191-13-08), которое рассматривается в модели надежности, необходимо учитывать интервал диагностических проверок, время ремонта и любые другие задержки при восстановлении.

6.3.2 Если для достижения требуемой вероятности случайных опасных отказов аппаратных средств необходима(ы) функция(и) диагностики и подсистема имеет устойчивость к сбоям аппаратных средств, равную нулю, то обнаружение сбоя и заданная на него реакция должны быть выполнены до того, как может произойти опасная ситуация, предусмотренная СБФУ.

Исключение к 6.3.2. Если подсистема реализует конкретную СБФУ, у которой устойчивость к сбоям аппаратных средств равна нулю, а отношение частоты диагностического тестирования к частоте запросов превышает 100, то интервал диагностического тестирования этой подсистемы должен быть таким, чтобы она удовлетворяла требование к вероятности опасного случайного сбоя технических средств.

6.3.3 Если выполнение функции реакции на сбой как части СБФУ, для которой определен УПБ 3, привело к остановке машины, то последующая нормальная работа машины с СБЭСУ (например, ее повторный запуск) не должна выполняться до тех пор, пока сбой не будет восстановлен или исправлен. Для СБФУ с заданной полнотой безопасности менее УПБ 3 поведение машины после выполнения функции реакции на сбой (например, перезапуск нормальной работы) должно зависеть от спецификации соответствующих функций реакции на сбой (см. 5.2.3).

6.4 Требования к систематической полноте безопасности СБЭСУ

6.4.1 Требования для предотвращения систематических отказов аппаратных средств

6.4.1.1 Должны быть применены следующие меры:

a) необходимо, чтобы СБЭСУ была спроектирована и реализована в соответствии с планом функциональной безопасности (см. 4.2);

b) правильные выбор, состав, схемы, сборка и установка подсистем, в том числе кабелей, проводов и любых соединений;

c) применение СБЭСУ в соответствии со спецификацией производителя;

d) следование указаниям производителя по применению, например каталог, инструкции по установке, и использование хорошей технической практики (см. также D.1 ИСО 13849-2);

e) применение подсистем с совместимыми рабочими характеристиками (см. также D.1 ИСО 13849-2);

f) СБЭСУ должна быть защищена в соответствии с МЭК 60204-1;

g) предотвращение потери функции заземления в соответствии с МЭК 60204-1;

h) не должны использоваться документально не оформленные режимы работы компонентов (например, «зарезервированные» регистры программируемого оборудования);

i) рассмотрение предсказуемого неправильного использования, изменений окружающей среды или модификации(й).

6.4.1.2 Кроме этого, должен(на) быть применен(а) по крайней мере один(на) из следующих методов и/или мер, с учетом сложности СБЭСУ и УПБ для тех функций, которые будут реализованы СБЭСУ:

a) анализ проекта аппаратных средств СБЭСУ (например, с помощью проверки или сквозного контроля) для выявления в результате осмотров и/или анализа расхождений между спецификацией и реализацией;

Примечание — Для того чтобы выявить несоответствия между спецификацией и реализацией, любые точки сомнения или потенциально слабые места реализации, исполнения и использования изделия документально оформляют так, чтобы они могли быть решены, учитывая, что во время процедуры проверки автор пассивен, а инспектор активен, а при процедуре сквозного контроля автор активен, и инспектор пассивен;

b) средства для консультации, например пакеты автоматизированного проектирования, выполняющие моделирование или анализ, и/или средства автоматизированного проектирования, чтобы выполнять процедуры проектирования на систематической основе с использованием предварительно разработанных элементов, которые уже доступны и протестированы.

Примечание — Полнота этих инструментов может быть продемонстрирована конкретным тестированием, обширной историей удовлетворительного использования или независимой верификацией их выходных результатов для конкретно разрабатываемой СБЭСУ (см. 6.11.3.4);

c) моделирование, которое систематически и полно реализует представление проекта СБЭСУ как в терминах функциональных характеристик, так и с точки зрения правильного определения размеров и взаимодействия ее подсистем.

Пример — Функция СБЭСУ может быть смоделирована на компьютере с помощью программного обеспечения, моделирующего поведение (см. 6.11.3.4), где отдельные подсистемы или каждый их элемент имеют собственное моделируемое поведение, а реакция всей схемы, в которую они включены, проверяется при предельных значениях данных для каждой подсистемы или ее элемента.

6.4.2 Требования к управлению систематическими сбоями

Должны быть применены следующие меры:

a) использование обесточивания: необходимо, чтобы СБЭСУ были сконструированы таким образом, чтобы при потере их электропитания машины переходили в безопасное состояние или оставались в нем;

b) контроль за влиянием временных отказов подсистемы: СБЭСУ должна быть сконструирована таким образом, чтобы, например:

- изменение напряжения (прерывания, падения и др.) в отдельных подсистемах или элементах подсистемы не приводило к опасности (например, прерывание напряжения, влияющее на цепи управления двигателем, не должно привести к неожиданному его запуску, когда питание восстанавливается).

Примечание — См. также соответствующие требования в МЭК 60204-1. В частности:

- перенапряжение или пониженное напряжение должно быть обнаружено достаточно рано, чтобы все выходы могли быть переведены в безопасное состояние процедурой отключения питания или переключены на второй энергоблок;

- в случае необходимости, перенапряжение или пониженное напряжение должно быть обнаружено достаточно рано, чтобы внутреннее состояние могло быть сохранено в энергонезависимой памяти и все выходы могли быть установлены или переведены в безопасное состояние процедурой отключения питания или переключены на второй энергоблок;

- воздействие электромагнитных помех от физического окружения или подсистем(ы) не приводило к опасности;

c) управление последствиями ошибок и прочими последствиями, возникающими в результате любого процесса передачи данных, включая ошибки передачи, повторы, удаления, вставки, повторное упорядочивание, искажения, задержка и нелегальное проникновение.

Примечания

1 Более подробную информацию можно найти в МЭК 61784-3 и МЭК 61508-2.

2 Термин «нелегальное проникновение» означает, что истинное содержание сообщения определено неправильно. Например, сообщения от опасного компонента приняты как сообщения от безопасного;

d) если в интерфейсе происходит опасный сбой, то должна быть выполнена функция реакции на отказ до того, как опасность может произойти из-за этого сбоя. Если происходит сбой, который снижает устойчивость к отказам аппаратных средств до нуля, то реакция на этот сбой должна быть выполнена за время, не превышающее предполагаемое *MTTR* (см. перечисление g) 6.7.4.4.2).

Требования перечисления d) относятся к интерфейсам, которые являются входами и выходами подсистем и всех других частей подсистем, включающих или использующих кабельные соединения в процессе интеграции (например, выходной сигнал переключения устройства световой завесы, выход датчика положения ограждения).

Примечание — Подсистема или ее элемент не должны сами выявлять сбой на своих выходах. Функция реакции на отказ может быть инициирована также любой последующей подсистемой после выполнения диагностического теста.

6.4.3 Электромагнитная (ЭМ) устойчивость

Кроме требований МЭК 61000-6-2 и требований к ЭМ процессам, приведенным в МЭК 61326-3-1, СБЭСУ должна удовлетворять следующим критериям электромагнитной устойчивости для функциональной безопасности:

- опасные условия или опасности не должны вноситься;

- связанные с безопасностью функции управления должны выполняться без перебоев;

- выполнение СБФУ, реализуемых СБЭСУ, может быть нарушено временно или постоянно, если безопасное состояние машины поддерживается или достигнуто до возникновения опасности. Если ЭМ явления могут привести к повреждению компонентов, то необходимо удостовериться (например, путем

анализа), что они не повлияют на функциональную безопасность, в том числе и для более низких значений параметров ЭМ явлений, которые могут привести к частичному повреждению.

Примечание — Следует рассмотреть вопрос о поведении СБЭСУ при воздействии на нее ЭМ явлений для всех значений характеристик, приведенных в МЭК 61326-3-1.

6.5 Выбор связанной с безопасностью электрической системы управления

Если поставщик предоставляет СБЭСУ для конкретной функции, указанной в спецификации требований к безопасности системы, то им могут быть выбраны заранее разработанные СБЭСУ вместо проекта, заказанного клиентом, при условии, что эти решения соответствуют спецификации требований к безопасности системы, а также 6.3, 6.4 и 6.6.1.

Примечание — Выбор заранее разработанных СБЭСУ является альтернативой проектирования и разработки конкретных СБЭСУ в соответствии с 6.6.

6.6 Проектирование и разработка СБЭСУ

6.6.1 Общие требования

6.6.1.1 СБЭСУ должна быть спроектирована и разработана в соответствии со спецификацией требований к безопасности СБЭСУ (см. 5.2).

6.6.1.2 Необходимо соблюдать четко структурированный процесс проектирования, он также должен быть документально оформлен (см. 6.6.2).

6.6.1.3 Если для достижения требуемой полноты безопасности при обнаружении сбоя необходимо использование диагностики, то СБЭСУ должна выполнять заданную функцию реакции на отказ (см. 5.2 и 6.3).

6.6.1.4 Если СБЭСУ или компонент СБЭСУ (т. е. ее подсистема(ы)) реализует СБФУ и другие функции, не относящиеся к безопасности, то все ее технические средства и программное обеспечение следует рассматривать как связанные с безопасностью до тех пор, пока не будет установлено, что СБФУ и другие функции выполняются достаточно независимо (т. е. нормальная работа или отказ какой-либо функции не станет причиной отказа СБФУ).

Примечание — Достаточную независимость выполнения устанавливают демонстрацией того, что вероятность зависимого отказа между компонентами, не связанными и связанными с безопасностью, эквивалентна уровню полноты безопасности СБЭСУ.

6.6.1.5 Если СБЭСУ или ее подсистемы реализуют связанные с безопасностью функции управления с различными уровнями полноты безопасности, то требования к аппаратным средствам и программному обеспечению СБЭСУ или ее подсистем следует определять уровнем полноты безопасности СБФУ с самым высоким уровнем полноты безопасности, если не будет установлено, что выполнение СБФУ с различными уровнями полноты безопасности достаточно независимо.

Примечание — Достаточную независимость выполнения устанавливают демонстрацией того, что вероятность зависимого отказа между компонентами, выполняющими СБФУ с различными уровнями полноты безопасности, эквивалентна уровню полноты безопасности, достигаемому СБЭСУ.

6.6.1.6 Соединения (например, проводники, кабели), кроме используемых для цифровой передачи данных, следует рассматривать как элементы одной из подсистем, к которой они подключены (см. также перечисление g) 6.4.2).

6.6.1.7 Если система цифровой передачи данных реализуется как часть СБЭСУ, то она должна удовлетворять соответствующим требованиям МЭК 61508-2 в соответствии с целевыми значениями УПБ для СБФУ.

6.6.1.8 Информация по применению СБЭСУ должна определять методы и меры, необходимые для использования в течение проектных стадий жизненного цикла СБЭСУ и обеспечения соответствующего уровня полноты безопасности.

6.6.2 Процесс проектирования и разработки

Проектирование и разработка следует выполнять в соответствии с четко определенным процессом, учитывающим все связанные с ним аспекты и представленным на рисунке 2.

Примечание — В настоящем стандарте используется подход, основанный на применении структурированного процесса проектирования СБЭСУ, начиная с требований, определенных в спецификации требований к системе безопасности. На рисунке 2 представлен процесс проектирования и терминология, которая применяется на разных стадиях.

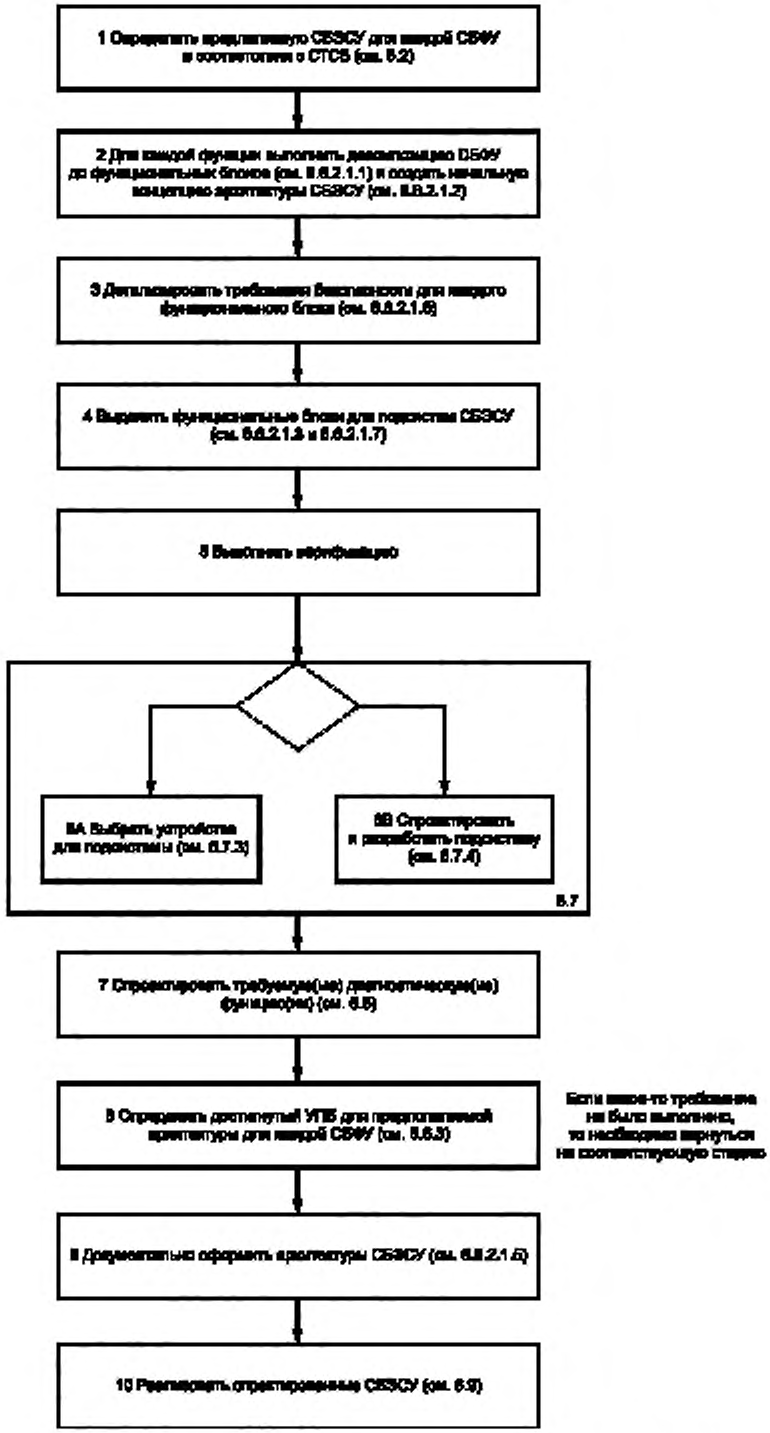


Рисунок 2 — Структура процесса проектирования и разработки СБЭСУ

6.6.2.1 Проектирование архитектуры системы

6.6.2.1.1 Каждая СБФУ, как указано в спецификации требований к безопасности СБЭСУ, должна быть структурно декомпозирована до функциональных блоков, например, как показано на рисунке 3. Необходимо, чтобы такая структура была документально оформлена и включала:

- ее описание;
- требования к безопасности (функциональные, к полноте) для каждого функционального блока;
- определение входов и выходов каждого функционального блока.

Примечания

1 Процесс декомпозиции позволяет сформировать структуру функциональных блоков, полностью описывающую функциональные требования и требования к полноте СБФУ. Этот процесс должен быть применен до уровня, позволяющего установить функциональные требования и требования к полноте для каждого функционального блока, который будет реализован в подсистеме, если такое выделение функциональных блоков и полных требований для реализации подсистемами возможно. Тем не менее можно реализовать несколько функциональных блоков в одной подсистеме, но невозможно один функциональный блок реализовать несколькими подсистемами, каждая из которых имеет свои функциональные требования и требования к полноте безопасности. Если это необходимо, то следует выделить функциональные требования одного функционального блока для их реализации дополнительными элементами подсистемы, см. 6.7.4.

2 На входах и выходах каждого функционального блока может быть обрабатываемая информация, например о скорости, положении, режиме работы и т. д.

3 Функциональные блоки представляют функции СБФУ (см. 3.2.16) и не включают диагностические функции СБЭСУ (см. 3.2.17). Для достижения целей настоящего стандарта диагностические функции рассматриваются как отдельные, которые могут иметь структуру, отличную от СБФУ (см. 6.8).

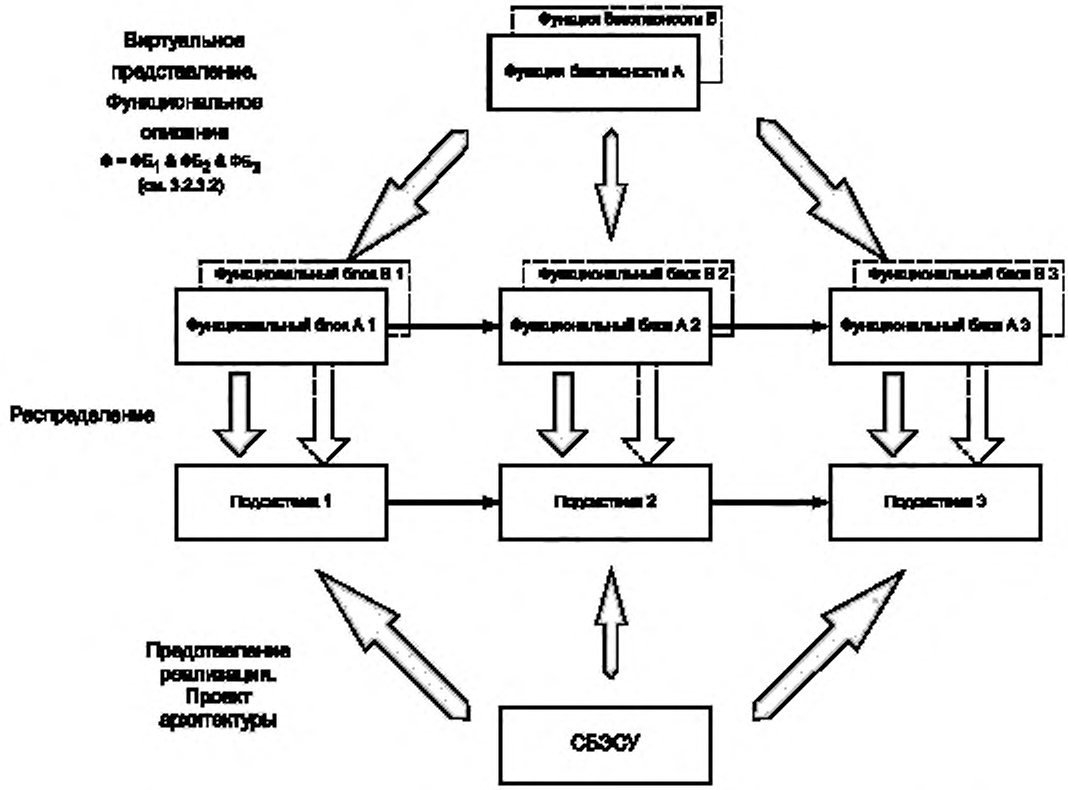


Рисунок 3 — Распределение требований к безопасности между функциональными блоками в подсистемах (см. 6.6.2.1.1)

6.6.2.1.2 Необходимо, чтобы начальная концепция архитектуры СБЭСУ была создана в соответствии со структурой функциональных блоков.

Примечание — Должно быть постоянное сотрудничество между разработчиком связанной с безопасностью архитектуры (системы) управления, организацией, ответственной за конфигурацию устройств, и разработчиком программного обеспечения. В процессе такого сотрудничества уточняются требования к безопасности программного обеспечения и возможные его архитектуры, что может повлиять на архитектуру аппаратных средств СБЭСУ, поэтому такое тесное сотрудничество между разработчиком архитектуры СБЭСУ, поставщиком(ами) подсистемы, разработчиком программного обеспечения и, по мере необходимости, проектировщиком машины или пользователем может помочь сократить возможность появления систематических отказов.

6.6.2.1.3 Каждый функциональный блок должен быть реализован соответствующей подсистемой в архитектуре СБЭСУ. Одна подсистема может реализовать более одного функционального блока.

6.6.2.1.4 Каждая подсистема и реализуемые в ней функциональные блоки должны быть четко определены.

6.6.2.1.5 Необходимо, чтобы архитектура была документально оформлена, ее подсистемы и их взаимосвязи были описаны.

6.6.2.1.6 Требования к безопасности для каждого функционального блока должны быть сформулированы, как указано в спецификации требований к безопасности соответствующей СБФУ, в терминах:

- функциональных требований (например, входная информация, внутренняя логика работы и выходная информация функционального блока);
- требований к полноте безопасности.

6.6.2.1.7 Требования к безопасности для подсистемы должны быть такими же, как и для функциональных блоков, которые она реализует. Если подсистема реализует более одного блока, то для нее применяется требование с наибольшим значением полноты безопасности (см. 6.6.3). Эти требования должны быть документально оформлены в качестве спецификации требований к безопасности подсистемы.

6.6.3 Требования к оценке полноты безопасности, достигаемой СБЭСУ

6.6.3.1 Общие положения

УПБ, который может быть достигнут СБЭСУ, следует рассматривать отдельно для каждой СБФУ, выполняемой СБЭСУ.

УПБ, который может быть достигнут СБЭСУ, определен вероятностью опасных случайных отказов технических средств, архитектурными ограничениями, а также систематической полнотой безопасности подсистем, входящих в СБЭСУ. Достигаемый с помощью СБЭСУ УПБ меньше или равен наименьшему значению предельного требования к УПБ любой из подсистем, входящих в СБЭСУ.

6.6.3.2 Полнота безопасности технических средств

6.6.3.2.1 Вероятность опасного отказа каждой СБФУ из-за случайных опасных отказов технических средств должна быть меньше или равна целевой величине отказов, заданной в спецификации требований к безопасности.

Примечание — Целевые значения отказов, связанные с УПБ, приведены в таблице 2.

6.6.3.2.2 Вероятность опасного отказа каждой СБФУ из-за случайных опасных отказов технических средств должна быть оценена с учетом:

a) архитектуры СБЭСУ, поскольку это касается каждой рассматриваемой СБФУ.

Примечание — При этом приходится решать, какие виды отказов подсистем находятся в последовательной связи (любой отказ вызывает отказ соответствующей СБФУ, которая должна выполняться), а какие — в параллельной (для сбоя соответствующей СБФУ необходимы совпадающие отказы);

b) оцененной частоты отказов каждой подсистемы для функциональных блоков, которые она реализует, в любых режимах, способных вызвать опасный отказ СБЭСУ.

