ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 60987— 2024

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ СТАНЦИЙ

Требования к аппаратным средствам

(IEC 60987:2021, Nuclear power plants — Instrumentation and control important to safety — Hardware requirements, IDT)

Издание официальное

Москва
Российский институт стандартизации
2024

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Русатом Автоматизированные системы управления» (АО «РАСУ») на основе перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 322 «Атомная техника»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 июля 2024 г. № 956-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 60987:2021 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Требования к техническим средствам» (IEC 60987:2021 «Nuclear power plants — Instrumentation and control important to safety — Hardware requirements», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

Дополнительная информация, выделенная курсивом, приведена в сносках для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Положения настоящего стандарта действуют в целом в отношении атомных станций, сооружаемых по российским проектам за пределами Российской Федерации.

Положения настоящего стандарта могут применяться в отношении атомных станций, сооружаемых или модернизируемых в Российской Федерации в частях, не противоречащих требованиям федеральных норм и правил, действующим в области использования атомной энергии

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

Содержание

Введение

a) Техническая справка, основные вопросы и организация настоящего стандарта

Настоящий стандарт описывает требования к аппаратным средствам (материальной части) Э/Э/ПЭ-элементов в составе систем контроля и управления, обеспечивающих функции безопасности в соответствии с определением по МЭК 61226.

Настоящий стандарт взаимосвязан с МЭК 61513 и дополняет его. Мероприятия, относящиеся преимущественно к системному уровню (например, комплексирование систем, валидация и монтаж), в настоящем стандарте подробно не рассматриваются. Требования, которые не относятся непосредственно к аппаратным средствам, установлены в МЭК 61513.

Основные принципы проектирования контрольно-измерительных приборов для атомной промышленности, применяемых в системах, важных для безопасности атомных станций, были впервые изложены в стандартах атомной отрасли применительно к аппаратным системам, а именно в Руководстве по безопасности МАГАТЭ 50 SG D3, которое впоследствии было заменено на Руководство МАГАТЭ SSG-39.

МЭК 60987 был впервые издан в 1989 году для рассмотрения аспектов, связанных с аппаратными средствами, при проектировании цифровых систем в составе систем, важных для безопасности.

Несмотря на то, что многие требования, изложенные в первом издании, по-прежнему остаются актуальными, существовали серьезные причины, сделавшие необходимой разработку настоящего пересмотренного издания МЭК 60987, в том числе:

- использование различных технологий, включающих традиционное аппаратное оборудование[1)], программируемое цифровое оборудование или комбинацию указанных двух типов оборудования;
- введение в действие МЭК 61226 и МЭК 61513, распространяющихся на СКУ, выполняющие функции трех различных категорий (A, B и C), и системы трех разных классов (классы 1, 2 и 3);
- использование разработанных ранее компонентов, значительно выросшее по сравнению с уникальными разработками.

b) Положение настоящего стандарта в структуре серии стандартов подкомитета МЭК ПК 45А

В серии стандартов подкомитета ПК 45А МЭК документом верхнего уровня на СКУ, важные для безопасности атомных станций (АС), является МЭК 61513. МЭК 60987 является стандартом второго уровня серии стандартов подкомитета ПК 45А МЭК, рассматривающим общие вопросы, связанные с требованиями к аппаратным средствам СКУ.

МЭК 60880 и МЭК 62138 являются стандартами второго уровня, которые вместе охватывают аспекты, связанные с программным обеспечением компьютерных систем, используемых для выполнения важных для безопасности АС функций. МЭК 60880 и МЭК 62138 напрямую ссылаются на IEC 60987 в части требований к аппаратным средствам СКУ.

МЭК 62566 и МЭК 62566-2 являются стандартами второго уровня, которые вместе охватывают вопросы разработки HDL-программируемых устройств, используемых для выполнения важных для безопасности АС функций. МЭК 62566 и МЭК 62566-2 напрямую ссылаются на МЭК 60987 в части требований к аппаратным средствам СКУ.

В МЭК 60987 приводятся ссылки на требования IEC/IEEE 60780-323 в части квалификации оборудования.

Более подробное описание структуры серии стандартов ПК 45А МЭК приведено в пункте d).

c) Рекомендации и ограничения, касающиеся применения настоящего стандарта

Настоящий стандарт не устанавливает дополнительных функциональных требований к классифицируемым по безопасности системам (требования к классификации систем см. в МЭК 61226).

Аспекты, по которым разработаны специальные рекомендации (с тем, чтобы обеспечить изготовление высоконадежных систем), включают:

- общий подход к жизненному циклу безопасности аппаратных средств;
- продвижение от спецификации требований к эксплуатации и техническому обслуживанию на площадке.

[1)] *Традиционное аппаратное оборудование — оборудование, реализованное с использованием электронных компонентов, изготовленных с использованием только аналоговых элементов (транзисторов, резисторов и т. п.), без применения микропроцессорных программируемых устройств.*

Технологии СКУ продолжают совершенствоваться, в связи с чем невозможно включить в такой документ, как настоящий стандарт, ссылки на все современные технологии и методики проектирования. Для гарантии того, что настоящий стандарт останется актуальным в будущем, особое внимание уделено принципиальным вопросам, а не конкретным технологиям проектирования аппаратных средств. В случае разработки новых методик проектирования можно оценить пригодность таких методик путем адаптации и применения принципов проектирования, изложенных в настоящем стандарте.

Область применения настоящего стандарта включает аппаратные средства СКУ для систем всех классов, важных для безопасности. Сюда относятся традиционное аппаратное оборудование, программируемое цифровое оборудование или комбинации обоих типов оборудования. В данном стандарте рассматриваются оценка и использование ранее разработанных изделий, например коммерческих продуктов серийного производства (COTS), а также разработка новых аппаратных средств.

Настоящий стандарт не рассматривает непосредственно проблему защиты систем от угроз, возникающих в связи со злонамеренными атаками, например кибербезопасность для программируемых цифровых элементов. МЭК 62645 устанавливает требования к программам обеспечения безопасности для программируемых цифровых элементов на всех этапах их разработки и эксплуатации на площадке.

d) Описание структуры серии стандартов подкомитета МЭК ПК 45А и их взаимосвязи с другими документами МЭК и документами других организаций (МАГАТЭ, ИСО)

Стандартами самого высокого уровня серии стандартов ПК 45А МЭК являются МЭК 61513 и МЭК 63046. МЭК 61513 содержит общие требования к СКУ и оборудованию, используемым для выполнения важных для безопасности АС функций. МЭК 63046 содержит общие требования к электроэнергетическим системам АС и распространяется на системы электроснабжения, включая системы питания СКУ. МЭК 61513 и МЭК 63046 следует рассматривать вместе и на одном уровне. МЭК 61513 и МЭК 63046 формируют структуру серии стандартов ПК 45А МЭК и создают законченную концепцию, определяющую общие требования к системам контроля и управления и к электротехническим системам атомных станций.

МЭК 61513 и МЭК 63046 содержат прямые ссылки на другие стандарты ПК 45А МЭК по общим вопросам, связанным с категоризацией функций и классификацией систем, квалификацией, разделением, защитой от отказов по общим причинам, проектированием пунктов управления, электромагнитной совместимостью, кибербезопасностью, программными и аппаратными аспектами программируемых цифровых систем, согласованием требований безопасности и защиты информации и управлением старением. Стандарты, на которые напрямую ссылаются МЭК 61513 и МЭК 63046, являющиеся стандартами второго уровня, следует рассматривать вместе с МЭК 61513 и МЭК 63046, как единый комплект документов.

Третий уровень стандартов ПК 45А МЭК составляют стандарты, на которые отсутствуют прямые ссылки в МЭК 61513 или МЭК 63046, относящиеся к конкретному оборудованию, техническим методам или определенным видам деятельности. Как правило, эти стандарты, содержащие ссылки на стандарты второго уровня по общим темам, могут быть использованы самостоятельно.

Четвертый уровень документов ПК 45А МЭК представлен техническими отчетами, которые не являются нормативными документами.

Серия стандартов ПК 45А МЭК последовательно реализует и детализирует принципы безопасности и защиты информации, а также базовые аспекты, содержащиеся в соответствующих стандартах безопасности МАГАТЭ и соответствующей серии документов МАГАТЭ по ядерной безопасности (NSS). В частности, к этим документам относятся нормы безопасности МАГАТЭ SSR-2/1, устанавливающие требования безопасности, связанные с проектированием АС, Руководство по безопасности МАГАТЭ SSG-30, в котором рассмотрена классификация безопасности конструкций, систем и компонентов АС, Руководство по безопасности МАГАТЭ SSG-39, относящееся к проектированию систем контроля и управления АС, Руководство по безопасности МАГАТЭ SSG-34, рассматривающее проектирование электроэнергетических систем для АС, а также внедряемое руководство NSS17 по компьютерной безопасности оборудования атомных станций. Термины и определения, используемые в стандартах ПК 45А по безопасности и защите информации, соответствуют терминам и определениям, используемым в документах МАГАТЭ.