6.6.3.2.3 Оценка вероятности опасных отказов должна быть основана на вероятности случайных опасных отказов аппаратных средств каждой соответствующей подсистемы, которая определяется с использованием информации, перечисленной в 6.7.2.2, с учетом в соответствующих случаях 6.7.2.2, перечисление к) для цифровой передачи данных между процессами подсистем. Вероятность случайных отказов аппаратных средств в СБЭСУ является суммой вероятностей опасных случайных отказов аппаратных средств всех подсистем, участвующих в реализации СБФУ, и включает в случае необходимости вероятность опасных ошибок цифровой передачи данных коммуникационных процессов:

$$PFH_D = PFH_{D1} + ... + PFH_{Dn} + P_{TE}.$$

Примечания

1 Данный подход основан на определении функционального блока, отказ любого функционального блока может привести к отказу СБФУ (см. 3.2.16).

2 Взаимодействия, отличные от цифровой передачи данных, считаются частью подсистем.

6.6.3.3 Ограничения архитектуры

УПБ, достигаемый СБЭСУ в соответствии с архитектурными ограничениями, меньше или равен наименьшему значению предельного требования к УПБ любой из подсистем (см. 6.7.6), участвующих в выполнении СБФУ.

Примечание — Например, СБЭСУ состоит из двух последовательно соединенных подсистем (подсистема 1 и подсистема 2), где ДБО и устойчивость к отказам каждой подсистемы равны значениям, показанным в таблице 3. Оценка *PFHD* для СБЭСУ $8 \cdot 10^{-8}$, что соответствует УПБ 3. Тем не менее в соответствии с таблицей 4 архитектурное ограничение подсистемы 2 лимитирует УПБ, которое может быть достигнуто СБЭСУ, до УПБ 2.

Таблица 3 — Характеристики подсистем 1 и 2, используемые в примере (см. примечание к 6.6.3.3)

Подсистема	Устойчивость к отказам технических средств	ДБО	Предельное требование к УПБ в соответствии с ограничениями архитектуры (см. таблицу 4)
1	1	95 %	УПБ 3
2	1	80 %	УПБ 2

6.7 Реализация подсистем

6.7.1 Цель

Цель состоит в том, чтобы реализовать подсистему, отвечающую всем требованиям к безопасности, определенным для реализуемых ею функциональных блоков (см. рисунок 3). Рассматриваются два подхода:

- выбор устройства, которое является достаточным для выполнения требований данной подсистемы, т. е. она должна отвечать спецификации требований к безопасности каждого из реализуемого ею функционального блока и требованиям настоящего стандарта;
- проектирование и разработка подсистемы на основе комбинирования элементов функциональных блоков с учетом их организации и взаимодействия в функциональном блоке.

6.7.2 Общие требования к реализации подсистемы

6.7.2.1 Подсистема должна быть реализована с помощью выбора из существующих подсистем (см. 6.7.3) либо спроектирована (см. 6.7.4) в соответствии с ее спецификацией требований к безопасности (см. 6.6.2.1.7) с учетом всех требований 6.2. Подсистема(ы), включающая(ие) сложные компоненты, должна(ы) удовлетворять МЭК 61508-2 и МЭК 61508-3 для требуемого УПБ, и проект должен использовать Способ 1_H (см. 7.4.4.2 МЭК 61508-2).

Исключение. Если проект подсистемы включает элемент подсистемы, являющийся сложным компонентом, то применяют требования 6.7.4.2.3.

Примечание — В настоящем стандарте предполагается, что проектирование сложных программируемых электронных подсистем или их элементов удовлетворяет соответствующим требованиям МЭК 61508 и используется Способ 1_H (см. 7.4.4.2 МЭК 61508-2). Считается, что Способ 2_H (7.4.4.3 МЭК 61508-2) не подходит в общем случае для машинного оборудования, поэтому настоящий стандарт не рассматривает Способ 2_H. В настоящем стандарте представлена методология для применения, а не разработки подсистем и их элементов, являющихся частью СБЭСУ.

6.7.2.2 Для каждой подсистемы должна быть доступна следующая информация:

a) функциональная спецификация для тех функций и интерфейсов подсистемы, которые могут использоваться СБЭСУ;

b) предполагаемые интенсивности отказов (из-за случайных отказов аппаратных средств), заявленные в любых режимах, способные вызвать опасный отказ СБЭСУ.

Примечание — Для электромеханических подсистем вероятность отказа должна быть оценена с учетом количества операционных циклов, заявленных изготовителем, и рабочим циклом (см. 5.2.3). Необходимо, чтобы эта информация была основана на величине B_{10} (см МЭК 61649) при условиях эксплуатации, утвержденных производителем. См. например приложение К МЭК 60947-4-1;

c) ограничения, накладываемые на подсистему:

– окружающей средой и условиями эксплуатации, которые необходимо контролировать, чтобы обеспечить соответствие планируемых интенсивностей отказов из-за случайных отказов аппаратных средств,

- сроком жизни подсистемы, который нельзя превышать, чтобы обеспечить соответствие планируемых интенсивностей отказов из-за случайных отказов аппаратных средств;

d) любые требования к тестированию и/или техническому обслуживанию;

e) охват диагностикой и интервал диагностических проверок (если требуется, см. примечание).

Примечание — Перечисление e) касается диагностических функций, которые являются внешними к подсистеме. Эта информация требуется только тогда, когда необходимо доверие к модели надежности СБЭСУ при реализации диагностических функций, выполняемых в подсистеме;

f) любая дополнительная информация (например, о временах ремонта), которая необходима для определения среднего времени восстановления *MTTR* после обнаружения ошибки диагностикой.

Примечание — Перечисления b) — f) необходимы для оценки вероятности отказа в 1 ч для СБЭСУ;

g) предельное требование к УПБ вследствие архитектурных ограничений (см. 6.7.6), или:

- вся информация, которая необходима для вычисления доли безопасных отказов (ДБО) подсистемы, как это принято для СБЭСУ.

Примечания

1 Необходима информация о возможных режимах отказов подсистемы. На основе информации о режиме отказа подсистемы можно решить, вызывает ли ее отказ безопасный или опасный отказ СБЭСУ.

2 Более подробно об оценке ДБО см. 6.7.7;

- и устойчивость к отказам аппаратных средств подсистемы;

h) любые ограничения на применение подсистемы, которые необходимо рассмотреть для предотвращения систематических отказов;

i) самый высокий уровень полноты безопасности, на который может претендовать СБЭСУ и который использует подсистема на основе:

- мер и методов, применяемых для предотвращения систематических отказов во время разработки и реализации аппаратных средств и программного обеспечения подсистемы,

- конструктивных особенностей, допускающих в подсистеме систематические ошибки.

Примечание — Перечисления h) и i) необходимы, чтобы определить самый высокий уровень полноты безопасности, на который может претендовать СБЭСУ согласно ограничениям архитектуры. Кроме того, эти перечисления могут использоваться для обеспечения связи (см. таблицы 3 и 4) с требованиями к категориям из ИСО 13849-1 и с точки зрения обнаружения ошибок, и с точки зрения устойчивости к отказам аппаратных средств;

j) любая информация, которая требуется для идентификации конфигурации аппаратных средств и программного обеспечения подсистемы, чтобы обеспечить управление конфигурацией СБЭСУ в соответствии с 6.11.3.2;

k) вероятность опасных ошибок передачи для цифровых процессов передачи данных, когда это применимо.

6.7.3 Требования к выбору существующих (предварительно спроектированных) подсистем

6.7.3.1 Если поставщик предлагает подсистему для конкретной СБФУ, указанной в спецификации требований к безопасности, то может быть выбрана заранее разработанная подсистема, а не специально спроектированная, при условии, что она удовлетворяет спецификацию требований к безопасности для подсистемы, 6.4.3 и 6.7.3.2 или 6.7.3.3.

6.7.3.2 Подсистемы, включающие сложные компоненты, должны соответствовать МЭК 61508-2 и МЭК 61508-3 в зависимости от требуемого УПБ, и проект должен использовать Способ 1_H (см. 7.4.4.2 МЭК 61508-2).

Исключение. Если в проекте подсистемы ее элемент является сложным компонентом, то применяется 6.7.4.2.3.

Примечание — В настоящем стандарте предполагается, что проектирование сложных программируемых электронных подсистем или их элементов удовлетворяет соответствующим требованиям МЭК 61508 и используется Способ 1_H (см. 7.4.4.2 МЭК 61508-2). Считается, что Способ 2_H (7.4.4.3 МЭК 61508-2) не подходит в общем случае для машинного оборудования, поэтому настоящий стандарт не рассматривает Способ 2_H. В настоящем

стандарте представлена методология для применения, а не разработки подсистем и их элементов, являющихся частью СБЭСУ.

6.7.3.3 Подсистемы с компонентами только низкой сложности должны соответствовать 6.7.4.4.1, 6.7.6.2, 6.7.6.3, 6.7.7, 6.7.8 и 6.8.

6.7.4 Проектирование и разработка подсистем

6.7.4.1 Цели

6.7.4.1.1 Первая цель заключается в разработке подсистемы, отвечающей требованиям к безопасности для реализуемого(ых) функционального(ых) блока(ов).

6.7.4.1.2 Вторая — в создании архитектуры на уровне совместно работающих элементов подсистемы, удовлетворяющей функциональные требования и требования к полноте безопасности всех функциональных блоков, ею реализуемых.

6.7.4.2 Общие требования

6.7.4.2.1 Необходимо, чтобы подсистема была спроектирована в соответствии со спецификацией требований к системе безопасности.

6.7.4.2.2 Подсистема должна удовлетворять все следующие требования:

a) к полноте безопасности аппаратных средств, включающие:

- ограничения архитектуры на полноту безопасности аппаратных средств (см. 6.7.6);
- требования к вероятности случайных опасных отказов аппаратных средств (см. 6.7.8);

b) систематической полноте безопасности, включающие:

- требования к предотвращению отказов (см. 6.7.9.1), а также к управлению систематическими отказами (см. 6.7.9.2);
- подтверждение того, что работа оборудования «доказана на практике». В этом случае подсистема должна отвечать соответствующим требованиям 7.4.10 МЭК 61508-2;

c) поведению подсистемы при обнаружении отказа (реакция на отказ) (см. 6.3).

6.7.4.2.3 Если проект подсистемы включает сложный компонент (в качестве элемента подсистемы), который удовлетворяет все соответствующие требования МЭК 61508-2 и МЭК 61508-3, связанные с предельным требованием к УПБ и использует Способ 1_H (см. 7.4.4.2 МЭК 61508-2), то он может рассматриваться как компонент низкой сложности в контексте проекта подсистемы, так как известна информация о его соответствующих режимах отказов, поведении при их обнаружении, интенсивности отказов, а также другая связанная с безопасностью информация. Такие компоненты следует использовать только в соответствии со спецификацией и информацией по их применению, предоставляемой их поставщиком.

Примечание — В настоящем стандарте предполагается, что проектирование сложных программируемых электронных подсистем или их элементов удовлетворяет соответствующим требованиям МЭК 61508 и используется Способ 1_H (см. 7.4.4.2 МЭК 61508-2). Считается, что Способ 2_H (см. 7.4.4.3 МЭК 61508-2) не подходит в общем случае для машинного оборудования, поэтому настоящий стандарт не рассматривает Способ 2_H. В настоящем стандарте представлена методология для применения, а не разработки подсистем и их элементов, являющихся частью СБЭСУ.

6.7.4.3 Процесс проектирования и разработки подсистемы

Проектирование и разработка подсистемы должны следовать четко определенной процедуре, учитывающей все аспекты, охватываемые процессом (он показан на рисунке 4).

6.7.4.3.1 Проектирование архитектуры подсистемы

6.7.4.3.1.1 В процессе проектирования архитектуры подсистемы декомпозиция должна привести к структуре элементов функционального блока, которые полностью представляют функциональные требования этого блока. Данный процесс нужно применять до того уровня, который позволит установить функциональные требования для каждого элемента функционального блока, реализуемого элементами подсистемы (см. пример на рисунке 5).

Примечание — Структура процесса проектирования показана на рисунке 4.

6.7.4.3.1.2 Архитектура подсистемы должна быть описана в терминах ее элементов и их взаимосвязей. В случае необходимости это описание должно также включать информацию об элементах функциональных блоков, которые реализуются элементами подсистемы.

6.7.4.4 Требования к выбору и проектированию элементов подсистемы

6.7.4.4.1 Необходимо, чтобы элементы подсистемы были пригодны для их предполагаемого использования и соответствовали определенным стандартам, если таковые существуют.

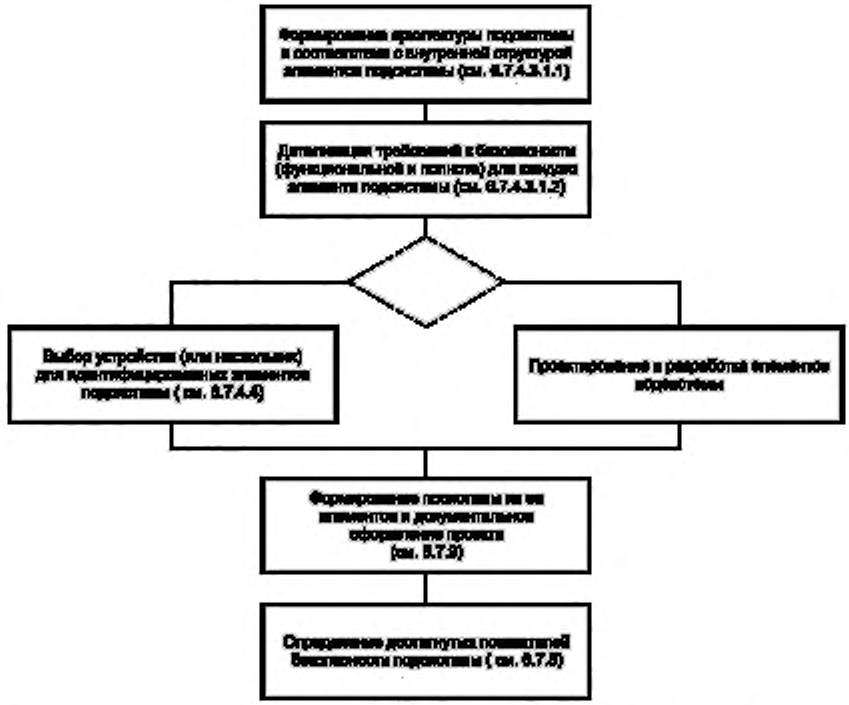


Рисунок 4 — Структура процесса проектирования и разработки подсистемы (см. блок 6В на рисунке 2)

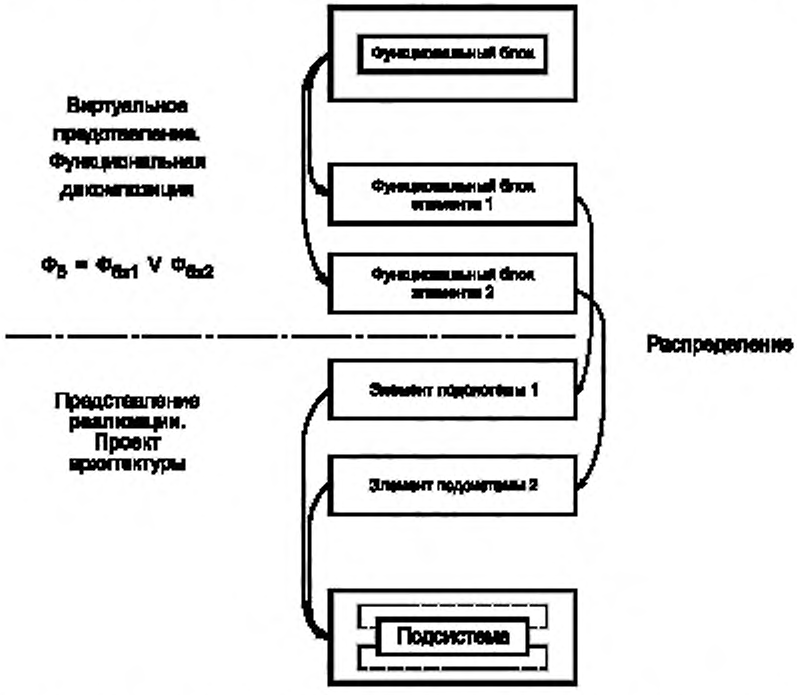


Рисунок 5 — Декомпозиция функционального блока на его элементы и связанные с ними элементы подсистемы

6.7.4.4.2 Для каждого элемента подсистемы должна быть доступна следующая информация:

a) функциональные характеристики элемента подсистемы;

b) спецификация интерфейса элемента подсистемы (например, электрические характеристики);

c) вид каждого отказа и вероятность его возникновения, а также, в соответствующих случаях (например, при использовании сложных компонентов в соответствии с 6.7.4.2.3), охват диагностикой и вероятность опасных отказов.

Примечание — Для электромеханических подсистем вероятность отказа должна быть оценена с учетом числа операционных циклов, заявленных изготовителем, и рабочим циклом (см. 5.2.3). Необходимо, чтобы эта информация была основана на величине B_{10} (см. МЭК 61649) при условиях эксплуатации, утвержденных производителем. См., например, приложение К МЭК 60947-4-1.

d) ограничения, накладываемые на элемент подсистемы:

- окружающей средой и условиями эксплуатации, которые необходимо контролировать, чтобы обеспечить соответствие информации, заданной в перечислении c),

- сроком жизни элемента подсистемы; он не должен быть превышен для обеспечения соответствия информации, заданной в перечислении c);

e) любые требования к периодическим контрольным проверкам и/или техническому обслуживанию;

f) особенности, которые могут влиять на диагностику (например, механическое соединение контактов);

g) любая дополнительная информация (например, о времени ремонта), необходимая для определения среднего времени восстановления *MTTR* после обнаружения ошибки диагностикой;

h) любые ограничения на применение элемента подсистемы, которые необходимо рассмотреть для предотвращения систематических отказов;

i) устойчивость к отказам аппаратных средств.

6.7.5 Определение показателей безопасности подсистемы

Показатели безопасности подсистемы характеризуются предельным требованием к УПБ, определяемым ее архитектурными ограничениями (см. 6.7.6), предельным требованием к УПБ для систематической полноты (см. 6.7.9) и вероятностью случайных опасных отказов аппаратных средств (см. 6.7.8).

Примечания

1 Предельное требование к УПБ подсистемы устанавливает предельное значение для максимального уровня полноты безопасности, которое может быть востребовано СБФУ, реализуемой этой подсистемой.

2 Информация обо всех трех аспектах необходима для определения УПБ, который достигается связанной с безопасностью системой управления, реализующей соответствующую СБФУ.

6.7.6 Ограничения архитектуры на полноту безопасности аппаратных средств подсистем

6.7.6.1 Наиболее высокий уровень полноты безопасности аппаратных средств, который может потребоваться для функции безопасности, ограничивается устойчивостью к отказам аппаратных средств и долей безопасных отказов подсистем, которые выполняют эту СБФУ. В таблице 4 определяем наибольший уровень полноты безопасности, который может потребоваться для СБФУ, которую реализует подсистема, с учетом устойчивости к отказам аппаратных средств и доли безопасных отказов этой подсистемы. Ограничения архитектуры, приведенные в таблице 4, должны применяться к каждой подсистеме. В соответствии с этими требованиями:

a) устойчивость к отказам аппаратных средств *N* означает, что отказ *N* + 1 может привести к потере СБФУ. В определении устойчивости к отказам не должны учитываться средства, которые могли бы управлять влиянием ошибок, например диагностики;

b) если одна ошибка непосредственно приводит к одной или более последующим, то ее рассматривают как одиночную ошибку;

c) в определении устойчивости к отказам аппаратных средств некоторые ошибки могут быть исключены при условии, что вероятность их возникновения очень мала по отношению к требованиям полноты безопасности подсистемы. Любые исключения ошибок должны быть обоснованы и документально оформлены (см. 6.7.7).

6.7.6.2 Ограничения архитектуры по таблице 4 должны применяться к каждой подсистеме, реализующей функциональный блок СБФУ.

6.7.6.3 Подсистема, включающая в себя только один элемент, должна удовлетворять требованиям таблицы 4. В частности, если подсистема имеет устойчивость к отказам аппаратных средств, равную нулю (т. е. *N* = 0), то значение ДБО более чем 99% должно быть достигнуто функцией(ями) диагностики СБЭСУ.

Примечание — Это требование, необходимое для обеспечения соответствующего вида архитектурного ограничения, применяется для подсистем, которые включают только один элемент подсистемы, для того, чтобы подтвердить предельное требование к УПБ для УПБ 3.

6.7.6.4 Электромеханические подсистемы, у которых доля безопасных отказов менее 60% и отказоустойчивость технических средств равна нулю, используемые, успешно испытанные (см. примечание) программируемые логические контроллеры, соответствующие ИСО 13849-1, категория 1, должны рассматриваться как достигаемые предельного требования к УПБ, равного УПБ1.

Примечание — Успешно испытанным компонентом для связанного с безопасностью применения является компонент, который или:

a) широко использовался в прошлом с успешными результатами в подобных приложениях,

b) создан и проверен на основе принципов, которые демонстрируют его пригодность и надежность для связанных с безопасностью приложений.

Таблица 4 — Архитектурные ограничения подсистем. Максимальное значение УПБ, которое может быть достигнуто СБФУ, реализуемой этой подсистемой

Доля безопасных отказов	Устойчивость к отказам аппаратных средств (см. примечание 1)		
	$N = 0$	$N = 1$	$N = 2$
< 60 %	Не оговаривается	УПБ1	УПБ 2
60–90 %	УПБ 1	УПБ 2	УПБ 3
90–99 %	УПБ 2	УПБ 3	УПБ 3 (см. примечание 2)
≥ 99 %	УПБ 3	УПБ 3 (см. примечание 2)	УПБ 3 (см. примечание 2)

Примечания

1 Отказоустойчивость аппаратных средств N означает, что $N + 1$ отказ приведет к потере связанной с безопасностью функции управления.

2 УПБ 4 в качестве предельного требования в настоящем стандарте не рассматривается. Об УПБ 4 см. МЭК 61508-1.

3 См. исключение в 6.7.7.

6.7.7 Оценка доли безопасных отказов (ДБО)

6.7.7.1 Для определения предельных требований к УПБ с учетом архитектурных ограничений, где это необходимо, должна быть выполнена оценка ДБО.