МЭК 61513 и МЭК 63046 представлены в том же формате, что и основной стандарт по безопасности МЭК 61508, с той же схемой жизненного цикла в целом и схемой жизненного цикла системы. В отношении ядерной безопасности МЭК 61513 и МЭК 63046 содержат толкование основных требований, действующих в атомной энергетике и изложенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4. В этой

структуре МЭК 60880, МЭК 62138 и МЭК 62566 соответствуют МЭК 61508-3 для атомной энергетики. МЭК 61513 и МЭК 63046 содержат ссылки на документы ИСО, а также на документы МАГАТЭ GS-R, часть 2, МАГАТЭ GS-G-3.1 и МАГАТЭ GS-G-3.5 по вопросам, связанным с обеспечением качества (ОК). На втором уровне по вопросам ядерной безопасности вводным документом для серии стандартов по безопасности ПК 45А МЭК является МЭК 62645. Он основан на действующих принципах высокого уровня и главных концепциях стандартов по безопасности, в частности ИСО/МЭК 27001 и ИСО/МЭК 27002. МЭК 62645 адаптирует и дополняет их применительно к атомной отрасли и приводит в соответствие с серией стандартов МЭК 62443. По пунктам управления на втором уровне первичным документом для стандартов ПК 45А МЭК является МЭК 60964, а по вопросам управления старением — МЭК 62342.

Примечание — Предполагается, что при проектировании систем контроля и управления АС, реализующих стандартные функции безопасности (например, обеспечение безопасности работников, защита объекта, химическая безопасность, энергетическая безопасность технологических процессов), будут применяться международные или национальные стандарты.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ СТАНЦИЙ

Требования к аппаратным средствам

Instrumentation and control important to safety of nuclear power plants. Hardware requirements

Дата введения — 2024—11—01

1 Область применения

Системы контроля и управления (СКУ), важные для безопасности, могут быть реализованы с использованием традиционных аппаратных средств, программируемого цифрового оборудования или с использованием комбинации обоих типов оборудования.

В настоящем стандарте содержатся требования и рекомендации по аспектам, связанным с аппаратными средствами СКУ, вне зависимости от используемой технологии. Стандарт применим к системам всех классов безопасности с учетом дифференцированного подхода (в соответствии с МЭК 61513).

Требования, установленные в настоящем стандарте, распространяются, в частности, на выбор ранее разработанных компонентов, на аспекты, связанные с техническими средствами, определяющие рабочий проект системы и его реализацию, а также на изготовление оборудования.

Настоящий стандарт не рассматривает обеспечение защиты систем от угроз, возникающих в связи со злонамеренными атаками, например кибербезопасность для программируемых цифровых элементов. Требования к программам обеспечения безопасности программируемых цифровых элементов на всех этапах разработки и эксплуатации на площадке установлены в МЭК 62645.

Ранее разработанные элементы могут представлять собой микроконтроллеры или HPD и при наличии у них встроенного ПО или программных файлов должны быть «прозрачны» для пользователя. В таких случаях настоящий стандарт может быть использован в качестве руководства при организации процесса оценки таких компонентов. Примером того, где такой подход может считаться уместным, является оценка современных процессоров, содержащих набор микрокодов. Такой код является обычно неотъемлемой частью «аппаратного средства», в связи с чем будет уместным проводить оценку процессора (включая набор микрокодов) как единого аппаратного компонента, используя настоящий стандарт.

ПО, не встроенное в аппаратные средства системы, разрабатывают или оценивают согласно требованиям соответствующего стандарта на ПО (например, МЭК 60880 для систем класса 1 и МЭК 62138 для систем классов 2 и 3).

Аналогичным образом разработку или оценку невстроенных HDL-программируемых устройств осуществляют в соответствии с требованиями стандарта, применимого для данного HPD (например, МЭК 62566 для систем класса 1 и МЭК 62566-2 для систем классов 2 и 3).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения)]:

IEC/IEEE 60780-323, Nuclear facilities — Electrical equipment important to safety — Qualification (Объекты использования атомной энергии. Электрическое оборудование, важное для безопасности. Квалификация)

Издание официальное

IEC 60812, Failure modes and effects analysis (FMEA and FMECA) [Анализ видов и последствий отказов (FMEA и FMECA)]

IEC 60880, Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А)

IEC/IEEE 60980-344, Nuclear facilities — Equipment important to safety — Seismic qualification (Объекты использования атомной энергии. Оборудование, важное для безопасности. Сейсмическая квалификация)

IEC 61000 (all parts), Electromagnetic compatibility (EMC) [Электромагнитная совместимость (ЭМС)]

IEC 61025, Fault tree analysis (FTA) [Анализ дерева отказов (FTA)]

IEC 61513:2011, Nuclear power plants — Instrumentation and control important to safety — General requirements for systems (Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования)

IEC 61709, Electrical components — Reliability — Reference conditions for failure rates and stress models for conversion (Электрические компоненты. Надежность. Стандартные условия для частоты отказов и прочностные модели для преобразования)

IEC 62003, Nuclear power plants — Instrumentation, control and electrical power systems — Requirements for electromagnetic compatibility testing (Атомные станции. Системы контроля, управления и электроэнергетические системы. Требования для испытаний на электромагнитную совместимость)

IEC 62138:2018, Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category B or C functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С)

IEC 62566:2012, Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Разработка HDL-программируемых интегральных схем для систем, выполняющих функции категории А)

IEC 62566-2, Nuclear power plants — Instrumentation and control systems important to safety — Development of HDL-programmed integrated circuits — Part 2: HDL-programmed integrated circuits for systems performing category B or C functions (Атомные станции. Системы контроля и управления, важные для безопасности. Разработка HDL-программируемых интегральных схем. Часть 2. HDL-программируемые интегральные схемы для систем, выполняющих функции категорий В или С)

ISO 28590, Sampling procedures for inspection by attributes — Introduction to the ISO 2859 series of standards for sampling for inspection by attributes (Процедуры выборочного контроля по качественным признакам. Введение в стандарты серии ISO 2859 по процедурам выборочного контроля по качественным признакам)

IPC-A-610, Acceptability of Electronic Assemblies (Приемлемость электронных сборок)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **класс СКУ** (class of an I&C system): Одно из трех возможных обозначений (1, 2, 3) СКУ, важных для безопасности, присваиваемое в результате рассмотрения требований, предъявляемых к выполнению СКУ функций, имеющих разное значение для безопасности.

Примечания

1 Если СКУ не выполняет функции, важные для безопасности, то ее не классифицируют.

2 См. также термины «категория функции СКУ», «элементы, важные для безопасности», «системы безопасности».

[МЭК 61513:2011, 3.6, измененный — последнее предложение определения вынесено в примечание 1]

3.2 **отказ по общей причине;** ООП (common cause failure, CCF): Отказ двух или более устройств, систем или компонентов вследствие единичного конкретного события или по одной конкретной причине[1)].

Примечание — Общие причины могут быть внутренними или внешними по отношению к СКУ.

[Глоссарий МАГАТЭ по вопросам безопасности, 2018, измененный — добавлено примечание]

3.3 **компонент** (component): Одна из составных частей системы.

Примечания

1 Компонент может быть аппаратным, программным или HDL-программируемым и может подразделяться на другие компоненты.

2 Также см. термины «СКУ», «оборудование».

3 Термины «оборудование», «компонент» и «модуль» часто являются взаимозаменяемыми. Взаимоотношение между данными терминами пока не стандартизовано.

4 Настоящее определение ПК 45А МЭК сопоставимо с дополнительным определением термина «Компонент», приведенным в Глоссарии МАГАТЭ по вопросам безопасности 2018 г. в составе статьи «Структуры, Системы и Компоненты (ССК)». Тем не менее, поскольку в указанной статье в качестве примеров компонентов приведены только аппаратные средства, это может ввести читателя в заблуждение, в связи с чем ПК 45А МЭК предпочитает использовать определение, явным образом распространяющееся и на программные компоненты.

[МЭК 61513:2011, 3.10, измененный — последнее предложение определения вынесено в примечание 1; определение, приведенное в Глоссарии МАГАТЭ по вопросам безопасности 2007 г., изменено для издания 2018 г.]

3.4 **компьютерный элемент** (computer-based item): Элемент, действие которого зависит от программных команд, выполняемых микропроцессорами или микроконтроллерами.