6.7.7.2 Для оценки ДБО для каждой подсистемы должен быть проведен анализ (например, анализ дерева отказов, видов и последствий отказов), чтобы определить все соответствующие отказы и их виды. Является ли отказ безопасным или опасным, зависит от СБЭСУ и выполняемых, связанных с безопасностью функций управления, включая функцию реакции на отказ. Вероятность каждого вида отказа должна быть определена на основании вероятности связанного(ых) с ним сбоя(ев) с учетом заданного применения подсистемы и может быть получена из таких источников, как:

a) надежные данные об интенсивности отказов, собранные из практического опыта производителя и связанные с заданным применением;

b) данные об отказе компонента из признанных отраслевых источников и связанные с заданным применением;

c) данные об интенсивности отказов, полученные по результатам тестирования и анализа.

Исключение. Для подсистемы с устойчивостью к сбоям аппаратных средств, равной нулю, в которой исключение сбоя может привести к опасному отказу, предельное требование к УПБ из-за ограничений архитектуры такой подсистемы ограничено максимальным значением УПБ 2.

Примечания

1 Информация о соотношениях видов отказов для электрических / электронных компонентов может быть найдена в нескольких источниках, включая:

MIL-HDBK 217F(Notice 2) Reliability Prediction of Electronic Equipment (28-02-95), Parts Stress Analysis,

MIL-HDBK 217F(Notice 2) Reliability Prediction of Electronic Equipment (28-02-95), Appendix A, Parts Count, Reliability Prediction,

SN 29500 Part 7, Failure Rates of Components, Expected Values for Relays, April 1992,

SN 29500 Part 11, Failure Rates of Components, Expected Values for Contactors, August 1990.

Документы серии SN 29500 общедоступны и могут быть получены от:

- Siemens AG, SI SR CT

Отто-Хэн-Ринг 6

D-81739 München.

UTE C 80-810 RDF 2000: Reliability data handbook — A universal model for reliability prediction of electronic components, PCBs and equipment,

Failure mode/mechanism distributions FMD-91, RAC 1991.

2 Рекомендуется использовать данные об интенсивности отказов и данные о соотношениях видов отказов, полученные от производителей.

3 В некоторых стандартах содержатся соответствующие данные (например, приложение К МЭК 60947-4-1).

4 Если подробный анализ каждого вида отказа практически не возможен, то общепринятым соотношением является: 50% безопасных отказов и 50% опасных отказов.

5 Списки сбоев, которые должны рассматриваться в случае применения механических, пневматических, гидравлических и электрических технологий, даны в приложениях А, В, С и D ИСО 13849-2.

6.7.7.3 Применение исключения сбоя должно быть обосновано (например, путем анализа) и документально оформлено.

Примечание — Исключение сбоев допустимо в соответствии с 3.3 и таблицей D.5 ИСО 13849-2.

6.7.8 Требования к вероятности опасных случайных отказов аппаратных средств подсистем

6.7.8.1 Общие требования

6.7.8.1.1 Вероятности опасного случайного отказа аппаратных средств должна быть меньше или равна целевой мере отказов, определенной в спецификации требований к безопасности подсистемы (см. 6.6.2.1.7).

6.7.8.1.2 Вероятность опасного отказа каждой подсистемы, выполняющей соответствующие функциональные блоки, из-за случайного отказа аппаратных средств должна быть оценена с учетом:

a) архитектуры подсистемы, поскольку она связана с распределением реализуемых функциональных блоков.

Примечание — При этом необходимо решать, существует или не существует устойчивость к отказам аппаратных средств;

b) интенсивности отказов каждого элемента подсистемы любых видов, которые могли бы вызвать опасный отказ подсистемы, но были обнаружены диагностической проверкой (см. 6.3);

c) интенсивности отказов каждого элемента подсистемы любых видов, которые могли бы вызвать опасный отказ подсистемы и не были обнаружены диагностической проверкой (см. 6.3);

d) восприимчивости подсистемы к отказам по общей причине, которые могли бы вызвать опасный отказ подсистемы (см. примечание к настоящему перечислению и примечание 1 к перечислению g).

Примечание — Если для обнаружения сбоев используется сравнение избыточных компонентов, то может произойти отказ средств обнаружения сбоя, когда избыточные компоненты отказывают одновременно с одинаковым видом отказа. Такой отказ может происходить из-за общей причины и называется отказом по общей причине (ООП), который описывается бета-фактором (β).

Упрощенный подход к оценке восприимчивости к отказам по общей причине приведен в 6.7.8.3. Дополнительную информацию по количественной оценке влияния связанных с аппаратными средствами отказами по общей причине см. в МЭК 61508-6, приложение D;

e) охвата диагностическими тестами (см. 3.2.38) и связанного с ним диагностического испытательного интервала;

f) интервалов времени, на которых реализуются контрольные проверки для обнаружения опасных ошибок, не обнаруживаемых диагностическими тестами, и/или заданного срока эксплуатации для элемента(ов) подсистемы, который не должен быть превышен в целях обеспечения подтверждения соответствия информации, представленной в перечислениях b) и c);

g) времени ремонта для обнаруженных отказов, если подсистема спроектирована для выполнения ремонта в неавтономном режиме.

Примечания

1 Максимальное время ремонта составляет часть времени восстановления (см. МЭС 191-10-05 [4]), включающего в себя также время обнаружения отказа и период, в течение которого ремонт невозможен (пример использования среднего времени восстановления для вычисления вероятности отказа приведен в приложении В МЭК 61508-6). Для ситуаций, когда ремонт может быть выполнен в течение конкретного периода времени, например, в то время, когда машина отключена или находится в безопасном состоянии, особенно важно, чтобы при полном расчете был учтен период, когда ремонт не может быть произведен, особенно, когда этот период является относительно большим.

2 Упрощенный подход, который может быть использован для оценки вероятности случайного опасного отказа аппаратных средств подсистем приведен в 6.7.8.2. Доступны другие методы и наиболее подходящий будет зависеть от обстоятельств. Возможные методы моделирования включают в себя:

a) анализ дерева ошибок (см. МЭК 61508-7, B.6.6.5 и МЭК 61025);

b) Марковские модели (см. МЭК 61508-7, B.6.6.6 и МЭК 61165);

c) блок-диаграммы надежности (см. МЭК 61508-7, B.6.6.7 и МЭК 61087).

3 Отказы по общей причине и процессов передачи данных могут быть результатом других влияний, отличных от реальных отказов компонентов аппаратных средств (например, электромагнитных помех, ошибок декодирования и т. п.). См. 6.7.9.

6.7.8.1.3 Для подсистем и их элементов, где вероятность отказа задана в отношении к числу операционных циклов, эти значения должны быть преобразованы в зависимые от времени с использованием заданного рабочего цикла для соответствующих СБФУ (см. 5.2.3).

6.7.8.1.4 Диагностический испытательный интервал любой подсистемы, обладающей величиной устойчивости к отказам аппаратных средств большей нуля, должен быть таким, чтобы подсистема удовлетворяла требованиям к вероятности случайных отказов аппаратных средств (см. 6.3.1).

Примечание — Этот диагностический испытательный интервал должен быть таким, чтобы ошибка обнаруживалась до появления последующей ошибки, способной привести к опасному отказу подсистемы и превысить целевую величину отказов.

6.7.8.1.5 Диагностический испытательный интервал любой подсистемы, обладающей величиной устойчивости к отказам аппаратных средств больше нуля, должен быть таким, чтобы были выполнены требования 6.3.2.

6.7.8.2 Упрощенный подход для оценки вероятности опасных случайных отказов аппаратных средств подсистем

6.7.8.2.1 Общие положения

Данный подпункт описывает упрощенный подход к оценке вероятности опасных случайных отказов аппаратных средств для ряда базовых архитектур подсистем и представляет формулы, которые могут быть использованы для подсистем, собранных либо из элементов низкой сложности, либо из сложных элементов. По существу, эти формулы являются упрощенными выражениями теории анализа надежности и предназначены для выполнения расчетов, связанных с безопасностью. Все формулы, приведенные в настоящем подпункте, справедливы при условии $1 >> \lambda \cdot T_1$, где T_1 — наименьшее из значений интервала между контрольными проверками или срока службы, и для подсистем, работающих в «режиме с высокой частотой запросов или непрерывном режиме» (см. 3.2.27, 6.8.6).

Примечания

1 Полученные результаты представляют собой ограничения на вероятность опасных случайных отказов аппаратных средств подсистем, а где это неприемлемо, можно применять более точные методы моделирования (см. 6.7.8.1.1).

2 Для уравнений (A)–(D), приведенных в 6.7.8.2, интенсивность отказов элементов подсистемы (λ) предполагается постоянной и достаточно низкой ($1 >> \lambda \cdot T$); это означает, что среднее время между опасными отказами должно быть гораздо больше интервала между контрольными проверками или срока службы подсистемы. Поэтому можно использовать следующее основное уравнение:

$\lambda = 1/MTTF$.

Для электромеханических устройств интенсивность отказов определяется с помощью величины B_{10} и числа рабочих циклов C, заданных для применения (см. 5.2.3):

$\lambda = 0{,}1 \cdot C/B_{10}$.

3 Далее используют следующие характеристики:

$\lambda = \lambda_S + \lambda_D$, где λ_S — интенсивность безопасных отказов и λ_D — интенсивность опасных отказов;

$PFH_D = \lambda_D \cdot 1$ ч — средняя вероятность опасных отказов в 1 ч;

T_2 — интервал диагностических проверок;

T_1 — интервал между контрольными проверками или срок службы (в зависимости от того, что меньше).

6.7.8.2.2 Базовая архитектура подсистемы типа А. Устойчивость к отказам равна нулю, без функции диагностики

В данной архитектуре любой опасный отказ элемента подсистемы вызывает отказ СБФУ. Для архитектуры типа А вероятность опасного отказа подсистемы равна сумме вероятностей опасных отказов всех элементов подсистемы:

$$\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{Den} \quad (A)$$

$$PFH_{DssA} = \lambda_{DssA} \cdot 1 \text{ ч.}$$

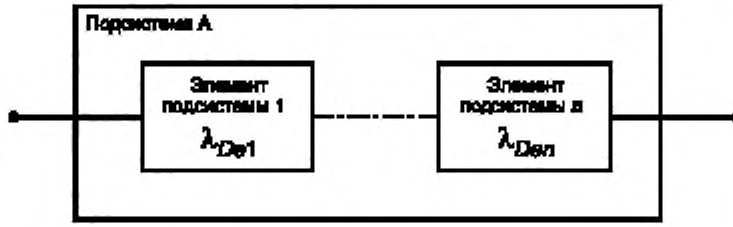


Рисунок 6 — Логическое представление подсистемы типа А

Примечание — На рисунке 6 показано логическое представление архитектуры подсистемы типа А, которое не должно рассматриваться как ее физическая реализация.

6.7.8.2.3 Базовая архитектура подсистемы типа В. Устойчивость к отказам равна единице, без функции диагностики

В данной архитектуре одиночный опасный отказ элемента подсистемы не вызывает отказ СБФУ. Таким образом, должен произойти опасный отказ более чем одного элемента прежде, чем может произойти отказ СБФУ. Для архитектуры типа В вероятность опасного отказа подсистемы равна:

$$\lambda_{DssB} = (1 - \beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2 \quad (B)$$

$$PFH_{DssB} = \lambda_{DssB} \cdot 1 \text{ ч,}$$

где T_1 — интервал между контрольными проверками или срок службы (в зависимости от того, что меньше);

β — восприимчивость к отказам по общей причине.

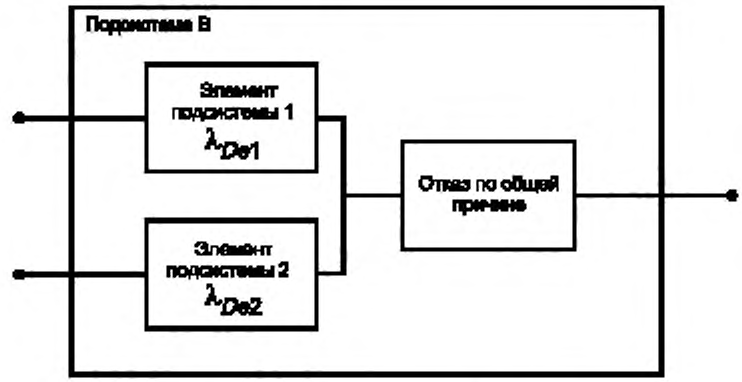


Рисунок 7 — Логическое представление подсистемы типа В

Примечание — На рисунке 7 показано логическое представление архитектуры подсистемы типа В, которое не должно рассматриваться как ее физическая реализация.

6.7.8.2.4 Базовая архитектура подсистемы типа С. Устойчивость к отказам равна нулю, с функцией диагностики

В данной архитектуре любой невыявленный опасный сбой элемента подсистемы приводит к опасному отказу СБФУ. Если выявлен сбой элемента подсистемы, то диагностическая(ие) функция(ии) инициирует(ют) функцию реакции на сбой (см. 6.3.2). Для архитектуры типа С вероятность опасного отказа подсистемы равна:

$$\lambda_{DssC} = \lambda_{De1} (1 - DC_1) + \ldots + \lambda_{Den} (1 - DC_n) \qquad C)$$

$$PFH_{DssC} = \lambda_{DssC} \cdot 1 \text{ ч.}$$

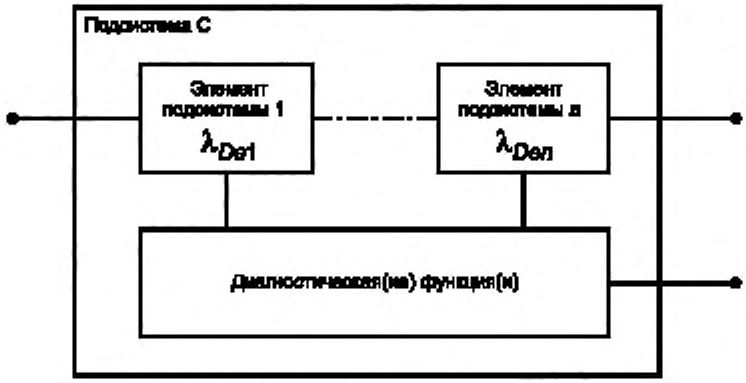


Рисунок 8 — Логическое представление подсистемы типа С

Примечание — На рисунке 8 показано логическое представление архитектуры подсистемы типа С, которое не должно рассматриваться как ее физическая реализация. Показанная функция диагностики может осуществляться:

- диагностируемой подсистемой;
- другими подсистемами СБЭС;
- подсистемами, не участвующими в выполнении связанных с безопасностью функций управления.

6.7.8.2.5 Базовая архитектура подсистемы типа D. Устойчивость к отказам равна единице, без функции(й) диагностики

В данной архитектуре одиночный отказ любого элемента подсистемы не вызывает отказ СБФУ, где

T_2 — интервал диагностических проверок;

T_1 — интервал между контрольными проверками или срок службы (в зависимости от того, что меньше);

β — восприимчивость к отказам по общей причине;

$\lambda_D = \lambda_{DD} + \lambda_{DU}$, где λ_{DD} — интенсивность обнаруженных опасных отказов и λ_{DU} — интенсивность необнаруженных опасных отказов.

$$\lambda_{DD} = \lambda_D \cdot DC$$

$$\lambda_{DU} = \lambda_D \cdot (1 - DC).$$

Для элементов подсистемы различной конструкции:

λ_{De1} — интенсивность опасных отказов 1-го элемента подсистемы;

DC_1 — охват диагностикой 1-го элемента подсистемы;

λ_{De2} — интенсивность опасных отказов 2-го элемента подсистемы;

DC_2 — охват диагностикой 2-го элемента подсистемы.

$$\lambda_{DssD} = (1 - \beta)^2 \{[\lambda_{De1} \cdot \lambda_{De2} \cdot (DC_1 + DC_2)] \cdot T_2/2 + [\lambda_{De1} \cdot \lambda_{De2} \cdot (2 - DC_1 - DC_2)] \cdot T_1/2\} +$$

$$+ \beta \cdot (\lambda_{De1} + \lambda_{De2})/2 \qquad (D.1)$$

$$PFH_{DssD} = \lambda_{DssD} \cdot 1 \text{ ч.}$$

Для элементов подсистемы одинаковой конструкции:
λ_{De} — интенсивность опасных отказов 1-го или 2-го элемента подсистемы;
DC — охват диагностикой 1-го или 2-го элемента подсистемы.

$$\lambda_{DssD} = (1-\beta)^2 \{[\lambda_{De}{}^2 \cdot 2 \cdot DC] \cdot T_2/2 + [\lambda_{De}{}^2 \cdot (1-DC)] \cdot T_1\} + \beta \cdot \lambda_{De}, \quad (D.2)$$

$PFH_{DssD} = \lambda_{DssD} \cdot 1$ ч.

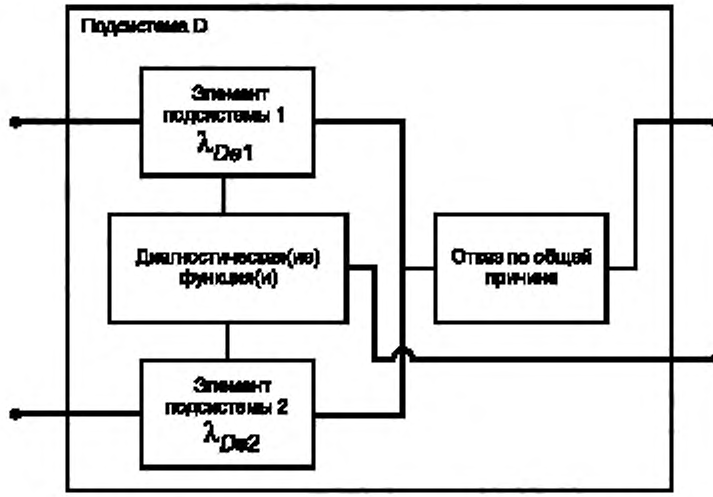


Рисунок 9 — Логическое представление подсистемы типа D

Примечания

1 На рисунке 9 показано логическое представление архитектуры подсистемы типа D, которое не должно рассматриваться как ее физическая реализация. Показанная функция диагностики может быть осуществлена:

- диагностируемой подсистемой;
- другими подсистемами СБЭСУ;
- подсистемами, не участвующими в выполнении связанных с безопасностью функций управления.

2 Предполагается, что реакцией на отказ такой подсистемы является прекращение соответствующей операции согласно требованиям 6.3.1. Если ремонт в неавтономном режиме предусматривается в проекте, в котором реакцией на сбой является сообщение о сбое, но выполнение соответствующей операции не прекращается, то в таком случае для остальной архитектуры должно быть определено новое значение PFH_D для подсистемы после появления первого сбоя.

6.7.8.3 Упрощенный подход для оценки вклада отказов по общей причине (ООП)

6.7.8.3.1 Для оценки вклада отказов по общей причине в вероятность опасных случайных отказов технических средств подсистемы требуются знания о восприимчивости подсистемы к отказам по общей причине (см. 6.7.8.1).

6.7.8.3.2 Если используется избыточная архитектура для достижения требуемой вероятности опасных случайных отказов технических средств подсистемы и отказы по общей причине могут устранить результат этой избыточности, то вероятность опасного случайного отказа технических средств, основанная на вероятности появления общей причины, должна быть добавлена к вероятности опасного случайного отказа технических средств подсистемы, использующей избыточность.

6.7.8.3.3 Вероятность возникновения отказов по общей причине, как правило, зависит от сочетания технологии, архитектуры, применения и окружающей среды. Для эффективного предотвращения многих видов отказов по общей причине необходимо использовать приложение F.

6.7.8.3.4 Приложение F содержит таблицу оценок и соответствующую методологию, которые могут быть использованы для оценки эффективности мер, применяемых при проектировании подсистемы для ограничения ее восприимчивости к отказам по общей причине.

6.7.9 Требования к систематической полноте безопасности подсистем

Если выполнены требования 6.7.9.1 и 6.7.9.2, то предельное требование к УПБ, связанное с систематической полнотой безопасности подсистемы, достигает УПБ 3.

6.7.9.1 Требования к предотвращению систематических отказов

6.7.9.1.1 Должны быть применены следующие меры:

a) выполнять правильный выбор, комбинацию, размещение, сборку и установку компонентов, в том числе кабелей, проводов и любых соединений, применяя указания производителя и используя передовую инженерную практику;

b) использовать понятия «подсистема» и «элементы подсистемы» в спецификации изготовителя и инструкции по установке;

c) обеспечить совместимость, применяя компоненты с совместимыми эксплуатационными характеристиками;

d) обеспечить работоспособность в заданных условиях окружающей среды, разрабатывая подсистему так, чтобы она была способна работать во всех ожидаемых и в любых обозримых предсказуемых условиях, например температуры, влажности, вибрации и электромагнитных помех (см. D.1 ИСО 13849-2);

e) использовать компоненты, которые удовлетворяют требованиям соответствующих стандартов, режимы отказов которых хорошо определены, для снижения риска необнаруженных сбоев путем применения компонент с заданными характеристиками;

f) использовать подходящие материалы и соответствующие производства, выбирая материал, технологию производства и обработку с учетом, например, напряжения, прочности, упругости, трения, износа, коррозии, температуры, проводимости, диэлектрической стойкости;

g) корректировать размеры и формы при анализе влияния, например, напряжения, деформации, усталости, температуры, шероховатости, допусков при изготовлении.

6.7.9.1.2 Кроме того, одна или несколько из следующих мер должны применяться с учетом сложности подсистемы:

a) анализ проекта аппаратных средств (например, проверка или сквозной контроль) для выявления в результате осмотров и/или анализа расхождений между спецификацией и реализацией.

Примечание — Чтобы выявить несоответствия между спецификацией и реализацией, любые точки сомнения или потенциально слабые места реализации, исполнения и использования изделия документально оформляют так, чтобы они могли быть решены; учитывая, что во время процедуры проверки автор пассивен, а инспектор активен, а при процедуре сквозного контроля автор активен, и инспектор пассивен;

b) средства автоматизированного проектирования для моделирования и анализа, систематически выполняющие проектную процедуру и автоматически включающие подходящие уже имеющиеся и проверенные элементы конструкции.

Примечание — Полнота этих средств может быть продемонстрирована с помощью конкретного испытания, наличием достаточной информации о предыдущем удовлетворительном их использовании или независимой проверкой их результатов для конкретной разрабатываемой подсистемы (см. 6.11.3.4);

c) систематически выполняемое моделирование проекта подсистемы для анализа ее эксплуатационных характеристик и корректного определения размеров ее компонентов.

Примечание — Функции подсистемы могут быть смоделированы на компьютере с помощью программного обеспечения, реализующего модель ее поведения (см. 6.11.3.4), где каждый отдельный компонент схемы имеет свою собственную модель поведения. В результате реакция всей подсистемы, содержащей эти компоненты, анализируется для предельных значений характеристик каждого компонента.