Примечания

1 В данном термине и его определении слово «элемент» может быть заменено словами: система, оборудование или устройство.

2 Компьютерный элемент — это разновидность программируемого цифрового элемента.

3 Этот термин эквивалентен термину «программный элемент».

4 Определения терминов: Э/Э/ПЭ-элемент, электрический элемент, СКУ, программируемый цифровой элемент, компьютерный элемент, аппаратный элемент, программируемое логическое устройство, HDL-программируемое устройство — должны рассматриваться в связи друг с другом, так как они являются полностью согласованными и внутренне непротиворечивыми. Они также не противоречат и полностью взаимосвязаны с общими требованиями, установленными МЭК 61513 и МЭК 63046 к системам контроля и управления и электроэнергетическим системам атомных станций.

[МЭК 62138:2018, 3.8, измененный — добавлено примечание 4]

3.5 **электрический/электронный/программируемый электронный элемент;** Э/Э/ПЭ элемент (electrical/electronic/programmable electronic item, E/E/PE item): Элемент, основанный на электрической (Э), и/или электронной (Э), и/или программируемой электронной (ПЭ) технологии.

Примечания

1 В данном термине и его определении слово «элемент» может быть заменено словами: система, оборудование или устройство.

2 Определения терминов: Э/Э/ПЭ элемент, электрический элемент, СКУ, программируемый цифровой элемент, компьютерный элемент, аппаратный элемент, программируемое логическое устройство, HDL-программируемое устройство — должны рассматриваться в связи друг с другом, так как они являются полностью согласованными и внутренне непротиворечивыми. Они также не противоречат и полностью взаимосвязаны с общими требованиями, установленными МЭК 61513 и МЭК 63046 к системам контроля и управления и электроэнергетическим системам атомных станций.

[МЭК 62138:2018, 3.15, измененный — добавлено примечание 2]

3.6 **система энергоснабжения;** СЭ (electrical power system, EPS): Система, осуществляющая генерацию, передачу и распределение электроэнергии, выполняющая функцию питания для работы оборудования АС (насосов, клапанов, подогревателей и др.).

---

1) *Согласно НП-001-15, приложение № 2, пункт 46: «Отказы по общей причине — отказы систем (элементов), возникающие вследствие одного отказа или ошибки персонала, или внутреннего или внешнего воздействия (события), или иной причины».*

Примечание — Электрическая система может включать Э/Э/ПЭ-элементы для выполнения своего внутреннего электрического управления и защиты.

[МЭК 63046:2020, 3.12]

3.7 **оборудование** (equipment): Одна или более частей системы.

Примечания

1 Элемент оборудования — отдельно определяемый (и обычно съемный) элемент или часть системы.

2 См. также термины «компонент», «СКУ».

3 Оборудование может включать в себя программное обеспечение.

4 Термины «оборудование», «компонент» и «модуль» часто являются взаимозаменяемыми. Соотношение между данными терминами пока не стандартизовано.

[МЭК 61513:2011, 3.16, измененный — последнее предложение определения вынесено в примечание 1, а примечание 4 МЭК 61513 удалено]

3.8 **аппаратно-программное обеспечение** (firmware): Программное обеспечение, тесно связанное с характеристиками аппаратного средства, в которое его устанавливают.

Примечания

1 Наличие аппаратно-программного обеспечения обычно «прозрачно» для пользователя компонента аппаратных средств и может рассматриваться фактически как неотъемлемая часть конструкции аппаратных средств (хорошим примером такого программного обеспечения является микрокод процессора).

2 В общем аппаратно-программное обеспечение может быть изменено пользователем только путем замены компонентов аппаратных средств (например, микросхемы процессора, платы, перепрограммируемого постоянного запоминающего устройства), включающих данное ПО, на компоненты, содержащие модифицированное ПО (аппаратно-программное обеспечение). В таком случае управление конфигурацией компонентов аппаратных средств пользователями оборудования фактически обеспечивает управление конфигурацией аппаратно-программного обеспечения. Как следует из настоящего стандарта, аппаратно-программное обеспечение по сути является программным обеспечением (ПО), встроенным в аппаратное средство.

3.9 **функция** (function): Конкретная цель или задача, которая должна быть достигнута и которую можно определить или описать без привязки к физическим средствам ее достижения.

[Глоссарий МАГАТЭ по вопросам безопасности, 2018]

3.10 **аппаратный элемент** (hardwired item): Элемент, созданный на основе реле, аналоговых электронных или дискретных цифровых логических схем.

Примечания

1 В данном термине и его определении слово «элемент» может быть заменено словами: система, оборудование или устройство.

2 Этот термин, используемый ПК 45А МЭК, приблизительно эквивалентен «электронному элементу», используемому в МЭК 61508. Реле представляют собой электромеханические, а не электронные элементы, но их относят к термину «аппаратный элемент».

3 Аппаратные элементы также принято называть «традиционными элементами».

4 Определения терминов: Э/Э/ПЭ элемент, электрический элемент, СКУ, программируемый цифровой элемент, компьютерный элемент, аппаратный элемент, программируемое логическое устройство, HDL-программируемое устройство — должны рассматриваться в связи друг с другом, так как они являются полностью согласованными и внутренне непротиворечивыми. Они также не противоречат и полностью взаимосвязаны с общими требованиями, установленными МЭК 61513 и МЭК 63046 к системам контроля и управления и электроэнергетическим системам атомных станций.

3.11 **язык описания аппаратных средств;** HDL (Hardware Description Language, HDL): Язык, используемый для формального описания функций и/или структуры электронного компонента для ведения документации, моделирования или синтеза.

Примечание — Наиболее широко используемыми HDL являются VHDL (IEEE 1076) и Verilog (IEEE 1364).

[МЭК 62566:2012, 3.6]

3.12 **HDL-программируемое устройство;** HPD (HDL-Programmed Device, HPD): Интегральная микросхема, конфигурированная с использованием языков описания аппаратных средств и соответствующих программных средств.

Примечания

1 Языки описания аппаратных средств и сопутствующие инструменты (например, средство моделирования, синтезирующее устройство) используют для реализации требований к надлежащей сборке предварительно разработанных микроэлектронных ресурсов.

2 При разработке HPD могут использоваться предварительно разработанные блоки.

3 HPD, как правило, основаны на заготовках ПЛИС или подобных микроэлектронных технологиях.

4 HPD является разновидностью программируемого цифрового элемента.

5 Определения терминов: Э/Э/ПЭ элемент, электрический элемент, СКУ, программируемый цифровой элемент, компьютерный элемент, аппаратный элемент, программируемое логическое устройство, HDL-программируемое устройство — должны рассматриваться в связи друг с другом, так как они являются полностью согласованными и внутренне непротиворечивыми. Они также не противоречат и полностью взаимосвязаны с общими требованиями, установленными МЭК 61513 и МЭК 63046 к системам контроля и управления и электроэнергетическим системам атомных станций.

[МЭК 62566:2012, 3.7, измененный — добавлены примечания 4 и 5]

3.13 **система контроля и управления;** СКУ (I&C system): Система, основанная на применении электрической, и/или электронной, и/или программируемой электронной технологии, выполняющая функции контроля и управления, а также функции обслуживания и наблюдения, связанные с эксплуатацией самой системы.

Примечания

1 Этот термин используется как общий, включающий в себя все элементы системы, такие как внутренние источники электроснабжения, датчики и другие устройства ввода данных, магистрали передачи данных и другие каналы связи, интерфейсы с исполнительными механизмами и прочими устройствами вывода. Различные функции внутри системы могут использовать специальные или общие ресурсы.

2 См. также «система, функция контроля и управления».

3 Элементы, включенные в конкретную СКУ, определены в спецификации границ системы.

4 В соответствии со стандартным функционалом МАГАТЭ подразделяет СКУ на системы автоматизации/управления, системы человеко-машинного интерфейса (ЧМИ), системы блокировки и системы защиты.

[МЭК 61513:2011, 3.29, измененный — последнее предложение определения вынесено в примечание 1]

3.14 **интеграция** (integration): Последовательная сборка компонентов и их проверка внутри завершенной системы.

[МЭК 62138:2018, 3.27]

3.15 **периодические испытания** (periodic testing): Проведение испытаний в заданные промежутки времени для подтверждения того, что функциональные возможности систем и оборудования СКУ, важных для безопасности, сохраняются на необходимом уровне, и параметры, учитываемые в анализе безопасности, находятся в удовлетворительных пределах.

[МЭК 60671:2007, 3.7]

3.16 **ранее разработанные элементы** (pre-existing items): Аппаратные средства, жестко вмонтированные элементы аппаратных средств или программируемые цифровые элементы, которые уже существуют как коммерчески доступное или запатентованное изделие, доступное для применения.