6.7.9.2 Требования по управлению систематическими отказами

6.7.9.2.1 Должны быть применены следующие меры:

a) по борьбе с последствиями пробоя изоляции, колебаний и прерываний напряжения, повышенного и пониженного напряжения: реакция поведения подсистемы в условиях пробоя изоляции, колебаний и прерываний напряжения, повышенного и пониженного напряжения должна быть предварительно определена так, чтобы подсистема могла достигать или поддерживать безопасное состояние СБЭСУ.

Примечание — См. также соответствующие требования МЭК 60204-1. В частности:

- повышение напряжения должно быть обнаружено достаточно рано, чтобы все выходы могли быть переключены в безопасное состояние процедурой отключения питания или переключением на второй источник питания;
- должно контролироваться напряжение схемы управления, и если оно оказывается вне указанного для него диапазона, то инициируется отключение питания или выполняется переключение на второй источник питания;
- повышение и понижение напряжения должно быть обнаружено достаточно рано, чтобы внутреннее состояние могло быть (при необходимости) сохранено в энергонезависимой памяти и все выходы могли быть установлены в безопасное состояние процедурой отключения питания или переключением на второй источник питания;

b) по контролю и предотвращению влияния физической среды (например, температуры, влажности, воды, вибрации, пыли, агрессивных веществ, электромагнитных помех и их последствий): реакция поведения подсистемы на воздействие физической среды должна быть предварительно определена так, чтобы СБЭСУ могла достигать или поддерживать безопасное состояние машины (см. также МЭК 60204-1);

c) по контролю и предотвращению влияния повышения или снижения температуры, если изменение температуры может произойти: подсистема должна быть спроектирована так, чтобы, например, перегрев мог быть обнаружен до того, как подсистема начнет работать при температурах вне диапазона, заданного спецификацией.

Примечание — Более подробно см. в А.10 МЭК 61508-7.

6.7.9.2.2 Кроме того, для управления систематическими отказами при необходимости должны применяться следующие меры:

- выявление отказов при выполнении контроля в неавтономном режиме;
- тестирование, основанное на сравнении избыточных аппаратных средств;
- использование разнообразных аппаратных средств;
- работа в позитивном режиме (например, концевой выключатель нажат, когда защита открыта);
- ориентированность на режим отказа;
- использование аппаратных средств с увеличенными номинальными значениями параметров на соответствующий коэффициент, если производитель может показать, что снижение их номинальных значений улучшает надежность.

Примечания

1 Если увеличение значений необходимо, то величина коэффициента по крайней мере должна быть равна 1,5.

2 Более подробную информацию можно найти в D.3 ИСО 13849-2.

6.7.10 Формирование подсистемы

Элементы подсистемы должны быть объединены, чтобы сформировать подсистему в соответствии с 6.7.4.3.1.2 и подробную документацию проекта.

6.8 Реализация функций диагностики

6.8.1 Каждая подсистема должна быть обеспечена связанными с ней функциями диагностики, которые необходимы для выполнения требований к архитектурным ограничениям (см. 6.7.6) и к вероятности опасных случайных отказов технических средств (см. 6.7.8).

6.8.2 Функции диагностики рассматриваются как отдельные, которые могут иметь отличную от СБФУ структуру и могут выполняться:

- самой подсистемой, требующей диагностики;
- другими подсистемами СБЭСУ;
- подсистемами СБЭСУ, не выполняющими СБФУ.

Примечание — См. также примечание 3 к 6.6.2.1.1.

6.8.3 Функции диагностики должны удовлетворять следующим, применимым к связанным с ними СБФУ требованиям:

- по предотвращению систематических отказов (см. 6.7.9.1);
- управлению систематическими отказами (см. 6.7.9.2).

6.8.4 Вероятность отказа функции(й) диагностики СБЭСУ должна быть учтена при оценке вероятности опасного отказа СБФУ.

Примечания

1 См. также примечание 3 к 6.6.2.1.1.

2 Временные ограничения, применяемые к тестированию подсистемы, выполняющей функции диагностики, могут отличаться от тех, которые применяются к СБФУ, и в общем случае интервал тестирования должен соответствовать требованиям, применяемым к подсистеме с устойчивостью к отказам аппаратных средств равной 1.

3 Должен быть обнаружен отказ функции(й) диагностики, и должны быть выполнены соответствующие действия для уверенности в том, что вклад функции диагностики в полноту безопасности СБФУ остался тем же. Отказ функции(й) диагностики может быть обнаружен тестированием в неавтономном режиме, перекрестной проверкой избыточных аппаратных средств и т.д.

6.8.5 Должно быть предоставлено ясное описание функции(й) диагностики СБЭСУ, их способности обнаружить отказ или их реакции на отказ, а также выполнен анализ их вклада в полноту безопасности соответствующих СБФУ.

6.8.6 Для выполнения упрощенного подхода при оценке вероятности случайных опасных отказов технических средств подсистем (см.6.7.8.2) применяется следующее:

- если для достижения требуемой вероятности опасного случайного отказа технических средств необходима функция(и) диагностики СБЭСУ и подсистема обладает устойчивостью к сбоям аппаратных средств больше нуля, то обнаружение сбоя и заданная реакция на сбой должны быть выполнены до наступления опасной ситуации из-за этого сбоя;
- при реализации функции(й) диагностики СБЭСУ должно быть как минимум принято, что вероятность случайного отказа технических средств и систематическая полнота безопасности одинаковы и равны значению, заданному для соответствующей(их) СБФУ;

Примечание — Ограничения архитектуры на полноту безопасности аппаратных средств не применяются при реализации функции(й) диагностики;

- если значение вероятности опасного случайного отказа технических средств на порядок больше, чем задано для СБФУ, то должна быть выполнена проверка, чтобы определить, будет ли работоспособна функция(и) диагностики или диагностирующие устройства. Предполагается, что такая проверка должна быть выполнена как минимум 10 раз в промежутке между контрольными проверками подсистемы.

Примечания

1 Проверка функции(й) диагностики должна, насколько это практически возможно, охватывать на 100 % те компоненты, которые реализуют функцию(и) диагностики.

2 Если функция диагностики реализуется логическим устройством СБЭСУ, то нет необходимости отдельно выполнять ее тестирование функции, так как ее отказ может быть обнаружен как отказ СБФУ.

3 Проверка может быть выполнена либо внешними средствами (например, с помощью испытательного оборудования), либо при помощи внутренних динамических проверок (например, встроенных в логическое устройство) СБЭСУ.

6.9 Реализация технических средств СБЭСУ

Необходимо, чтобы СБЭСУ была реализована в соответствии с проектной документацией на СБЭСУ.

6.9.1 Межсоединения в СБЭСУ

6.9.1.1 Межсоединения в СБЭСУ должны быть реализованы так, чтобы удовлетворять соответствующим частям спецификации требований к безопасности СБЭСУ, а также требованиям, относящимся к применению проводников, кабелей, проводов, представленным в МЭК 60204-1.

6.9.1.2 Меры по предотвращению и контролю отказов в соединительных проводах и кабелях должны быть реализованы в соответствии с 6.4.1 и 6.4.2.

6.10 Спецификация требований к безопасности программного обеспечения

6.10.1 Общие положения

Если программное обеспечение должно использоваться в какой-либо части СБЭСУ, реализующей СБФУ, то необходимо разработать и документально оформить спецификацию требований к безопасности программного обеспечения.

6.10.2 Требования

6.10.2.1 Спецификация требований к безопасности программного обеспечения должна быть разработана для каждой подсистемы на основе спецификации и архитектуры СБЭСУ.

6.10.2.2 Спецификация требований к безопасности программного обеспечения для каждой подсистемы должна быть получена из (1) требований к безопасности, заданных для СБФУ, (2) требований, вытекающих из архитектуры СБЭСУ, и (3) любых требований к планированию функциональной безопасности (см. 4.2). Эта информация должна быть доступна для разработчика прикладного программного обеспечения.

6.10.2.3 Спецификация требований к безопасности прикладного программного обеспечения должна быть достаточно подробной для того, чтобы обеспечить выполнение стадий проектирования и внедрения СБЭСУ для достижения требуемой полноты безопасности и позволить выполнить верификацию.

6.10.2.4 Разработчик прикладного программного обеспечения должен просмотреть информацию, содержащуюся в спецификации для того, чтобы гарантировать, что требования определены адекватным образом. В частности, разработчик программного обеспечения должен в соответствии с настоящим стандартом учесть следующее:

- связанные с безопасностью функции управления;
- конфигурацию или архитектуру системы;

- производительность и время отклика;
- интерфейсы оборудования и оператора;
- все соответствующие режимы работы машины, как указано в спецификации требований к безопасности;
- диагностические тесты внешних устройств (например, датчиков и исполнительных элементов).

6.10.2.5 Заданные для безопасности программного обеспечения требования должны быть выражены и структурированы так, чтобы они:

- были ясными, пригодными для верификации, тестирования, поддержки и выполнения и соразмерными с уровнем полноты безопасности;
- были пригодными для того, чтобы можно было определить их источник в спецификации требований к безопасности СБЭСУ;
- не содержали информации и описаний, которые являются двусмысленными.

6.10.2.6 Спецификация требований к безопасности программного обеспечения должна выражать необходимые характеристики каждой подсистемы, предоставляя информацию, позволяющую выполнить соответствующий требованиям выбор оборудования. Должны быть определены следующие требования для программируемых СБФУ:

- логика (т. е. функциональность) всех функциональных блоков, выполняемых каждой подсистемой;
- входные и выходные интерфейсы, предназначенные для каждого функционального блока;
- формат и диапазоны значений входящих и исходящих данных и их связь с функциональными блоками;
- соответствующие данные, описывающие любые ограничения каждого функционального блока, например, максимальное время отклика, предельные значения для проверки достоверности;
- функции, которые позволяют машине достигать или поддерживать безопасное состояние;
- функции, связанные с обнаружением, оповещением и обработкой ошибок;
- функции, связанные с периодическим тестированием СБФУ в автономном и неавтономном режимах;
- функции, предотвращающие несанкционированные изменения в СБЭСУ;
- интерфейсы функций, не связанных с безопасностью;
- производительность и время отклика.

Примечание — Интерфейсы включают в себя средства программирования как в автономном, так и в неавтономном режиме.

6.10.2.7 В случае необходимости в документации должны использоваться полуформальные методы, такие как логика, метод функциональных блоков или последовательностных диаграмм.

Примечание — Руководящие указания по документированию программного обеспечения даны в МЭК 61506, ИСО/МЭК 15910 и ИСО/МЭК 9254.

6.11 Проектирование и разработка программного обеспечения

6.11.1 Проектирование и разработка встроенного программного обеспечения

Встроенное программное обеспечение, включенное в подсистемы, должно соответствовать МЭК 61508-3 и требуемому УПБ.

Примечания

1 См. также 6.7.3.2.

2 В приложении С рассматривается проектирование и разработка встроенного программного обеспечения, используемого для реализации СБФУ для СБЭСУ.

6.11.2 Программное обеспечение, основанное на параметризации

6.11.2.1 В программном обеспечении, основанном на параметризации, связанные с безопасностью параметры должны рассматриваться как связанные с безопасностью аспекты проектирования СБЭСУ, которые описаны в спецификации требований к безопасности программного обеспечения (см. 6.10). Параметризация должна выполняться с помощью специального инструментального средства, предоставляемого поставщиком СБЭСУ либо связанного с подсистемой(ами). Это инструментальное средство имеет свою идентификацию (название, версия и т. д.). Оно должно предотвратить несанкционированную модификацию, например, с помощью пароля.

6.11.2.2 Должна поддерживаться полнота всех данных, используемых для параметризации. Это нужно достичь путем применения мер по управлению:

- диапазоном допустимых входных данных;
- поврежденными данными перед передачей;
- последствиями ошибок в процессе передачи параметров;
- последствиями неполной передачи параметров;
- последствиями сбоев и отказов технических средств и программного обеспечения в инструментальных средствах, используемых для параметризации.

6.11.2.3 Необходимо, чтобы инструментальное средство, используемое для параметризации, отвечало:

- всем соответствующим требованиям к подсистеме в соответствии с настоящим стандартом для обеспечения корректной параметризации;
- использовалась специальная процедура для установки связанных с безопасностью параметров. Эта процедура должна включать подтверждение:
- входных параметров для СБЭСУ путем повторной передачи измененных параметров в инструментальное средство параметризации либо применением других средств, подтверждающих полноту параметров,
- результата (например, соответственно подготовленным специалистом и автоматической проверкой инструментальным средством параметризации).

Примечание — Это особенно важно, если параметризация осуществляется с помощью устройства, специально не предназначенного для этой цели (например, персонального компьютера или аналогичного устройства);

- использование для предотвращения систематических отказов разнообразия в функции(ях) модулей программного обеспечения, предназначенных для кодирования или декодирования в процессе приема/передачи, и модулей программного обеспечения, предназначенных для визуализации пользователю связанных с безопасностью параметров.

6.11.2.4 В документации на программное обеспечение на основе параметризации должны указываться используемые данные (например, предварительно определенные наборы параметров), а также информация, необходимая для идентификации параметров, связанных с СБЭСУ, о лице(ах), осуществляющем(их) параметризацию вместе с другой соответствующей информацией, такой как дата параметризации.

6.11.2.5 Должны применяться следующие действия по верификации для программного обеспечения на основе параметризации:

- верификация правильности установки для каждого связанного с безопасностью параметра (минимальное, максимальное и репрезентативные значения);
- верификация того, что связанные с безопасностью параметры проверяются на достоверность, например, путем обнаружения недопустимых значений и т. д.;
- верификация того, что несанкционированные изменения связанных с безопасностью параметров невозможна;
- верификация того, что данные/сигналы для параметризации создаются и обрабатываются таким образом, что сбои не могут привести к потере СБФУ.

Примечание — Это особенно важно, если параметризация осуществляется с помощью устройства, специально не предназначенного для этой цели (например, персонального компьютера или аналогичного устройства).

6.11.3 Проектирование и разработка прикладного программного обеспечения

Примечание — Содержание данного пункта основано на МЭК 61508-3.

6.11.3.1 Общие требования

6.11.3.1.1 Требования МЭК 61508-3 распространяются на языки с полной изменчивостью. Следующие требования должны применяться к программному обеспечению применений, реализованных на языках с ограниченной изменчивостью.

6.11.3.1.2 Результаты действий, осуществляемых в процессе разработки программного обеспечения применения, должны быть проверены на соответствующих стадиях.

6.11.3.1.3 В соответствии с требуемым уровнем полноты безопасности для СБФУ выбранные метод проектирования и прикладной язык должны обладать соответствующими применению характеристиками, которые упрощают:

а) абстракцию, разделение на модули и другие характеристики, контролирующие уровень сложности; где это возможно, программное обеспечение должно быть основано на хорошо зарекомендовавших

себя логических функциях, которые могут подключать функции пользовательских библиотек и четко определенные правила для связи логических функций;

b) выражение:

- выполняемых функций, в идеале как логическое описание или в виде алгоритмических функций,
- обмена данными между компонентами модуля,
- требований, относящихся к последовательности и времени выполнения,
- ограничений синхронизации,
- структур данных, их свойств, включая типы и обоснованность диапазонов значений;

c) понимание разработчиками и другими лицами, которые должны иметь дело с проектом, как функциональности применения, так и ограничений технологии СБЭСУ;

d) верификацию и подтверждение соответствия, в том числе структурное тестирование (белый ящик) прикладного программного обеспечения, функциональное тестирование (черный ящик) интегрированной прикладной программы и тестирование интерфейсов (серый ящик) взаимодействия с СБЭСУ и ее конкретной конфигурации технических средств;

e) безопасную модификацию.

6.11.3.1.4 Тестирование должно быть основным методом верификации для прикладного программного обеспечения. Планирование тестирования должно охватывать следующие аспекты:

- политику верификации интеграции программного и аппаратного обеспечения и технических средств;
- тестовые примеры и результаты тестирования;
- типы испытаний, которые должны быть выполнены;
- испытательное оборудование, включая инструменты, поддержку программного обеспечения и описание конфигурации;
- критерии тестов, по которым будет оцениваться завершение испытания;
- территориальное расположение (например, завод или площадка потребителя);
- зависимость от внешней функциональности;
- число необходимых тестов;
- полноту связанных функций или требований.

6.11.3.1.5 Если прикладное программное обеспечение должно реализовать функции управления как относящиеся, так и не относящиеся к безопасности, то оно в целом должно рассматриваться как относящееся к безопасности, если только в проекте не продемонстрирована достаточная независимость между этими функциями.

6.11.3.1.6 Проект должен включать проверку полноты данных и обоснованность проверки на уровне применений (например, проверки в каналах связи, проверки граничных значений на входах датчиков, граничных значений параметров данных).

6.11.3.1.7 Разработка прикладного программного обеспечения включает самоконтроль потока управления и потока данных, если эти функции не включены во встроенное программное обеспечение. В случае выявления несоответствия должны быть выполнены соответствующие меры, чтобы достичь или поддерживать безопасное состояние.

6.11.3.1.8 Если в проекте частично должно использоваться ранее разработанное программное обеспечение, то должна быть обоснована его способность удовлетворять спецификации требований к безопасности программного обеспечения. Эта способность должна основываться на данных по удовлетворительной работе в схожих применениях, для которых была продемонстрирована аналогичная функциональность, или быть предметом тех же самых процедур верификации и подтверждения соответствия, которые подразумеваются для любого вновь разрабатываемого программного обеспечения, связанного с безопасностью. Следует оценить ограничения, связанные с окружением программного обеспечения (например, зависимость от операционной системы и компилятора).

6.11.3.1.9 Любые модификации или изменения прикладного программного обеспечения подлежат анализу, который должен выявить все затронутые изменениями программные модули и определить необходимые действия для повторной верификации, чтобы подтвердить, что программное обеспечение по-прежнему удовлетворяет спецификации требований к безопасности.

6.11.3.2 Управление конфигурацией программного обеспечения

6.11.3.2.1 План функциональной безопасности должен определять стратегию разработки, интеграции, верификации и подтверждения соответствия программного обеспечения.

6.11.3.2.2 Управление конфигурацией программного обеспечения должно:

- обеспечивать выполнение всех необходимых операций и продемонстрировать, что требуемая полнота безопасности программного обеспечения была достигнута,

- поддерживать аккуратно и с уникальной идентификацией все документы, относящиеся к объектам конфигурации, необходимым для поддержания полноты СБЭСУ. Объекты конфигурации должны включать, по крайней мере, следующее:
  - анализ безопасности и требований к ней,
  - спецификацию программного обеспечения и проектную документацию,
  - модули программного обеспечения в исходных кодах,
  - планы и результаты тестирования,
  - уже существующие программные модули и пакеты, которые должны быть включены в СБЭСУ,
  - все инструментальные средства и среды разработки, которые используются для создания, тестирования или выполнения любых действий по применению программного обеспечения,
- применять процедуры контроля изменений :
  - для предотвращения несанкционированных изменений,
  - запросов на изменение документов,
  - анализа влияния предлагаемых изменений, а также для того, чтобы принять или отклонить запрос(ы),
  - подготовки документа, подробно описывающего и разрешающего все принятые изменения,
  - документирования конфигурации программного обеспечения в соответствующих точках при разработке программного обеспечения,
- документально оформить следующую информацию, чтобы позволить последующий аудит: статус релиза, обоснование и согласование всех модификаций, а также подробную информацию о модификации,
- официально зарегистрировать выпуск прикладного программного обеспечения. Мастер-копии программного обеспечения и вся связанная с ним документация должны храниться, чтобы обеспечить обслуживание и модификацию в течение всего срока эксплуатации выпущенного программного обеспечения.

6.11.3.3 Требования к архитектуре программного обеспечения

Примечания

1 Архитектура программного обеспечения определяет основные элементы и подсистемы системы и прикладного программного обеспечения, их взаимосвязь, и как достигаются требуемые характеристики. Примерами модулей прикладного программного обеспечения являются прикладные функции, которые реплицируются по всей машине, ввод/вывод машины, переопределение и запрет выполнения компонентов, проверка достоверности данных и диапазонов их значений и т. д.

2 Архитектура программного обеспечения также зависит от базовой архитектуры подсистемы, предоставляемой поставщиком.

6.11.3.3.1 Проект архитектуры программного обеспечения должен быть основан на заданной спецификации обеспечения безопасности СБЭСУ в рамках ограничений системной архитектуры проекта СБЭСУ и подсистемы.

6.11.3.3.2 Проект архитектуры программного обеспечения должен:

a) обеспечить полное описание внутренней структуры и функционирования СБЭСУ и его компонентов (см. примечание);

b) включать спецификации всех идентифицируемых компонентов программного обеспечения, а также описание связей и взаимодействия между этими компонентами (программного обеспечения и аппаратных средств);

c) включать внутренний проект и архитектуру всех идентифицированных компонентов, которые не являются «черными ящиками»;

d) определить модули программного обеспечения, входящие в СБЭСУ, но не использующиеся в каком-либо связанном с безопасностью режиме эксплуатации.

Примечание — Особенно важно, чтобы документация на архитектуру СБЭСУ была актуальной и полной.

6.11.3.3.3 Для того чтобы удовлетворить спецификации, должен быть описан и обоснован набор методов и мер, необходимых для проектирования прикладного программного обеспечения. Эти методы и меры должны быть направлены на обеспечение предсказуемости поведения СБЭСУ и согласовываться с любыми ограничениями, указанными в документации СБЭСУ.

6.11.3.3.4 Должны быть описаны и обоснованы меры, используемые для сохранения полноты всех данных. Такими данными могут быть данные входные/выходные, коммуникационные, операционные данные интерфейса, технического обслуживания и содержание базы данных.

6.11.3.4 Требования к инструментальным средствам поддержки, руководству пользователя и языкам программирования

6.11.3.4.1 Должен быть выбран подходящий набор инструментальных средств, в том числе по управлению конфигурациями, моделированию и тестированию. Следует учитывать способность инструментальных средств (необязательно тех, которые использовались при первоначальной разработке системы) выполнять необходимые задачи на протяжении всего срока жизни СБЭСУ. Такую способность необходимо объяснить и документально оформить.

Примечание — Выбор средства разработки зависит от характера деятельности при разработке программного обеспечения, встроенного программного обеспечения и архитектуры программного обеспечения. Могут быть необходимы верификация и подтверждение соответствия инструментальных средств, таких как анализаторы кода, а также средства моделирования.

6.11.3.4.2 В случае необходимости должно быть определено подмножество прикладного языка программирования.

6.11.3.4.3 Прикладное программное обеспечение должно быть спроектировано с учетом ограничений и известных недостатков, включенных в руководство пользователя СБЭСУ и подсистем.

6.11.3.4.4 Выбранный прикладной язык должен либо обладать следующим:

- иметь транслятор/компилятор, который должен быть оценен для установления его пригодности;
- быть полностью и однозначно определенным либо ограниченным до подмножества однозначно определяемых элементов;
- соответствовать характеристикам применения.

Примечание — К характеристикам применения, например, относятся любые ограничения рабочих характеристик;

- обладать свойствами, облегчающими обнаружение ошибок программирования;
- поддерживать характеристики, соответствующие методу проектирования,

либо недостатки языка должны быть документально оформлены в описании проекта архитектуры программного обеспечения и должна быть разъяснена пригодность языка для конкретной цели, включая дополнительные меры, необходимые для устранения выявленных недостатков языка.

6.11.3.4.5 Процедуры использования прикладного языка должны задавать хорошую практику конфигурирования, запрещать небезопасные возможности программного обеспечения (например, неопределенные особенности языка, неструктурированные конструкции и т. д.), определять проверки, которые могут быть использованы для обнаружения ошибок в конфигурации и указывать процедуры документирования прикладных программ. Документация, относящаяся к прикладной программе, должна содержать по меньшей мере следующую информацию:

a) юридическое лицо (например, компании, автор(ы), и т. д.);
b) описание;
c) отслеживание функциональных требований применения;
d) отслеживание стандартных функций библиотеки;
e) входные и выходные данные;
f) историю изменения конфигурации.

6.11.3.5 Требования к проектированию прикладного программного обеспечения

6.11.3.5.1 До начала детального проектирования прикладного программного обеспечения должна быть доступна следующая информация:

- спецификация требований к безопасности программного обеспечения;
- описание проекта архитектуры программного обеспечения, включая определение логики применения и функций, реализующих устойчивость к сбоям, список входных и выходных данных, общеиспользуемые программные модули и инструментальные средства поддержки, а также процедуры конфигурирования прикладного программного обеспечения с доступными документами, чтобы обеспечить функциональность применения для определенных входных/выходных данных;
- план подтверждения соответствия безопасности программного обеспечения.

6.11.3.5.2 При разработке прикладного программного обеспечения должен применяться структурированный подход с целью обеспечения:

- модульной функциональности применения и данных, управляющих вводом/выводом;
- тестируемости функциональности (в том числе устойчивости к отказам) и внутренней структуры;
- возможности безопасной модификации с использованием адекватной прослеживаемости и объяснений функций применения и связанных с ними ограничений.

6.11.3.5.3 Дальнейшее уточнение проекта для каждого основного компонента/подсистемы в описании проекта архитектуры прикладного программного обеспечения (см. 6.11.3.5.1) должно учитывать:

- повторно использующиеся функции в проекте;
- отображение входной/выходной информации модулей прикладного программного обеспечения;
- реализацию прикладных функций с использованием общих функций программного обеспечения и отображений входа/выхода.

6.11.3.5.4 Необходимо определить проект каждого прикладного программного модуля и проверки структуры, которые должны выполняться для каждого прикладного программного модуля.

6.11.3.5.5 Должны быть определены соответствующие проверки интеграции программного обеспечения и СБЭСУ, гарантирующие, что прикладная программа удовлетворяет заданным требованиям к безопасности прикладного программного обеспечения. Необходимо рассмотреть следующее:

- разделение программного обеспечения на контролируемые интегрируемые подмножества;
- контрольные примеры;
- типы выполняемых проверок;
- условия тестирования, используемые инструменты, конфигурацию и программы;
- условия, при которых проверка считается выполненной;
- процедуры, которые необходимо выполнить, если проверка дала отрицательный результат.

6.11.3.6 Требования к реализации исходных текстов прикладных программ

6.11.3.6.1 Прикладное программное обеспечение должно:

- быть читаемым, понятным и пригодным к проверке;
- удовлетворять всем принципам проектирования;
- удовлетворять всем требованиям, определенным при планировании безопасности.

6.11.3.6.2 Прикладное программное обеспечение должно быть просмотрено, чтобы обеспечить соответствие специфицированному проекту, правилам кодирования и требованиям к планированию безопасности.

Примечание — Обзор прикладного программного обеспечения включает в себя такие методы, как проверка программного обеспечения или сквозной контроль, анализ кода или формальное доказательство. Эти методы должны быть использованы в сочетании с тестированием и/или моделированием, чтобы обеспечить уверенность в том, что прикладное программное обеспечение удовлетворяет связанной с ним спецификации.

6.11.3.7 Требования к тестированию программных модулей

Примечание — Процесс проверки того, что прикладное программное обеспечение корректно выполняет все требования, содержащиеся в спецификации тестирования, относится к процессам верификации. Сочетание просмотра исходных текстов и структурного тестирования программных модулей дает гарантию того, что программный модуль удовлетворяет требованиям своей спецификации, т. е. модуль верифицируется.

6.11.3.7.1 Необходимо проверить каждую конфигурацию входов и выходов в процессе анализа, тестирования или моделирования для подтверждения того, что входные/выходные данные сопоставляются с правильной логикой применения.

6.11.3.7.2 В процессе анализа, моделирования и тестирования нужно проверить каждый программный модуль, чтобы определить, что он выполняет функции, для которых предназначен, и не выполняет функции, которые не были для него предусмотрены.

6.11.3.7.3 Тесты должны соответствовать конкретному тестируемому модулю и должны обеспечить:

- проверку каждой ветви всех модулей прикладного программного обеспечения;
- проверку для граничных данных;
- корректное выполнение последовательности действий, с учетом соответствующих требований синхронизации.

6.11.3.7.4 Результаты тестирования программных модулей должны быть документально оформлены.

6.11.3.7.5 Если программное обеспечение уже было оценено или имеется информация о значительном положительном опыте его эксплуатации, то количество испытаний можно сократить.

6.11.3.8 Требования к тестированию интеграции прикладного программного обеспечения

Примечание — Процесс проверки того, что интеграция программного обеспечения является корректной, относится к процессам верификации.

6.11.3.8.1 Прикладное программное обеспечение должно быть проверено, чтобы убедиться, что все модули прикладного программного обеспечения и компоненты/подсистемы корректно взаимодействуют

друг с другом и со встроенным программным обеспечением для выполнения функций, для которых они предназначены, и не выполняют непредусмотренных функций, которые могли бы угрожать любой функции безопасности.

6.11.3.8.2 Результаты проверки интеграции прикладного программного обеспечения необходимо документально оформить, в них следует сформулировать:

- результаты проверки;
- были ли выполнены цели и критерии проверки.

6.11.3.8.3 Если тестирование окончилось неудачно, то причины неудачи и предпринятые корректирующие действия должны быть включены в документацию по результатам испытаний.

6.11.3.8.4 При интеграции прикладного программного обеспечения все модификации или изменения программного обеспечения должны быть объектом анализа влияния на безопасность, который должен определить:

- все программные модули, затрагиваемые изменениями;
- все необходимые действия для повторных верификации и проектирования.

6.12 Интеграция и тестирование СБЭСУ

Примечание — Интеграция СБЭСУ обычно проводится до установки, но в некоторых случаях интеграция СБЭСУ не может быть осуществлена до окончания установки (например, если разработка прикладного программного обеспечения не завершена).

6.12.1 Общие требования

6.12.1.1 СБЭСУ должна быть интегрирована в соответствии с конкретным проектом СБЭСУ. В рамках интеграции все подсистемы и элементы подсистем СБЭСУ, СБЭСУ должны быть испытаны в соответствии с конкретными тестами интеграции. Эти испытания должны показать, что все модули взаимодействуют правильно для выполнения функций, для которых они предназначены и не выполняют непредусмотренных функций.

6.12.1.2 Интеграция связанного с безопасностью программного обеспечения в СБЭСУ включает тесты, которые определяются на стадии проектирования и разработки, для обеспечения совместимости программного обеспечения с аппаратными средствами и встроенной платформой программного обеспечения так, чтобы были выполнены функциональные требования и требования безопасности.

Примечания

1. Тестирование всех входных комбинаций не проводится. Считается достаточным тестирование всех классов эквивалентности (см. В.5 и С.5.7 МЭК 61508-7). Статический анализ, динамический анализ или анализ отказов могут сократить число испытаний до приемлемого уровня. Использование структурного проектирования или полуформальных методов упрощает выполнение тестирования и верификации.

2 Использование структурного проектирования или полуформальных методов может позволить уменьшить глубину и количество тестов.

3 Статистические данные также могут быть использованы для уменьшения глубины и количества тестов.

6.12.1.3 Для тестирования интеграции СБЭСУ должна быть разработана соответствующая документация, устанавливающая результаты испытаний и определяющая достигнуты ли цели и критерии, определенные на стадиях проектирования и создания систем. В случае отказа должны быть документально оформлены его причины, выполнены действия по его корректировке и повторное тестирование.

6.12.1.4 В период интеграции и испытаний любые модификации или изменения СБЭСУ должны стать предметом анализа, при котором следует идентифицировать все компоненты, на которые влияют эти модификации или изменения, и дополнительных проверок.

6.12.1.5 При испытаниях интеграции СБЭСУ должна быть документально оформлена следующая информация:

a) версия спецификации испытаний;

b) критерии принятия испытаний интеграции;

c) версия испытуемой СБЭСУ;

d) используемые средства испытаний и оборудование с датой поверки;

e) результаты каждого испытания;

f) любое несоответствие между ожидаемыми и фактическими результатами;

g) проведенный анализ и принятое решение о продолжении испытаний или выпуске запроса на изменение (при наличии несоответствия).

6.12.2 Тесты, определяющие систематическую полноту безопасности в процессе интеграции СБЭСУ

6.12.2.1 Для того чтобы выявить неисправности и избежать сбоев в процессе интеграции прикладного программного обеспечения и аппаратных средств применяется тестирование. В ходе испытаний должен быть выполнен анализ, чтобы убедиться, что заданные характеристики СБЭСУ были достигнуты.

6.12.2.2 Должны быть выполнены следующие испытания:

a) функциональные тесты, в которых для СБЭСУ используются данные, адекватно характеризующие операции. Выходные данные тестов сравниваются с приведенными в спецификации. Отклонения от спецификации и указания о неполной ее проверке должны быть документально оформлены;

b) динамические испытания для проверки динамического поведения в реальных условиях функционирования и выявления отказов в соответствии с функциональной спецификацией СБЭСУ, а также для оценки полезности и надежности СБЭСУ.

Примечание — Функции системы или программы выполняются в конкретном окружении с конкретными тестовыми данными, которые были получены систематически из спецификации требований к безопасности СБЭСУ в соответствии с установленными критериями. Полученное поведение СБЭСУ сравнивается со спецификацией. Цель состоит в том, чтобы определить, правильно ли СБЭСУ и/или ее подсистемы выполняют все функции, заданные в спецификации. Методика формирования классов эквивалентности является одним из подходов формирования тестовых данных при тестировании методом «черного ящика». Пространство входных данных разделяется на конкретные диапазоны входных значений (классов эквивалентности) с помощью спецификации. Затем формируются тестовые примеры:

- из данных из допустимых диапазонов;
- данных из недопустимых диапазонов;
- данных из предельных значений диапазонов;
- экстремальных значений;
- комбинаций из вышеперечисленных классов.

Для выбора тестовых примеров в различных испытаниях (тестирование модуля, тестирование интеграции и тестирование системы) могут быть эффективны другие подходы.

6.13 Установка СБЭСУ

6.13.1 Целью требований данного подраздела является установка СБЭСУ, чтобы убедиться, что СБЭСУ подходит для использования по назначению и готова к подтверждению соответствия.

6.13.2 Требования

6.13.2.1 СБЭСУ должна быть установлена в соответствии с планом функциональной безопасности для окончательного подтверждения соответствия системы (см. перечисление h) 4.2.1).

6.13.2.2 Должны быть произведены соответствующие записи об установке СБЭСУ, а также все результаты испытаний. В случае отказа СБЭСУ его причины должны быть зарегистрированы.

7 Информация по применению СБЭСУ

7.1 Цель

СБЭСУ должна быть обеспечена информацией, позволяющей пользователю разрабатывать такие процедуры, которые гарантируют, что требуемая функциональная безопасность СБЭСУ поддерживается во время эксплуатации и технического обслуживания машины.

7.2 Документация по установке, эксплуатации и техническому обслуживанию

Примечания

1 См. также раздел 6 ИСО 12100-2, предоставляющий общую информацию, которую следует учитывать при составлении сопроводительных документов.

2 Один или несколько элементов документации, описанной в данном подразделе, были разработаны, чтобы охватить по возможности другие аспекты настоящего стандарта.

Документация должна предоставлять информацию по установке, использованию и техническому обслуживанию СБЭСУ. Она должно включать:

a) полное описание оборудования, установки и монтажа;

b) отчет о предполагаемом использовании СБЭСУ и любые меры, которые могут быть необходимы для предотвращения разумно предсказуемого неправильного использования;

c) сведения о физической среде (например, освещение, вибрация, уровни шума, атмосферные загрязнения) в случае необходимости;

d) обзор (блок) схем в случае необходимости;

e) принципиальные схемы;

f) интервал контрольных проверок или срок жизни;

g) описание (включая диаграммы взаимосвязей) взаимодействия (если таковые имеются) между функцией(ями) СБЭСУ и функцией(ями) электрической системы управления машины;

h) описание необходимых мер, гарантирующих разделение функций СБЭСУ и электрической системы управления машины;

i) описание защиты и средств, предусмотренных для обеспечения безопасности, если необходимо приостановить СБФУ (например, для ручного программирования, верификации программ);

j) информацию о программировании, где это необходимо;

k) описание требований к техническому обслуживанию, применяемых для СБЭСУ, в том числе:

1) журнал для записи хронологии технического обслуживания машины;

2) стандартные действия, которые должны быть выполнены для поддержания функциональной безопасности СБЭСУ, включая плановую замену компонентов с заранее определенным сроком эксплуатации,

3) поддержание процедур, которые должны соблюдаться при появлении сбоя или отказа в СБЭСУ, включая:

- процедуры диагностики и устранения сбоя,
- процедуры, подтверждающие правильность работы после ремонта,
- требования к записи о техническом обслуживании,

4) инструментальные средства, необходимые для технического обслуживания и повторного ввода в эксплуатацию, а также процедуры для поддержания инструментальных средств и оборудования,

5) спецификации для периодического тестирования, профилактического технического обслуживания и внепланового технического обслуживания.

Примечания

1 Периодические испытания — это такие функциональные испытания, которые необходимы для подтверждения правильности работы и обнаружения сбоев.

2 Профилактическое техническое обслуживание — это меры, применяющиеся для поддержания требуемых рабочих характеристик СБЭСУ.

3 Внеплановое техническое обслуживание включает в себя меры, предпринятые после наступления конкретного сбоя(ев), которые возвращают СБЭСУ в состояние «как спроектировано».

8 Подтверждение соответствия СБЭСУ

Примечание — Подтверждение соответствия СБЭСУ может быть частью действий по подтверждению соответствия, выполняемых для проекта всей машины.

8.1 Цель

Данный раздел определяет требования к процессу подтверждения соответствия, который должен выполняться для СБЭСУ. Он включает в себя проверку и тестирование СБЭСУ для обеспечения достижения требований, указанных в спецификации требований к безопасности.

8.2 Общие требования

8.2.1 Подтверждение соответствия СБЭСУ должно быть выполнено в соответствии с подготовленным планом (см. 4.2).

Примечания

1 В некоторых случаях подтверждение соответствия не может быть выполнено до окончания установки (например, если разработка прикладного программного обеспечения не завершена до окончания установки).

2 Подтверждение соответствия программируемой СБЭСУ включает подтверждение соответствия как технических средств, так и программного обеспечения. Требования к подтверждению соответствия программного обеспечения представлены в 6.11.3.

8.2.2 Все СБФУ, указанные в спецификации требований к СБЭСУ (см. 5.2), и все процедуры эксплуатации и технического обслуживания СБЭСУ должны пройти процедуру подтверждения соответствия с помощью испытаний и/или анализа.

8.2.3 Должна быть создана соответствующая документация о выполнении для СБЭСУ подтверждения соответствия безопасности, в которой для каждой СБФУ указываются:

a) используемая версия плана подтверждения соответствия безопасности для СБЭСУ и версия тестируемой СБЭСУ;

b) тестируемая (или анализируемая) СБФУ вместе с конкретными ссылками на требования, определенные во время планирования подтверждения соответствия безопасности для СБЭСУ;

c) используемые инструменты и оборудование, а также данные калибровки;

d) результаты действий по подтверждению соответствия;

e) расхождения между ожидаемыми и фактическими результатами.

8.2.4 В случае расхождения между ожидаемыми и фактическими результатами должны быть выполнены корректирующие действия и повторное тестирование (в случае необходимости), и эти действия документально оформляются.

8.3 Подтверждение соответствия СБЭСУ систематической полноте безопасности

8.3.1 Должно быть выполнено следующее:

a) функциональное тестирование для выявления отказов на стадиях спецификации, проектирования и интеграции, а также для предотвращения отказов в процессе подтверждения соответствия программного обеспечения и аппаратных средств СБЭСУ. Функциональное тестирование должно включать верификацию (например, путем проверки или испытания), чтобы оценить, защищена ли СБЭСУ от неблагоприятных воздействий окружающей среды, и быть основано на спецификации требований к безопасности.

Примечание — См. также 6.12.2.1;

b) тестирование устойчивости к электромагнитным воздействиям, чтобы гарантировать, что СБЭСУ удовлетворяет требованиям 5.2.3. Испытания на устойчивость к электромагнитным воздействиям не выполняются для подсистем СБЭСУ или элементов подсистемы, если с помощью анализа может быть показано, что для предполагаемого применения их устойчивость адекватна устойчивости СБЭСУ.

Примечание — В СБЭСУ должна быть, где это реально, загружена типовая прикладная программа, а на все периферийные линии (все цифровые, аналоговые и последовательные интерфейсы, а также соединительные шины и шины питания и т. д.) оказывают влияние стандартные сигналы шума. Для того чтобы получить количественную оценку, разумно достаточно осторожно приближаться к предельным значениям;

c) тестирование с введением неисправностей, если требуемая доля безопасных отказов ≥ 90 %. В таких испытаниях вводятся или имитируются неисправности в технических средствах СБЭСУ, а полученный результат документально оформляется.

8.3.2 Кроме того, должны применяться одна или несколько из следующих групп аналитических методов с учетом сложности СБЭСУ и заданного УПБ:

a) статический анализ и анализ отказов.

Примечания

1 Такое сочетание аналитических методов подходит только для СБЭСУ, которые реализуют СБФУ с заданными УПБ, не превышающим УПБ 2.

2 Более подробную информацию можно найти в B.6.4 и B.6.6 МЭК 61508-7.

b) статический анализ, динамический анализ и анализ отказов.

Примечания

1 Такое сочетание аналитических методов не рекомендуется для СБЭСУ, которые реализуют СБФУ с заданными УПБ ниже УПБ 2.

2 Более подробную информацию можно найти в B.6.4, B.6.5 и B.6.6 МЭК 61508-7;

c) моделирование и анализ отказов.

Примечания

1 Такое сочетание аналитических методов подходит только для СБЭСУ, которые реализуют СБФУ с заданными УПБ, не превышающими УПБ2.

2 Более подробную информацию можно найти в B.3.6 и B.6.6 МЭК 61508-7.

8.3.3 Кроме того, должны применяться одна или несколько из следующих групп методов тестирования учетом сложности СБЭСУ и заданного УПБ:

a) тестирование методом «черного ящика»: тест(ы) динамического поведения в реальных условиях функционирования выявляют несоответствия с функциональной спецификацией СБЭСУ, а также оценивают полезность и надежность СБЭСУ.

Примечание — См. также 6.12.2.1;

b) тестирование с введением (включением) неисправностей должны проводиться, если требуемая доля безопасных отказов < 90%. В таких испытаниях вводятся или имитируются неисправности в технических средствах СБЭСУ, а полученный результат документально оформляется;

c) тестирование «наихудшего случая» следует выполнять для оценки экстремальных (т. е. худших) случаев, определенных в результате применения аналитических методов (см. 8.3.2).

Примечание — Операционная способность СБЭСУ и ее измеряемые компоненты тестируются при наихудших случаях. Условия окружающей среды изменяются до их максимально допустимых предельных значений. Наиболее существенные результаты тестов СБЭСУ проверяются и сравниваются со спецификацией требований к безопасности;

d) практический опыт: использование практического опыта из различных применений как одна из мер, позволяющая избежать сбоев во время выполнения подтверждения соответствия СБЭСУ.

Примечание — См. также 6.12.2.

9 Модификация

9.1 Цель

Данный раздел определяет процедуру(ы) модификации, которые должны применяться при внесении изменений в СБЭСУ на стадиях проектирования, интеграции и подтверждения соответствия (например, во время установки и ввода в эксплуатацию СБЭСУ).

9.2 Порядок внесения изменений

9.2.1 Причинами для появления запроса на модификацию могут быть, например:
- изменение спецификации требований к безопасности;
- использование реальных условий;
- опыта происшествий/аварий;
- изменение обрабатываемого материала;
- модификации машины или ее режимов работы.

Примечание — Вмешательства (например, настройка, установка, ремонт) в СБЭСУ в соответствии с инструкцией для пользователя или инструкцией по эксплуатации СБЭСУ не считаются модификациями в контексте настоящего раздела.

9.2.2 Причина(ы) запроса на модификацию СБЭСУ должны быть документально оформлены.

9.2.3 Влияние запрашиваемого изменения должно быть проанализировано, чтобы установить его влияние на функциональную безопасность СБЭСУ.

9.2.4 Анализ влияния модификации и влияние на функциональную безопасность СБЭСУ должны быть документально оформлены.

9.2.5 Все принятые изменения, которые оказывают влияние на СБЭСУ, должны инициировать возвращение к соответствующей стадии проектирования аппаратных средств и/или программного обеспечения СБЭСУ (например, спецификация, проектирование, интеграция, установка, ввод в эксплуатацию и подтверждение соответствия). Все последующие стадии должны осуществляться в соответствии с процедурами, установленными для этих стадий согласно требованиям настоящего стандарта. Все соответствующие документы должны быть пересмотрены, изменены и переизданы соответственно.

9.2.6 Перед выполнением любой модификации на основе этих пересмотренных документов должен быть подготовлен полный план действий и документально оформлен.

9.3 Процедуры управления конфигурацией

9.3.1 Процедуры управления конфигурацией должны выполняться в соответствии с планом функциональной безопасности (см. 4.2.1), учитывая следующее:

a) план каждого процесса модификации;

b) документацию по процессу принятия решений и по каждому соответствующему решению для СБЭСУ;

c) документацию для процедур запроса на изменение в хронологическом порядке (например, журнал), включающую:

- выявленные опасности, которые могут влиять на работоспособность,
- описание запроса на изменение (для аппаратных средств и/или программного обеспечения),
- причина(ы) запроса на изменение (см. также. 9.2.1),
- принятое решение (и разрешение для каждого решения),
- анализ влияния,
- повторная верификация (каждой стадии) и повторное подтверждение соответствия,
- все документы, на которые оказало влияние выполнение запроса на изменение,
- все действия, которые были выполнены во время процесса изменений, и лиц, ответственных за них,

d) документация со следующей информацией, чтобы выполнить последующий аудит:

- статус конфигурации,
- статус выпуска (релиза, версии),
- обоснование и согласование всех модификаций,
- сведения о модификации.