Примечания

1 Данное определение также включает ранее разработанное программное обеспечение (ПО) или HDL (см. МЭК 60880, МЭК 62138, МЭК 62566 и МЭК 62566-2).

2 Ранее разработанные элементы могут быть коммерческими продуктами массового производства (также называемыми «COTS») или изделиями, защищенными правами интеллектуальной собственности, утилизированными изготовителем (см. МЭК 61513:2011, 6.2.3.2).

[МЭК 61513:2011, 3.36, измененный — определение и примечания к терминам изменены таким образом, чтобы включить электрический, электронный, программируемый электронный элементы и коммерческий продукт массового производства]

3.17 **программируемый цифровой элемент** (programmable digital item): Элемент для выполнения функции, основанный на программных инструкциях или программируемой логике.

Примечания

1 В данном случае термин «элемент» может быть заменен на термины «система», «оборудование» или «устройство».

2 К основным видам программируемых цифровых элементов относятся компьютерные элементы и элементы программируемой логики.

3 Данный термин, используемый МЭК ПК 45А, является эквивалентом термина «программируемый электронный элемент» (ПЭ элемент), определяемого согласно МЭК 61508.

4 Определения терминов: Э/Э/ПЭ элемент, электрический элемент, СКУ, программируемый цифровой элемент, компьютерный элемент, аппаратный элемент, программируемое логическое устройство, HDL-програм-

мируемое устройство — должны рассматриваться в связи друг с другом, так как они являются полностью согласованными и внутренне непротиворечивыми. Они также не противоречат и полностью взаимосвязаны с общими требованиями, установленными МЭК 61513, МЭК 60880, МЭК 62138, МЭК 62566 и МЭК 62566-2 к системам контроля и управления и электроэнергетическим системам атомных станций.

[МЭК 62138:2018, 3.34, измененный — добавлено примечание 4]

3.18 **элемент программируемой логики** (programmable logic item): Элемент, который основан на логических компонентах с интегральной схемой, состоящей из логических элементов со схемой взаимного соединения, части которой программирует пользователь.

Примечания

1 В данном термине и его определении слово «элемент» может быть заменено терминами «система», «оборудование» или «устройство».

2 Элемент программируемой логики является разновидностью программируемого цифрового элемента.

3 См. также термин «Э/Э/ПЭ элемент» и примечания к нему.

[МЭК 62138:2018, 3.35]

3.19 **квалификация** (qualification): Процесс определения, подходит ли система или компонент для эксплуатации. Квалификацию осуществляют с учетом класса СКУ и специальных квалификационных требований.

Примечания

1 Квалификационные требования формируются исходя из определенного класса СКУ и конкретного применения.

2 СКУ, как правило, реализуют на основе взаимодействующих комплектов оборудования. Подобное оборудование может быть разработано в рамках проекта или существовать как уже разработанное оборудование. Как правило, квалификационную оценку СКУ выполняют поэтапно: сначала осуществляют квалификацию уже существующего оборудования (обычно в начале процесса реализации системы), а затем — квалификацию объединенной СКУ (т. е. окончательно реализованного проекта).

3 При квалификации СКУ всегда учитывают конкретный тип АС и конкретную область применения. В то же время квалификация в значительной степени может быть основана на квалификационных мероприятиях, проведенных без привязки к конкретному проекту АС (так называемая «общая» или «предварительная» квалификация). Предварительная квалификация может значительно сократить трудозатраты на квалификацию с учетом конкретного типа АС, однако должно быть подтверждено выполнение квалификационных требований, учитывающих конкретную область применения.

[МЭК 61513:2011, 3.38, измененный — исключено примечание 2 с определением ранее разработанного оборудования и скорректировано последнее предложение примечания 3]

3.20 **случайный дефект** (random fault): Несистемный дефект компонентов аппаратных средств.

Примечание — Дефекты компонентов аппаратных средств являются последствием физических или химических воздействий, которые могут произойти в любое время. Корректное описание вероятности возникновения случайных дефектов может быть представлено статистически (как частота появления дефектов). Повышенная частота появления дефектов может быть результатом системных ошибок при проектировании или изготовлении аппаратных средств, если они возникают без временной корреляции, например как следствие преждевременного старения.