9.3.2 Процедуры для соответствующего процесса управления изменениями должны учитывать требования:

a) процедур для определения уникальной базовой конфигурации каждой версии СБЭСУ;

b) определения всех объектов конфигурации базовой конфигурации. Они должны включать по крайней мере:

1) результаты анализа и спецификацию требований к безопасности,

2) соответствующие документы по проектированию,

3) модули аппаратных средств и/или программного обеспечения,

4) планы и результаты тестирования,

5) отчеты по верификации и подтверждению соответствия,

6) информацию об уже существующих программных компонентах, которые должны быть включены в СБЭСУ,

7) инструменты и условия разработки, которые используются для создания и тестирования,

8) корректную поддержку уникальной идентификации всех объектов конфигурации, которые необходимы для обеспечения полноты СБЭСУ,

9) процедуры управления изменениями, чтобы:

- предотвращать несанкционированные изменения,
- документировать запросы на изменения,
- анализировать влияния предлагаемых в запросе изменений и принимать или отклонять запрос,
- документировать детали и авторизации для всех принятых изменений,
- устанавливать базовую конфигурацию в соответствующих точках разработки аппаратных средств или программного обеспечения и документировать (частично) тестирование интеграции, которое обосновывает базовую конфигурацию,
- гарантировать состав и формирование всех базовых конфигураций аппаратных средств или программного обеспечения (в том числе переформирование ранее созданных базовых конфигураций),

10) анализ и оценку влияния каждого запроса на изменение. Этот анализ должен также включать соответствующий анализ опасности и учитывать все другие действия при модификации СБЭСУ,

11) возврат к соответствующей стадии проекта аппаратных средств и/или программного обеспечения (например, спецификации, проектированию, интеграции, установке, вводу в эксплуатацию и подтверждению соответствия) СБЭСУ для всех принятых изменений, которые оказывают влияние на СБЭСУ. Все последующие стадии должны осуществляться в соответствии с процедурами, определенными для этих стадий согласно требованиям настоящего стандарта,

12) выполнение всех необходимых операций, чтобы продемонстрировать, что требуемая полнота безопасности была достигнута,

13) разрешение на выполнение необходимых действий по запросу на изменение должно зависеть от результатов анализа влияния.

9.3.3 Документация процесса управления изменениями должна содержать по крайней мере:

a) план процесса каждой модификации;

b) документацию по каждому из указанных выше организационных требований и процедурам;

c) документацию по процессу принятия решений и по каждому принятому решению, касающемуся СБЭСУ;

d) документацию в хронологическом порядке (журнал) процедур запроса на изменение, в том числе:

- выявленные опасности, которые могут влиять на работоспособность,
- описание запроса на изменение (для аппаратных средств и/или программного обеспечения),
- причина(ы) запроса на изменение (см. также 9.2.1),
- принятое решение (и разрешение для каждого решения),
- анализ влияния,
- повторные верификации (каждой стадии) и повторное подтверждение соответствия,
- все документы, на которые оказало влияние выполнение запроса на изменение,
- все действия, которые были выполнены во время процесса изменений, и лиц, ответственных за них;

e) документацию со следующей информацией, чтобы выполнить последующий аудит:

- статус конфигурации,
- статус выпуска (релиза, версии),
- обоснование и согласование всех модификаций,
- сведения о модификации.

10 Документация

10.1 Документация должна быть:

- точной и краткой;
- понятной для тех, кто должен ее использовать;
- пригодной для тех целей, для которых она предназначена;
- доступной и поддерживаемой.

10.2 Разработчик СБЭСУ должен готовить документацию для пользователя, проектирования и создания СБЭСУ.

10.3 Документы должны иметь названия или имена, указывающие на область содержащейся в них информации.

10.4 Документы должны иметь индекс версии (номер версии), позволяющий идентифицировать различные версии документа.

Примечание — Для получения дополнительной информации о методах, которые можно использовать для управления документацией (см. также МЭК 82045-1).

10.5 Таблица 5 обобщает информацию о доступной документации в случае необходимости.

Таблица 5 — Информация и документация на СБЭСУ

Необходимая информация	Подраздел (пункт, подпункт)
План функциональной безопасности	4.2.1
Спецификация требований к СБЭСУ	5.2
Спецификация требований к функциональной безопасности СБЭСУ	5.2.3
Спецификация требований к полноте безопасности СБЭСУ	5.2.4
Проект СБЭСУ	6.2.5
Структурированный процесс проектирования	6.6.1.2
Проектная документация на СБЭСУ	6.6.1.8
Структура функциональных блоков	6.6.2.1.1
Архитектура СБЭСУ	6.6.2.1.5
Спецификация требований к безопасности подсистемы	6.6.2.1.7

Окончание таблицы 5

Необходимая информация	Подраздел (пункт, подпункт)
Реализация подсистемы	6.7.2.2
Архитектура подсистемы (элементы и их взаимосвязи)	6.7.4.3.1.2
Требуемые исключения сбоев при оценке устойчивости к отказам/ДБО	6.7.6.1, перечисление c)/6.7.7.3
Формирование подсистемы	6.7.10
Спецификация требований к безопасности программного обеспечения	6.10.1
Программное обеспечение, основанное на параметризации	6.11.2.4
Пригодность инструментов разработки программного обеспечения	6.11.3.4.1
Документирование прикладной программы	6.11.3.4.5
Результаты тестирования модуля прикладного программного обеспечения	6.11.3.7.4
Результаты тестирования интеграции прикладного программного обеспечения	6.11.3.8.2
Документирование тестирования интеграции СБЭСУ	6.12.1.3
Документирование установки СБЭСУ	6.13.2.2
Документирование установки, эксплуатации и технического обслуживания	7.2
Документирование проверки подтверждения соответствия СБЭСУ	8.2.4
Документирование управления конфигурацией СБЭСУ	9.3.1

Приложение А
(справочное)

Определение уровня полноты безопасности

А.1 Общие положения

Данное приложение представляет один из примеров качественного подхода к оценке рисков и определению УПБ, которые могут быть применены к СБЭСУ для машин. Примеры других методов, которые могут быть использованы для определения УПБ, приведены в МЭК 61508-5 и будут представлены в технической спецификации, разрабатываемой в МЭК ТК 44.

Примечание — Методология, описанная в данном приложении, основана на использовании качественной оценки риска и предназначена в основном для определения УПБ СБЭСУ машин. Параметры риска (см. рисунок А.2), используемые в процессе применения этой методологии для конкретных машин и связанных с ними конкретных опасностей, должны быть согласованы с имеющимися для того, чтобы СБЭСУ могла обеспечить адекватное снижение рисков.

Для каждой конкретной опасности требования к полноте безопасности должны определяться отдельно для связанной(ых) с безопасностью функции(й) управления, реализуемой(ыми) СБЭСУ (см. 5.2.4.2).

На рисунке А.1 приведен пример практического способа выполнения оценки риска для конкретных опасностей, который приводит к оценке требования к УПБ для функции СБЭСУ. Эту методологию необходимо применить для каждого риска, который должен быть снижен связанной с безопасностью функцией управления, реализуемой СБЭСУ. Рисунок А.1 необходимо использовать совместно с указаниями настоящего приложения.

Оценка риска является итеративным процессом, это означает, что процесс должен выполняться более одного раза.

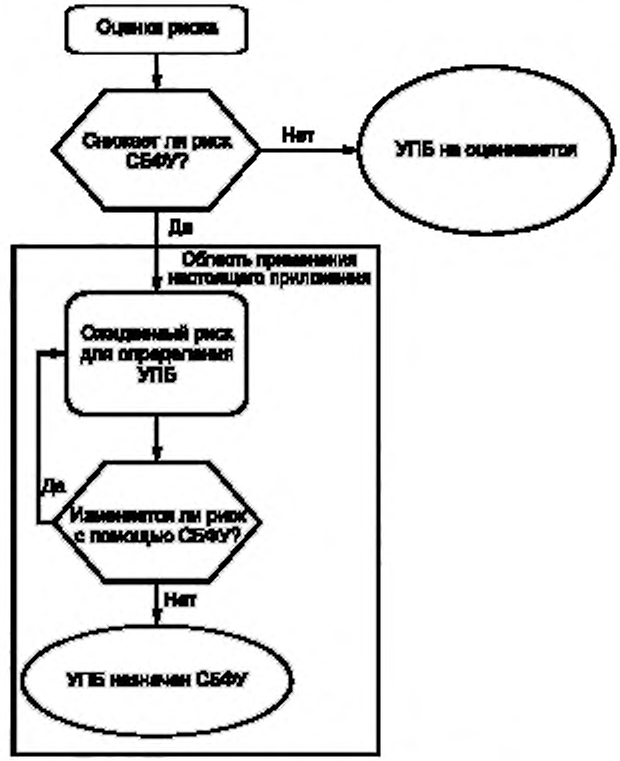


Рисунок А.1 — Структура процесса оценки УПБ

На рисунке А.1 стрелкой обратной связи показана оценка риска. Это необходимо выполнять, поскольку применение конкретной меры защиты, используемой для реализации СБФУ, может оказать влияние на параметры риска (например, использование защитной световой завесы способно привести к большей частоте доступа). Отказ световой завесы будет подвергать оператора большему риску, чем первоначально предполагалось. В этом случае необходимо повторить процесс оценки тем же способом, но с использованием измененных параметров риска.

В конце процесса, показанного на рисунке А.1, оцениваемый УПБ становится требованием к УПБ для связанной с безопасностью функции управления.

А.2 Оценка рисков и определение УПБ

А.2.1 Идентификация/индикация опасности

Указание опасностей, в том числе и из-за разумно предсказуемого неправильного использования, риск которых должен быть снижен путем реализации СБФУ. Они перечислены в столбце «опасности» в таблице А.5.

А.2.2 Оценка риска

Оценка риска должна проводиться путем определения параметров риска для каждой потенциально опасной ситуации и быть получена, как показано на рисунке А.2:

- из серьёзности (тяжести) вреда, *Se;*
- вероятности появления такого ущерба, который является функцией:
  - частоты и продолжительности воздействия опасности на людей, F_r;
  - вероятности возникновения опасного события, *Pr*;
  - вероятности предотвращения или ограничения вреда, *Av*.

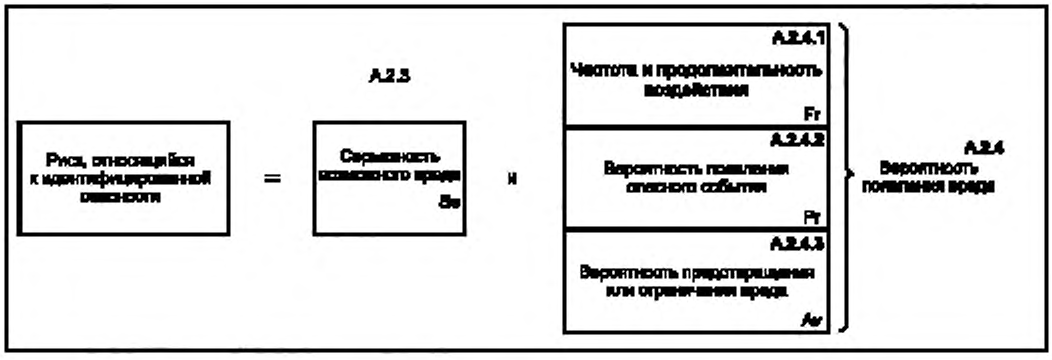


Рисунок А.2 — Параметры, используемые для оценки риска

Оценки параметров, используемые в таблице А.5, как правило, основаны на рассмотрении СБФУ в наихудших случаях. Тем не менее если, например, возможна необратимая травма, но со значительно меньшей вероятностью, чем обратимая, то каждый уровень серьезности должен иметь отдельную строку в таблице. Может произойти так, что различные СБФУ выполняются для каждой строки. Если одна СБФУ реализуется для двух строк, тогда должно использоваться наибольшее из них целевое требование к УПБ.

А.2.3 Серьезность (*Se*)

Серьезность (тяжесть) травмы или ущерба для здоровья может быть оценена с учетом обратимости травм, необратимости травм и смерти. Выбор соответствующего значения степени тяжести из таблицы А.1 основан на последствиях травм, где:

4 означает фатальную или значительную необратимую травму, после которой трудоспособность нарушается, если вообще возможна;

3 означает большую или необратимую травму, после которой возможно заниматься той же самой деятельностью. Сюда могут быть также включены тяжелые, но обратимые травмы, такие как переломы конечностей;

2 означает обратимую травму, включая серьезные рваные раны, колющие и сильные ушибы, которые требуют внимания со стороны врача;

1 означает незначительную травму, в том числе царапины и незначительные синяки, которые требуют оказания первой медицинской помощи.

Выберите соответствующую строку для серьезности последствий (*Se*) из таблицы А.1. Поместите соответствующий номер в столбец *Se* таблицы А.5.

Таблица А.1 — Классификация серьезности (*Se*)

Последствия	Серьезность (*Se*)
Необратимые: смерть, потеря глаза или руки	4
Необратимые: сломанные конечности, потеря пальца(ев)	3
Обратимые: требующие участия врача	2
Обратимые: требующие оказания первой медицинской помощи	1

А.2.4 Вероятность возникновения ущерба

Каждый из трех параметров вероятности возникновения ущерба (т. е. F_r, Pr и A_v) необходимо оценивать независимо друг от друга. Для каждого параметра должны быть использованы их значения для наихудшего случая, чтобы убедиться, что СБФУ присвоено правильное значение УПБ, а не более низкое, чем это необходимо. Настоятельно рекомендуется использование подхода, основанного на анализе задачи, для обеспечения уверенности, что оценке вероятности возникновения ущерба уделяется надлежащее внимание.

А.2.4.1 Частота и продолжительность воздействия

Рассмотрим следующие аспекты, чтобы определить уровень воздействия:

- необходимость доступа в опасную зону во всех режимах использования, например, при нормальной эксплуатации, при техническом обслуживании;
- характер доступа, например, ручная подача материала, ручная установка.

Это дает возможность оценить средний интервал между воздействиями и, следовательно, среднюю частоту доступа.

Также возможно предсказать продолжительность, например, если она будет больше чем 10 мин. Если продолжительность меньше чем 10 мин, то величина степени воздействия может быть уменьшена до значения следующей строки. Это не относится к частоте воздействия ≥ 1 в ч, для которой степень воздействия никогда не должна уменьшаться.

Примечание — Продолжительность воздействий связана с исполнением действий, выполняемых под защитой СБФУ. При длительных нахождениях в опасной ситуации к изоляции шин питания и рассеиванию энергии следует применять требования МЭК 60204-1 и ИСО 14118.

Рассматриваемый фактор не учитывает отказ СБФУ.

Выберите соответствующую строку для частоты и продолжительности воздействия (*Fr*) в таблице А.2. Вставьте соответствующее значение в столбец *Fr* таблицы А.5.

Таблица А.2 — Классификация частоты и продолжительности воздействия (*Fr*)

Частота и продолжительность воздействия (*Fr*)	
Частота воздействия	Степень воздействия, *Fr* (см. А.2.4.1)
≥ 1 в ч	5
от < 1 в ч до ≥ 1 в день	5
от < 1 в день до ≥ 1 за 2 недели	4
от <1 за 2 недели до ≥ 1 в год	3
от < 1 в год	2

А.2.4.2 Вероятность возникновения опасного события

Вероятность возникновения ущерба необходимо оценивать независимо от других параметров *Fr* и *Av*. Для каждого параметра должны быть использованы их значения для наихудшего случая, чтобы убедиться, что СБФУ не присвоено неправильно значение УПБ, более низкое, чем это необходимо. Для того чтобы это предотвратить, настоятельно рекомендуется использование подхода, основанного на анализе задачи, для обеспечения уверенности, что оценке вероятности возникновения ущерба уделяется надлежащее внимание.

Рассматриваемый параметр можно оценить, учитывая:

а) предсказуемость поведения составных частей машины, имеющей отношение к опасности в различных режимах использования (например, нормальная эксплуатация, техническое обслуживание, диагностика).

Требуется тщательное рассмотрение системы управления в отношении риска неожиданного запуска. Влияние защиты любой СБЭСУ не учитывается. Это необходимо для того, чтобы оценить степень риска, если в СБЭСУ

произойдет сбой. В целом следует учитывать, может ли машина или обрабатываемый материал вести себя неожиданным образом.

Поведение машины будет варьироваться от строго предсказуемого до непредсказуемого, но неожиданные события нельзя не учитывать.

Примечание — Значение предсказуемости часто связано со сложностью функционирования машины.

b) заданные или прогнозируемые характеристики поведения человека при взаимодействии с составными частями машины, имеющими отношение к опасности. Такими характеристиками могут быть:

- стресс (например, из-за нехватки времени, рабочей задачи, ограниченности воспринимаемого ущерба);
- недостаточная осведомленность об опасности. Она будет зависеть от таких факторов, как навыки, обучение, опыт и сложность машины/процесса.

Эти характеристики обычно не определяются разработчиком СБЭСУ непосредственно, но анализ задачи обнаружит действия, которые при общем понимании всех вопросов, в том числе и неожиданных результатов, нельзя разумно предположить.

«Очень высокая» вероятность возникновения опасного события должна быть выбрана, если необходимо отразить нормальные производственные ограничения и работу в наихудших случаях. Для любого более низкого значения требуются оправдывающие причины (например, хорошо определенное применение и компетенция пользователей, обладающих знаниями высокого уровня).

Примечание — Все требуемые или предполагаемые навыки, знания и т. д., должны быть указаны в информации для пользователя.

Выберите соответствующую строку для вероятности возникновения опасного события (*Pr*) в таблице А.3. Вставьте соответствующее значение в столбце *Pr* в таблице А.5.

Таблица А.3 — Классификация вероятности возникновения опасного события (*Pr*)

Вероятность возникновения	Значение *Pr*
Очень высокая	5
Вероятно	4
Возможно	3
Редко	2
Незначительная	1

А.2.4.3 Вероятность избежать или ограничить вред (*Av*)

Этот параметр оценивает, как учитываются различные аспекты проектирования машины и ее предполагаемого применения, которые способны помочь избежать или ограничить вред от опасности. К таким аспектам можно отнести, например:

- скорость появления опасного события: внезапно, быстро или медленно;
- пространственные возможности избежать опасность;
- природу компонента или системы, например нож, обычно острый, трубы в среде по переработке молока, как правило, горячие, электричество, как правило, опасно по своей природе, но невидимо;
- возможность распознавания опасности, например, опасность поражения электрическим током: медная шина не меняет свой внешний вид в зависимости от того, является ли она под напряжением или нет; чтобы человеку распознать, нужен инструмент для установления, находится ли электрическое оборудование под напряжением или нет; другим примером является влияние условий окружающей среды, например высокий уровень шума может помешать человеку услышать запуск машины.

Выберите соответствующую строку в таблице А.4 с вероятностью предотвращения или ограничения вреда (*Av*). Вставьте соответствующее значение в столбце *Av* в таблице А.5.

Таблица А.4 — Классификация вероятности избежать или ограничить вред (Av)

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

А.2.5 Класс вероятности вреда (*Cl*)

Для каждой рассматриваемой опасности и в зависимости от обстоятельств для каждого уровня серьезности сложить значения в столбцах *Fr*, *Pr* и *Av*, а результат поместить в столбец *Cl* таблицы А.5.

Таблица А.5 — Параметры, используемые для определения класса вероятности вреда (*Cl*)

№	Опасность	Se	Fr	Pr	Av	Cl
1						
2						
3						
4						

А.2.6 Определение УПБ

В таблице А.6 на пересечении строки, представляющей конкретное значение уровня серьезности (*Se*) для конкретной опасности, и столбцов, представляющих диапазоны значений класса вероятности вреда (*Cl*), указаны действия, если они требуются. Залитая черным цветом область указывает значение УПБ, являющееся целевым для СБФУ. Залитая серым цветом область указывает на рекомендуемые другие методы (ДМ), которые могут быть использованы.

Таблица А.6 — Матрица определения УПБ

Серьезность (*Se*)	Класс (*Cl*)				
	3–4	5–7	8–10	11–13	14–15
4	УПБ 2	УПБ 2	УПБ 2	УПБ 3	УПБ 3
3		(ДМ)	УПБ 1	УПБ 2	УПБ 3
2			(ДМ)	УПБ 1	УПБ 2
1				(ДМ)	УПБ 1

Пример — Для конкретной опасности, для которой Se = 3, Fr = 4, Pr = 5 и Av = 5, имеем:

Cl = Fr + Pr + Av = 4 + 5 + 5 = 14

В соответствии с таблицей А.6 для ослабления указанной опасности для СБФУ будет определен УПБ 3.

На рисунке А.3 показан пример документа, который может быть использован для записи результатов определения УПБ, выполненного с помощью данного приложения.

Номер документа

Часть №

Оценка риска и меры безопасности

Изделие: _____

Выпустил: _____

Дата _____

Черный фон = Требуемые меры безопасности

Серый фон = Рекомендуемые меры безопасности

	Предварительная оценка риска
	Средняя оценка риска
	Оценка риска наперед

Результат	Степень тяжести	Класс, CL					Частота и продолжительность		Вероятность опасного события, Pr		Предотвращение, Av	
		3–4	5–7	8–10	11–13	14–15						
Смерть, потеря глаза или руки	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 ч	5	Очень высокая	5		
Необратимое, потеря пальцев	3		OM	SIL 1	SIL 2	SIL 3	> 1 ч — <= 1 д	5	Высокая	5		
Обратимое, медицинский уход	2			OM	SIL 1	SIL 2	> 1 д — <= 2 нед	3	Средняя	4	Невозможно	5
Обратимое, первая помощь	1				OM	SIL 1	> 2 нед — <= 1 г	2	Низкая	3	Возможно	3
							> 1 г	1	Ничтожная	1	Скорее всего	1

№ п/п	№ опасн.	Опасность							Se	Fr	Pr	Av	Cl			Мера безопасности				Safe

Комментарии

Рисунок А.3 — Пример формы для документального оформления процесса определения УПБ

Приложение В
(справочное)

Пример проекта СБЭСУ с применением понятий и требований разделов 5 и 6

В.1 Общие положения

Структурированный подход к проектированию СБЭСУ, используемый в настоящем стандарте, определяет методологию, с которой функционал и требования к полноте безопасности связанных с безопасностью функций управления декомпозируются на ряд подфункций. Этот процесс используется для реализации в машиностроении технической платформы для функциональной безопасности, а рисунок В.1 описывает терминологию, используемую на каждом из этих уровней, что является важным при интеграции проекта СБЭСУ в процессе установки машины.

Эту методологию проектирования с помощью процессов верификации и подтверждения соответствия можно использовать для демонстрации того, что СБЭСУ соответствует спецификации требований к безопасности, описанной в разделе 5.

В последующем примере проект СБЭСУ предназначен для того, чтобы разъяснить принципы декомпозиции функционала и реализации заданной, связанной с безопасностью функции управления в соответствии с требованиями раздела 6. Данный пример упрощен и не учитывает дополнительные меры, которые могут потребоваться на практике, например, провести (подготовить) устройства к запуску.

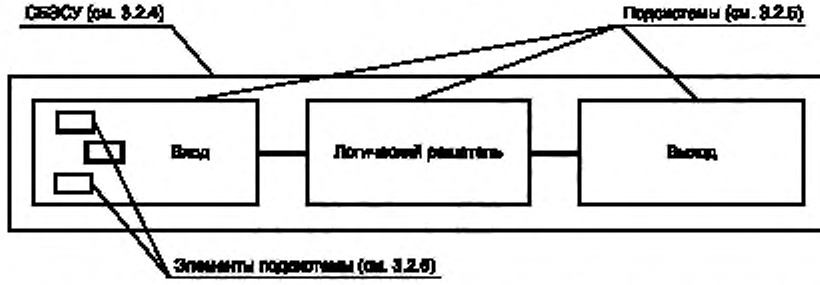


Рисунок В.1 — Терминология, используемая при функциональной декомпозиции

Термины, представленные на рисунке В.1, предназначены для разграничения процесса проектирования на два ключевых этапа, а именно:

- проектирование СБЭСУ, которое может быть выполнено конструктором машин или интегратором систем управления;
- проектирование подсистемы (и ее элемента), которое выполняется поставщиками электрического и управляющего оборудования (например, пускателей, переключателей с взаимной блокировкой, программируемых логических контроллеров) и конструкторами машин или интеграторами систем управления.

В.2 Пример

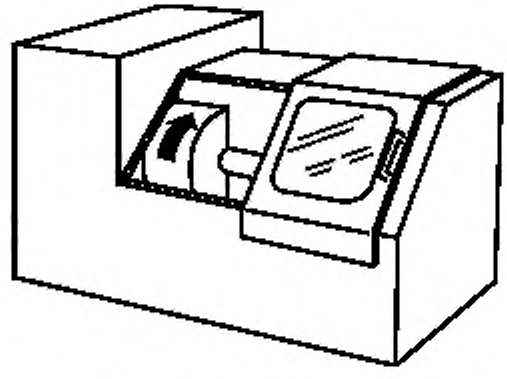


Рисунок В.2 — Пример машины

Методология, используемая в настоящем стандарте, основана на структурированном подходе сверху вниз: разработки спецификации связанных с безопасностью функций управления и проекта СБЭСУ, которая реализует эти функции.

Шаг 1: Спецификация требований к безопасности СБФУ (см. раздел 5).

Из спецификации требований к безопасности СБФУ можно получить следующую информацию:

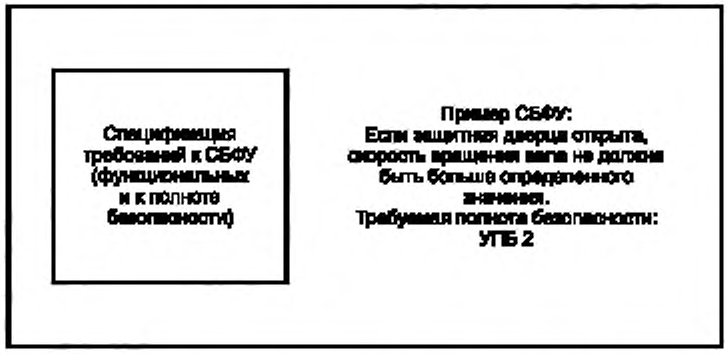


Рисунок В.3 — Спецификация требований к СБФУ

Шаг 2. Процесс разработки и проектирования СБЭСУ (см. 6.6.2)

Шаг 2.1. Как указано в спецификации требований к безопасности, связанная с безопасностью функция управления декомпозируется в структуру функциональных блоков.

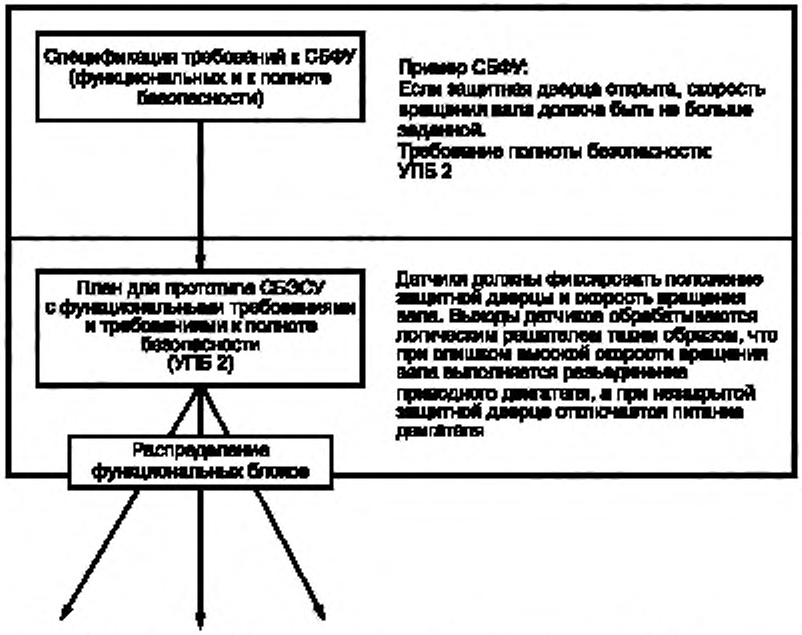


Рисунок В.4 — Декомпозиция в структуру функциональных блоков

Шаг 2.2. Структура функциональных блоков формирует начальную концепцию архитектуры СБЭСУ. Требования безопасности для каждого функционального блока выводятся из спецификации требований к безопасности соответствующей, связанной с безопасностью функции управления.

Элемент(ы), реализующие каждый функциональный блок, должен(ы) иметь по крайней мере то же значение УПБ, что и определенное для СБФУ. Это показано на рисунке В.5 для УПБ 2 (например, для ФБ1 предельное (требуемое) значение для УПБ равно 2 (ПТУПБ2) и т. д.).

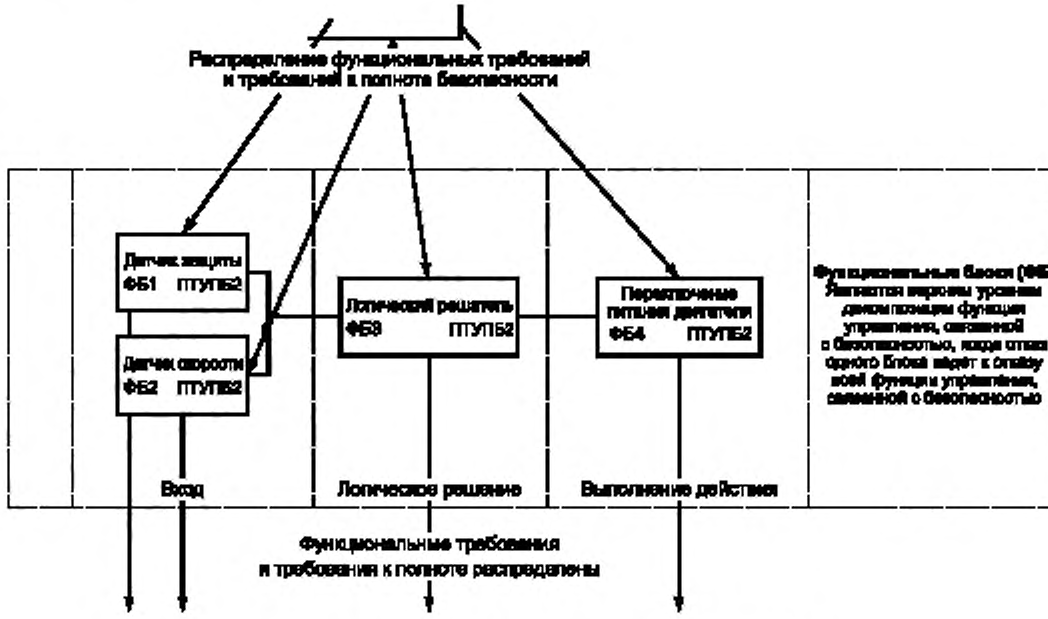


Рисунок В.5 — Начальная концепция архитектуры СБЭСУ

Шаг 3. Каждый функциональный блок реализуется подсистемой в рамках архитектуры СБЭСУ. Каждая подсистема может состоять из элементов подсистемы и при необходимости функций диагностики, чтобы убедиться, что сбои могут быть обнаружены и соответствующие меры приняты (см. 6.2).

Архитектура должна описывать СБЭСУ с точки зрения ее подсистем и их взаимосвязей. Для данного примера существует ряд альтернатив, которые могут быть использованы для реализации СБЭСУ и ее архитектуры подсистем.

Альтернатива 1. В этом случае (см. рисунок В.6) диагностические функции встроены в каждую подсистему.

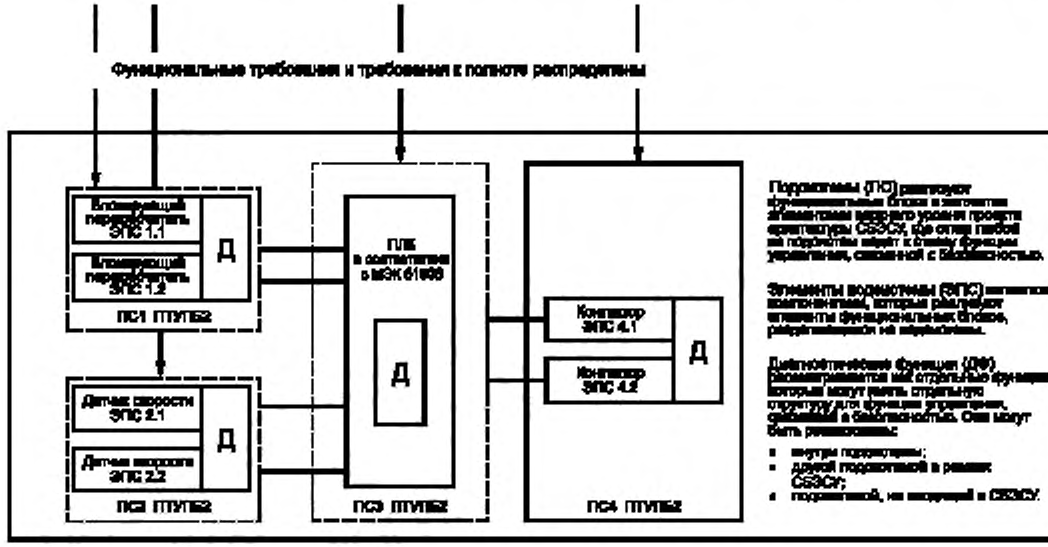


Рисунок В.6 — Архитектура СБЭСУ с диагностическими функциями, встроенными в каждую подсистему (подсистема 1 — подсистема 4)

Альтернатива 2. В данном случае (см. рисунок В.7) диагностические функции встроены в программируемый логический контроллер (ПЛК) в подсистему 3, что удовлетворяет соответствующим аспектам МЭК 61508.

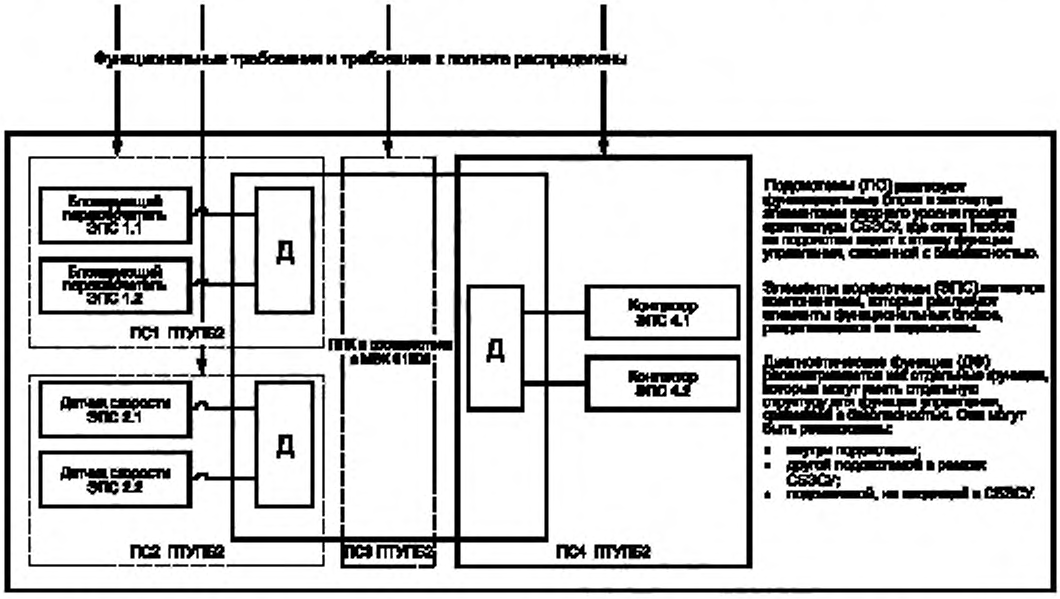


Рисунок В.7 — Архитектура СБЭСУ с диагностическими функциями, встроенными в подсистему 3

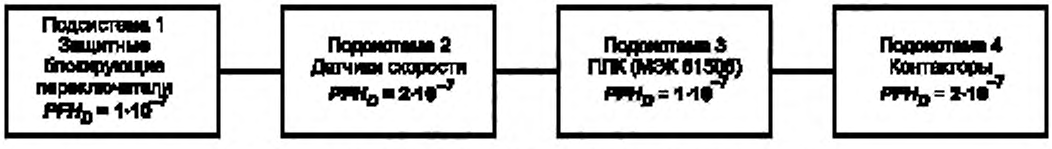
Шаг 4. Оценка УПБ, которая может быть достигнута СБЭСУ (см. 6.6.3).

Значение УПБ, которое может быть задано для СБЭСУ, должно быть меньше или равно предельному значению УПБ любой из подсистем. Вероятность опасных случайных отказов аппаратных средств СБЭСУ (PFH_{DSRECS}) является суммой вероятностей опасных отказов в час всех подсистем (от PFH_{D1} до PFH_{Dn}), участвующих в выполнении связанных с безопасностью функций управления, и включает в себя в случае необходимости вероятность опасных ошибок передачи (P_{TE}) для цифровой передачи данных, как:

$$PFH_{DSRECS} = PFH_{D1} + ... + PFH_{Dn} + P_{TE}.$$

Для данного примера целевое значение отказа для связанных с безопасностью функций управления определено как УПБ 2, а из таблицы 3 (см. 5.2.4.2) это эквивалентно вероятности опасных отказов в час (PFH_D) в диапазоне $\geq 10^{-7}$ до $< 10^{-6}$. Поэтому, предполагая, что вероятность опасных отказов в час каждой из подсистем определена, как показано ниже, сумма вероятностей опасного отказа в час всех подсистем может быть оценена, как показано на рисунке В.8.

Таким образом, в данном примере можно показать, что проект СБЭСУ удовлетворяет все требования для реализации УПБ 2, определенного для связанной с безопасностью функции управления.



$$PFH_{DSRECS} = (1 \cdot 10^{-7}) + (2 \cdot 10^{-7}) + (1 \cdot 10^{-7}) + (2 \cdot 10^{-7}) = 6 \cdot 10^{-7}$$

Рисунок В.8 — Оценка PFH_D для СБЭСУ

Приложение С
(справочное)

Руководство по проектированию и разработке встроенного программного обеспечения

Примечание — Данное приложение представляет основной подход, который удовлетворяет требованиям МЭК 61508-3. Сам по себе без применения дополнительных мер он не может обеспечить соответствие с МЭК 61508-3.

С.1 Общие положения

Данное приложение предназначено оказать помощь лицам при проектировании и разработке встроенного программного обеспечения для реализации связанных с безопасностью функций управления СБЭСУ.

Основная цель — дать общие указания по предотвращению отказов во встроенном программном обеспечении и любого другого неожиданного поведения встроенного программного обеспечения, которые могут привести к созданию опасного сбоя в системе.

Для того чтобы реализовать эту цель, необходимо рассмотреть следующее:

- описание основных характеристик, которыми должны обладать элементы программного обеспечения СБЭСУ, чтобы гарантировать их качество и безопасность (руководящие указания по элементам программного обеспечения);
- создание всех необходимых технических мероприятий и положений, связанных с разработкой программного обеспечения, для тех, кто участвует в проектировании программного обеспечения. Они могут быть использованы в качестве руководства для разработчика при создании этого типа программного обеспечения (руководящие указания по процессу разработки программного обеспечения);
- рекомендуемый подход для оценки программного обеспечения. Это позволяет разработчику программного обеспечения и/или аналитику провести анализ и решить, что элементы программного обеспечения соответствуют требованиям к безопасности СБЭСУ или подсистемы СБЭСУ (руководящие указания по верификации программного обеспечения).

Данное приложение предоставляет набор основных принципов, согласованных с МЭК 61508-3, которые адаптированы к встроенному программному обеспечению для микропроцессоров.

С.2 Руководящие указания по элементам программного обеспечения

Данный подраздел представляет руководящие указания, которые должны быть выполнены для встроенного программного обеспечения элемента СБЭСУ или подсистемы СБЭСУ для обеспечения их безопасности в эксплуатации и достаточно высокого качества. Для получения такого программного элемента должны быть установлены: набор мероприятий, определенная организация и ряд принципов. Это необходимо выполнить на ранних стадиях разработки.

С.2.1 Учет архитектуры системы

Необходимо, чтобы список ограничений, накладываемых архитектурой аппаратных средств на программное обеспечение, был определен и документально оформлен. Разработчиком должны быть определены и оценены последствия влияния любого программно-аппаратного взаимодействия на безопасность находящейся под контролем машины или системы, а также учтены при проектировании программного обеспечения.

Примечание — Существуют следующие ограничения: протоколы и форматы, частоты входных/выходных данных, по нарастающему и убывающему фронту или по уровню, входные данные, использующие обратную логику и т. д. Перечень этих ограничений учитывается в начале разработки и снижает риск несовместимости программного обеспечения и технических средств, если программное обеспечение устанавливается в заданные аппаратные средства.

С.2.2 Спецификации программного обеспечения

Спецификация программного обеспечения должна учитывать следующее:

- связанные с безопасностью функции управления с количественным описанием критериев эффективности функционирования (точность, корректность) и временными ограничениями (время отклика) с их допусками или допустимыми отклонениями, если это возможно;
- конфигурацию или архитектуру системы;
- указания, относящиеся к полноте безопасности аппаратных средств (логических устройств, датчиков, приводов и др.);
- указания, относящиеся к полноте программного обеспечения;
- ограничения, связанные с объемом памяти и временем отклика системы;
- интерфейсы оператора и оборудования;

- указания по самоконтролю программного обеспечения и контролю аппаратных средств, осуществляемому с помощью программного обеспечения;
- указания, позволяющие проверить все связанные с безопасностью функции управления во время работы систем (например, тестирование в неавтономном режиме, время захвата для быстрых сигналов, совмещение со скоростью сканирования).

Примечание — Указания для самоконтроля программного обеспечения, разработанные с учетом целей безопасности и операционных ограничений (продолжительность непрерывной работы и т. д.), могут включать использование таких устройств, как сторожевые устройства, контроль загрузки центрального процессора, обратная связь от выхода ко входу. Для контроля аппаратных средств, процессора, памяти, и т.д. должны быть включены в спецификации указания по верификации связанной с безопасностью функции управления: например, возможность периодической проверки правильности работы устройств безопасности.

Необходимо, чтобы функциональные требования были определены для каждого режима функционирования. Должен быть указан переход от одного режима к другому.

Примечание — Функциональные режимы могут включать номинальный и один или более ухудшенных режимов. Цель состоит в том, чтобы указать поведение во всех ситуациях и избежать неожиданного поведения в неноминальных режимах.

С.2.3 Уже существующее программное обеспечение

Термин «уже существующее» программное обеспечение относится к исходным модулям, которые не были разработаны специально для данной системы и будут интегрированы в созданное программное обеспечение. Оно включает в себя элементы программного обеспечения, созданного разработчиком для предыдущих проектов, или является коммерчески доступным программным обеспечением (например, модули для расчетов, алгоритмы сортировки данных).

При работе с таким типом программного обеспечения, особенно в случае элементов коммерческих программ, разработчик не всегда имеет доступ ко всем элементам, которые были необходимы для предыдущего удовлетворения требований (например, какие тесты были выполнены, доступна ли проектная документация). Поэтому может быть необходимо в самый кратчайший момент конкретное взаимодействие с аналитиком.

Разработчик должен показать аналитику, как используется уже существующее программное обеспечение, а также продемонстрировать, что оно имеет такой же уровень, как и другие элементы программного обеспечения. Такая демонстрация должна быть выполнена:

a) с помощью тех же мероприятий по верификации уже существующего программного обеспечения, как и для остальной части программного обеспечения;

b) или с использованием практического опыта, где уже существующее программное обеспечение функционирует в аналогичной системе сопоставимой окружающей среды (например, может быть необходимо оценить последствия изменения компилятора или другого формата архитектуры программного обеспечения).

Примечание — Цель взаимодействия с аналитиком по вопросам применения уже существующего программного обеспечения — начать с ним как можно раньше консультации о любых возможных трудностях, к которым может привести применение этого типа программного обеспечения. Интеграция уже существующих исходных модулей может быть причиной некоторых аномалий или небезопасного поведения, если они не были разработаны с той же строгостью, как и остальное программное обеспечение.

Уже существующее программное обеспечение должно быть определено с помощью тех же принципов управления конфигурацией и управления версиями, которые применяются к остальному программному обеспечению.

Примечание — Управление конфигурацией и управление версиями должны осуществляться для всех компонентов программного обеспечения независимо от их происхождения.

С.2.4 Проектирование программного обеспечения

Описание программного обеспечения должно включать в себя описание:

- программной архитектуры, которая определяет структуру, удовлетворяющую спецификациям;
- входов и выходов (например, в форме внутреннего и внешнего словаря данных) для всех модулей, составляющих архитектуру программного обеспечения;
- прерываний;
- глобальных данных;
- каждого программного модуля (входы/выходы, алгоритм, особенности проектирования и т. д.);
- используемого модуля или библиотеки данных;
- уже используемого программного обеспечения.

Программное обеспечение должно быть модульным и написано в логическом порядке, чтобы упростить его проверку и техническое обслуживание:

- каждый модуль или группа модулей должны соответствовать, если это возможно, некоторой функции в спецификации(ях);
- необходимо, чтобы интерфейсы между модулями были как можно более простыми.

Примечание — Обобщенную характеристику корректной архитектуры программного обеспечения можно сформировать следующим образом: модуль должен обладать высоким уровнем функциональной связности и простым интерфейсом с внешней средой.

Программное обеспечение должно:
- ограничивать количество или пространство глобальных переменных;
- управлять размещением массивов в памяти (чтобы избежать риска переполнения массива).

С.2.5 Кодирование

Исходный код должен:
- быть читаемым, понятным, и пригодным к проверке;
- удовлетворять специфицированным требованиям к проекту программного модуля;
- подчиняться руководящим указаниям по кодированию.

С.3 Указания по процессу разработки программного обеспечения

С.3.1 Процесс разработки. Жизненный цикл программного обеспечения

Целью последующих указаний, применимых к жизненному циклу программного обеспечения, является создание формализованного описания организации разработки программного обеспечения и, в частности, различных технических задач, составляющих такую разработку.

Жизненный цикл разработки программного обеспечения должен быть определен и документально оформлен (например, в плане качества программного обеспечения) и включать все технические мероприятия и стадии, необходимые и достаточные для разработки программного обеспечения.

Каждая стадия жизненного цикла должна быть разделена на элементарные задачи и включать в себя описание:
- входов (документы, стандарты и т. д.);
- выходов (подготовленные документы, аналитические отчеты и т. д.);
- мероприятий, которые будут осуществляться;
- проверок, которые необходимо выполнить (анализы, тесты и т. д.).

С.3.2 Документация. Управление документацией

Документация должна соответствовать требованиям раздела 10.

С.3.3 Управление конфигурацией и модификацией программного обеспечения

Результат управления конфигурацией и, следовательно, версиями является неотъемлемой частью любой разработки и требует утверждения. Утверждение действительно только в тех случаях, где данная конфигурация может быть идентифицирована. Управление конфигурацией включает в себя определение действий по конфигурации, управление изменениями, создание контрольных точек и архивирование элементов программного обеспечения, в том числе ассоциированных данных (документов, протоколов испытаний и т. д.). На протяжении всего жизненного цикла проекта основными целями является обеспечение:

- определенной и управляемой конфигурации программного обеспечения, которая гарантирует физическое архивирование и может быть использована для воссоздания соответствующего исполняемого кода (с дальнейшей разработкой программного обеспечения или его изменением в памяти);
- опорными конфигурациями для управления изменениями;
- средствами управления, такими, чтобы любые проблемы должным образом были проанализированы, а утвержденные изменения выполнены.

Что касается изменений, то их причины могут возникнуть, например, если:
- функциональная безопасность оказалась ниже заданной;
- имеется опыт работы с систематическими отказами;
- обновилось или изменилось законодательство по безопасности;
- изменилась машина или ее использование;
- изменились требования ко всей системе безопасности;
- анализ технических характеристик эксплуатации и технического обслуживания указывает, что производительность ниже целевого показателя.

С.3.4 Управление конфигурацией и архивированием

Процедура управления конфигурацией и изменениями должна быть определена, документально оформлена и включать в себя следующие пункты:

- объекты, которыми управляет конфигурация, по крайней мере: спецификация программного обеспечения, предварительный и детальный проекты программного обеспечения, модули исходного кода, планы, процедуры и результаты проверки подтверждения соответствия;
- правила идентификации (исходного модуля, версии программного обеспечения и т. д.);
- обработка модификаций (запись запросов и т. д.).

Для каждого объекта конфигурации должна существовать возможность для определения любых изменений, которые могут произойти, и версий любых связанных с ним элементов.

Примечание — Цель состоит в том, чтобы иметь возможность проследить развитие каждого объекта в хронологическом порядке: какие изменения были сделаны, почему и когда.

Управление конфигурацией программного обеспечения должно позволить получить точную и однозначную идентификацию версии программного обеспечения. Управление конфигурацией должно связать все объекты (и их версии), необходимые для демонстрации функциональной безопасности.

Все объекты в конфигурации программного обеспечения должны быть охвачены процедурой управления конфигурацией до проверки или до запроса аналитиком для оценки окончательной версии программного обеспечения.

Примечание — Цель состоит в том, чтобы обеспечить выполнение процедуры оценки программного обеспечения со всеми его элементами в точно определенном состоянии. Любое последующее изменение может потребовать пересмотра программного обеспечения, которое должно быть идентифицируемо аналитиком.

Должны быть установлены процедуры для архивирования программного обеспечение и связанных с ним данных (методы для хранения резервных копий и архивов).

Примечание — Эти резервные копии и архивы могут быть использованы для поддержания и изменения программного обеспечения в течение срока жизни его функционирования.

С.3.5 Управление изменениями программного обеспечения

Любое изменение программного обеспечения, оказывающее влияние на функциональную безопасность СБЭСУ, должно подчиняться правилам, установленным для управления изменениями и конфигурацией, поэтому процесс разработки возвращается на самый высокий уровень, необходимый для учета изменения и не снижающий функциональную безопасность.

Примечание — В частности, также должна быть обновлена документация и выполнены все необходимые мероприятия по проверке. Это гарантирует, что программное обеспечение будет сохранять все свои первоначальные свойства после любых модификаций.

С.4 Инструментальные средства разработки

Инструменты, используемые в процедуре разработки (компилятор, компоновщик, тесты и т. д.), должны быть определены (имя, ссылка, версия и т. д.) в документации, связанной с версией программного обеспечения (например, в документации управления версиями).

Примечание — Различные версии инструментальных средств необязательно дают одинаковые результаты. Таким образом, точная идентификация инструментального средства прямо свидетельствует о непрерывности процесса генерации исполняемой версии в том случае, если версия изменяется.

С.5 Воспроизводство, поставка

С.5.1 Создание исполнимого кода

Любой выбор или изменение при генерации во время создания программного обеспечения должны быть записаны (например, в листе версий) так, чтобы можно было определить, как и когда программа была создана.

С.5.2 Установка и эксплуатация программного обеспечения

Все отказы, относящиеся к связанным с безопасностью функциям управления, доводятся до сведения разработчика системы и должны быть записаны и проанализированы.

Примечание — Это означает, что разработчик знает о любом отказе, связанного с безопасностью программного обеспечения, которые доводятся до него, и он принимает соответствующие меры (например, предупреждения другим пользователям, модификацию программного обеспечения и т. д.).

С.6 Верификация и подтверждение соответствия программного обеспечения

Цель верификации — продемонстрировать, что элементы программного обеспечения, созданные на данной стадии цикла разработки соответствуют требованиям, установленным на предыдущих стадиях, а также всем применяемым стандартам и правилам. Они также служат средством выявления и учета любых ошибок, которые могли попасть в программное обеспечение в процессе его разработки.

Верификация программного обеспечения не просто серия тестов, даже при том, что она является основным действием для сравнительно небольшого элемента программного обеспечения, которое рассматривается в данном приложении. Другие виды действий, связанные с этими тестами или нет, такие как обзор и анализ, также считаются действиями по верификации. В некоторых случаях они могут заменить некоторые тесты (например, в том случае, если тест не может быть выполнен, потому что это может привести к ухудшению компонентов аппаратных средств).

С.7 Общие руководящие указания по верификации и подтверждению соответствия

Аналитик должен уметь выполнять оценку соответствия программного обеспечения путем проведения любых аудитов или экспертиз, считающихся полезными на различных стадиях разработки программного обеспечения.

Все технические аспекты процессов жизненного цикла программного обеспечения подлежат оценке аналитиком. Ему должны быть доступны все отчеты о проверке (тесты, анализы и т.д.) и все технические документы, используемые при разработке программного обеспечения.

Примечания

1 Вмешательство аналитика на стадии спецификации предпочтительнее его апостериорного вмешательства, так как оно должно ограничить влияние любых принимаемых решений. С другой стороны, финансовые и человеческие аспекты проекта не подвергаются оценке.

2 В интересах заявителя представить удовлетворительные свидетельства всех действий, выполненных во время разработки программного обеспечения.

3 Аналитик должен иметь все необходимые элементы в своем распоряжении для того, чтобы сформулировать мнение.

Оценка соответствия программного обеспечения выполняется для конкретной версии программного обеспечения, на которую ссылаются. О любой модификации ранее оцененного программного обеспечения, которое получило заключительное мнение от аналитика, необходимо сообщить последнему, чтобы были выполнены все дополнительные действия по оценке этой модификации.

Примечание — Любое изменение может изменить поведение программного обеспечения, поэтому оценка, выполняемая аналитиком, может быть применена только к строго конкретной версии программного обеспечения.

С.8 Анализ верификации и подтверждения соответствия

Аналитические действия и верификация проектирования программного обеспечения должны проверить соответствие спецификациям.

Примечание — Цель состоит в том, чтобы удостовериться, что требования к программному обеспечению и проект (и детализированный и предварительный) когерентны.

Внешний анализ подтверждения соответствия (с аналитиком) должен быть проведен в конце стадии подтверждения соответствия.

Примечание — Это может быть использовано, чтобы установить, удовлетворяет или нет элемент спецификации.

Необходимо, чтобы результат каждого анализа был документально оформлен и помещен в архив. Он должен включать список всех действий, выполненных в процессе анализа, и краткое заключения (решение о том, следует ли переходить к следующему действию). Виды действий, выполняемые при анализе, нужно контролировать и рассматривать.

С.9 Тестирование программного обеспечения

С.9.1 Общие положения о подтверждении соответствия

Перед написанием тестов важно создать стратегию тестирования в его плане. Эта стратегия определяет подход, цели, которые устанавливаются в терминах тестового охвата, окружающую среду и конкретные используемые методы, применяемые критерии успеха выполнения теста и т.д.

Цели тестов должны быть адаптированы к типу программного обеспечения и к конкретным факторам. Эти факторы определяют типы осуществляемых тестов: функциональные, испытание в предельных условиях, запредельные тесты, тесты производительности, нагрузочные, внешние тесты отказа оборудования, тесты конфигурации, а также круг объектов, которые должны быть охвачены тестами (тесты режима функционирования, связанной с безопасностью функции управления, для каждого элемента в спецификации и т. д.).

Верификация новой версии программного обеспечения должна включать в себя тесты стабильности.

Примечание — Тесты стабильности используются для того, чтобы изменения, выполняемые в программном обеспечении, не изменяли поведение программного обеспечения любым неожиданным образом.

С.9.2 Верификация спецификации программного обеспечения. Тесты подтверждения соответствия

Целью этих верификаций является выявление ошибок, связанных с программным обеспечением, в окружении целевой системы. Ошибки, обнаруженные этим типом верификации, включают в себя: любые некорректности при обработке прерываний, недостаточный учет требований для времени выполнения, неправильную реакцию программного обеспечения, работающего в неустановившемся режиме (пуск, входной поток, переключение в режим с сокращенными возможностями и т. д.), конфликты доступа к различным ресурсам или организационные проблемы в памяти, неспособность комплексных испытаний для обнаружения неисправностей, ошибки интерфейса программного обеспечения / аппаратных средств, переполнение стека. Тесты подтверждения соответствия — основные компоненты для верификации спецификации программного обеспечения.

Тестовый охват должен быть выполнен строго в соответствии с матрицей трассируемости и гарантировать, что:

- каждый элемент спецификации, включая механизмы обеспечения безопасности, охвачен тестом подтверждения соответствия;

- поведение программного обеспечения может быть верифицировано в любом режиме работы в реальном времени.

Кроме того, подтверждение соответствия нужно проводить в типичных условиях, в которых эксплуатируется СБЭСУ или подсистема СБЭСУ.

Примечание — Это гарантирует, что программа выполняется так, как и предполагалось при эксплуатации. Это относится только к случаям, когда условия испытания могут требовать разрушения элементов оборудования (например, физическая неисправность компонента, которая не может быть смоделирована). Подтверждение соответствия должно проводиться в условиях эксплуатации СБЭСУ или СБЭСУ подсистемы (т. е. с окончательными версиями программного обеспечения и аппаратных средств, а также программного обеспечения, установленного в целевой системе). Любая другая комбинация может привести к снижению эффективности теста и требует анализа его представления.

Результаты подтверждения соответствия следует записать в отчет о подтверждении соответствия, который должен содержать по крайней мере следующие моменты:

- версии программного обеспечения и системы, для которых была выполнена процедура подтверждения соответствия;
- описание выполненных тестов подтверждения соответствия (входы, выходы, процедуры тестирования);
- инструментальные средства и оборудование, используемые для подтверждения соответствия или оценки результатов;
- результаты, показывающие, является ли каждый тест подтверждения соответствия успешным или неудачным;
- оценка подтверждения соответствия: выявленные несоответствия, влияние на безопасность, решение о том, что программное обеспечение прошло подтверждение соответствия или нет.

Отчет о подтверждении соответствия должен быть доступен для каждой версии поставляемого программного обеспечения и содержать соответствующую информацию об окончательной версии каждого элемента поставляемого программного обеспечения.

Примечание — Данный отчет может быть использован для предоставления доказательств того, что испытания действительно были выполнены и результаты были правильными (или содержат объяснимые отклонения). Он также может быть использован для повторения испытаний в более поздние сроки для будущей версии программного обеспечения или для другого проекта. Это дает гарантию, что каждая поставляемая версия завершена и прошла подтверждение соответствия. С другой стороны, не предполагается полное подтверждение соответствия каждой модификации существующего кода — в некоторых случаях анализ влияния может частично обосновать подтверждение соответствия.

С.9.3 Верификация проекта программного обеспечения. Тесты интеграции программного обеспечения

Данная верификация нацелена на обеспечение корректности комплекса программных модулей и отношений между программными компонентами. Она может быть использована для выявления ошибок следующего вида: неправильная инициализация переменных и констант, ошибки в передаче параметров, любые изменения данных, особенно глобальных данных, неправильная последовательность событий и операций.

Тесты интеграции программного обеспечения должны проверять:

- последовательность выполнения программ;
- обмен данными между модулями;
- соблюдение критериев эффективности;
- неизменность глобальных данных.

Тестовый охват должен быть выполнен строго в соответствии с матрицей трассируемости и демонстрировать, что соответствие между выполняемыми тестами и целями испытаний определено.

Результаты тестирования интеграции необходимо записать в отчете о тестировании интеграции программного обеспечения, который должен как минимум содержать следующие пункты:

- версию интегрированного программного обеспечения;
- описание проведенных испытаний (входы, выходы, процедуры);
- результаты тестов интеграции и их оценку.

С.9.4 Верификация детального проектирования. Тесты модуля

Тесты модуля предназначены для проверки модулей программного обеспечения и их соответствия с деталями проекта. Эти действия могут быть необходимы для больших и сложных элементов программного обеспечения, но рекомендуются только для относительно небольших элементов программного обеспечения, рассматриваемых в настоящем стандарте. Эта стадия процедуры верификации позволяет выявить следующие виды ошибок:

- неспособность алгоритма удовлетворять спецификации программного обеспечения;
- некорректность выполнения циклических операций;
- некорректность выполнения логического выбора;
- неспособность верно вычислить правильные комбинации входных данных;
- некорректный результат в случае пропуска или изменения входных данных;
- нарушение границ массива;

- неправильная последовательность расчетов;
- недостаточная точность;
- некорректность и неэффективность алгоритма.

Для каждого программного модуля должна быть определена серия тестов, чтобы проверить использование входных данных, выполнение модулем функций, указанных на стадии детального проектирования.

Тестовый охват необходимо представить матрицей трассируемости, которая демонстрирует соответствие между результатами тестирования и целями заданных тестов.

Приложение D
(справочное)

Методология оценки чувствительности к отказам по общей причине (ООП)

D.1 Общие положения

В данном приложении представлен простой качественный подход для оценки ООП, который может быть применен к проектированию подсистемы.

D.2 Методология

Предложенный проект подсистемы необходимо оценить, чтобы установить эффективность мер, примененных для защиты от ООП. Из таблицы D.1 должны быть определены примененные для конкретного случая меры и установлена общая оценка, которая используется для определения фактора ООП из таблицы D.2 (в процентах).

Таблица D.1 — Критерии оценки ООП

Мера	Ссылка	Оценка
Разделение/выделение		
Проложены ли везде в СБЭСУ разные сигнальные кабели по разным каналам или достаточно ли они экранированы?	1a	5
Где используется информация кодирования/декодирования, достаточно ли ее для обнаружения ошибок передачи сигнала?	1b	10
Все ли сигнальные и силовые кабели в СБЭСУ отделены друг от друга или достаточно ли они экранированы?	2	5
Если элементы подсистемы могут способствовать ООП, то распределены ли реализующие их физические устройства по отдельным корпусам?	3	5
Диверсификация/избыточность		
Реализованы ли в подсистемах различные электрические технологии, например, одна подсистема электронная или программируемая электронная, а другая использует электромеханические реле?	4	8
Применяются ли в подсистеме устройства, реализованные на различных физических принципах (например, датчики защитной дверцы, которые используют механические и магнитные методы измерения)?	5	10
Применяются ли в подсистеме элементы с различным временем выполнения функций и/или видов отказов?	6	10
Есть ли элементы в подсистеме, которые имеют интервал диагностических проверок ≤ 1 мин?	7	10
Сложность/конструкция/применение		
Предотвращает ли перекрестная связь между каналами обмен любой информацией, кроме используемой для диагностического тестирования?	8	2
Оценка/анализ		
Были ли изучены результаты анализа видов и влияния отказов для того, чтобы установить источники отказов по общей причине, и устранены ли при проектировании предварительно известные источники отказов по общей причине?	9	9
Все ли возможные отказы были полностью проанализированы и учтены в проекте?	10	9
Компетентность/обучение		
Понимают ли разработчики подсистемы причины и последствия отказов по общей причине?	11	4

Окончание таблицы D.1

Мера	Ссылка	Оценка
Контроль состояния окружающей среды		
Возможно ли, что элементы подсистемы будут работать в заданных диапазонах температуры, влажности, коррозии, пыли, вибрации и т. д., в которых их работа была проверена, без использования внешнего контроля состояния окружающей среды?	12	9
Устойчива ли подсистема к неблагоприятным воздействиям электромагнитного излучения в пределах (и включая их), указанных в МЭК 61326-3-1.	13	9
Примечание — В таблице D.1 приведены альтернативные меры (например, 1a и 1b), при этом предполагается, что претендовать на вклад в предотвращение ООП может только наиболее подходящая из них.		

Необходимо выбрать те меры таблицы D.1, которые, по предположению, оказывают влияние на проект подсистемы, затем сложить соответствующие им значения оценок, чтобы получить общую оценку для реализуемого проекта. Если можно показать, что эквивалентный эффект по предотвращению ООП может быть достигнут за счет применения конкретных мер при проектировании (например, использование оптически изолированных устройств, вместо экранированных кабелей), то для этой меры может быть заявлена соответствующая оценка и можно считать, что она вносит такой же вклад в предотвращение ООП.

Эта общая оценка может быть использована для определения с помощью таблицы D.2 фактора отказов по общей причине (β).

Таблица D.2 — Оценка фактора ООП (β)

Общая оценка	Фактор отказов по общей причине (β)
< 35	10 % (0,1)
35–65	5 % (0,05)
65–85	2 % (0,02)
85–100	1 % (0,01)

Полученное значение β следует использовать при оценке вероятности опасного отказа в соответствии с требованиями 6.7.8.1.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60204-1	IDT	ГОСТ Р МЭК 60204-1—2007 «Безопасность машин. Электрооборудование машин и механизмов. Часть 1. Общие требования»
МЭК 61000-6-1	MOD	ГОСТ 30804.6.1—2013 «Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых в жилых, коммерческих зонах и производственных зонах с малым энергопотреблением. Требования и методы испытаний»
МЭК 61000-6-2	MOD	ГОСТ Р 51317.6.2—2007 «Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых в промышленных зонах. Требования и методы испытаний»
МЭК 61000-4	—	*
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898—2002 «Аспекты безопасности. Правила включения в стандарты»
МЭК 61131-3:2003	—	*
МЭК 61310 (все части)	—	*
ИСО/МЭК Руководство 51:1990	IDT	ГОСТ Р 51898—2002 «Аспекты безопасности. Правила включения в стандарты»
МЭК 61326-1:2005	MOD	ГОСТ Р 51522.1—2011 «Совместимость технических средств электромагнитная. Электрическое оборудование для измерения, управления и лабораторного применения. Часть 1. Общие требования и методы испытаний»
МЭК 61508-1:2010	IDT	ГОСТ Р МЭК 61508-1—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
МЭК 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
МЭК 61508-3:2010	IDT	ГОСТ Р МЭК 61508-3—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению»
МЭК 61508-4:2010	IDT	ГОСТ Р МЭК 61508-4—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
МЭК 61508-5:2010	IDT	ГОСТ Р МЭК 61508-5—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности»
МЭК 61508-7:2010	IDT	ГОСТ Р МЭК 61508-7—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 61511-1:2003	IDT	ГОСТ Р МЭК 61511-1—2011 «Безопасность функциональная. Системы безопасности приборные для промышленных процессов. Часть 1. Термины, определения и технические требования»
МЭК 61784-3-3:2007	—	*
ИСО 12100:2010	MOD	ГОСТ Р 54125—2010 «Безопасность машин и оборудования. Принципы обеспечения безопасности при проектировании»
ИСО 13849-1:1999	IDT	ГОСТ Р ИСО 13849-1—2003 «Безопасность оборудования. Элементы систем управления, связанные с безопасностью. Часть 1. Общие принципы конструирования»
ИСО 13849-2:2003	—	*
ИСО 14121	—	*

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

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

УДК 621.5:814.8:006.354	ОКС 13.110, 25.040.99, 29.020	Т51	IDT

Ключевые слова: безопасность функциональная; безопасность оборудования, системы управления электрические, электронные и программируемые электронные, функциональная безопасность электронных систем управления оборудованием; требования

Технический редактор *В.Н. Прусакова*
Корректор *Г.В. Яковлева*
Компьютерная верстка *Ю.В. Половой*

Сдано в набор 09.11.2015. Подписано в печать 25.02.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 8,84. Уч.-изд. л. 7,86. Тираж 33 экз. Зак. 573.

Набрано в ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
www.jurisizdat.ru y book@mail.ru

Издано и отпечатано во
ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www gostinfo.ru info@gostinfo.ru