[МЭК 62340:2007, 3.15]

3.21 **функция безопасности** (safety function): Определенная цель, которая должна быть достигнута для обеспечения безопасности объекта, или действие в целях предотвращения или устранения радиационных последствий при нормальной эксплуатации, нарушениях нормальной эксплуатации и авариях.

Примечания

1 Функции безопасности должны выполнять фундаментальные функции, обеспечивающие безопасность, которые включают (I) управление реактивностью, (II) отвод тепла из реактора и из хранилища топлива, (III) локализацию радиоактивного материала, экранирование от радиации и контроль плановых радиоактивных выбросов, а также ограничение аварийных радиоактивных выбросов [IAEA SSR-2/1, требование 4].

2 Функции безопасности — это главным образом функции, которые учитывают при анализе безопасности и которые включают функции, выполняемые на всех уровнях глубокоэшелонированной защиты.

[Глоссарий МАГАТЭ по вопросам безопасности, 2018]

3.22 **система** (system): Совокупность компонентов, взаимодействующих в соответствии с проектом, в котором элемент системы может представлять собой другую систему, называемую подсистемой.

Примечания

1 См. также термин «система контроля и управления».

2 СКУ отличают от механических и электрических систем АС.

3 Настоящее определение ПК 45А МЭК полностью сопоставимо с определением термина «система», приведенным в Глоссарии МАГАТЭ по вопросам безопасности 2018 г. в составе статьи «Структуры, Системы и Компоненты (ССК)».

[МЭК 61513:2011, 3.56, измененный — в примечании 3 издание Глоссария МАГАТЭ по вопросам безопасности 2007 г. заменено на издание 2018 г.]

3.23 **валидация системы** (system validation): Подтверждение посредством проверки и предоставления других доказательств того, что система полностью соответствует требованиям спецификации согласно целевому назначению (функциональность, время отклика, отказоустойчивость, надежность).

[МЭК 61513:2011, 3.59]

3.24 **системный дефект** (systematic fault): Дефект аппаратных средств или программного обеспечения, который систематически затрагивает некоторые или все компоненты определенного типа.

Примечания

1 Системные дефекты могут быть вызваны ошибками спецификации или проекта, производственными дефектами или неправильным техобслуживанием.

2 Компоненты, содержащие скрытый системный дефект, могут отказать произвольно или совместно, в зависимости от вида дефекта и механизмов, вызывающих дефект.

[МЭК 62340:2007, 3.24]

3.25 **невыявленный отказ аппаратных средств** (unrevealed hardware failure): Отказ аппаратных средств, который не выявлен системой автоматически и стал очевидным только при попытке использовать функцию, выполняемую с использованием отказавшего аппаратного средства.

Примечание — Подобные отказы могут быть выявлены путем функционального испытания или когда в систему поступает эксплуатационный запрос.

3.26 **верификация** (verification): Подтверждение посредством проверки и предоставления объективных доказательств того, что результаты деятельности соответствуют целям и требованиям, определенным для этой деятельности.

Примечание — В Глоссарии МАГАТЭ по вопросам безопасности издания 2018 г. приведены следующие два определения:

Валидация: Процесс определения, достаточно ли пригодны продукт или услуга для выполнения предусмотренной функции. Валидация (как правило, системы) предусматривает проверку, касающуюся спецификации требований, в то время как верификация (как правило, проектной спецификации, спецификации испытаний или отчета об испытании) относится к результату процесса. Валидация может включать более значительный элемент оценочного суждения, чем верификация.

Верификация: Процесс определения соответствия качества или рабочих характеристик продукта или услуги тому, что заявлено, необходимо по назначению или требуется. Верификация тесно связана с обеспечением качества и контролем качества.

Определение МАГАТЭ термина «верификация» очень похоже на его же определение термина «валидация», так как оба термина отнесены к конечному продукту или услуге.

В стандартах ПК 45А МЭК термины «верификация» и «валидация» отнесены к результату жизненного цикла конкретных изделий, а именно к оборудованию и системам контроля и управления, а не к услугам в целом.

Кроме того, термины «верификация» и «валидация» используются для обозначения двух разных, дополняющих друг друга типов оценки.

«Верификация» означает оценку результатов отдельного действия в зависимости от исходных данных.

«Валидация» означает оценку окончательного продукта относительно его задокументированных назначения и требований.

[МЭК 61513:2011, 3.62, измененный — в примечании 1 издание Глоссария МАГАТЭ по вопросам безопасности 2007 г. заменено на издание 2018 г. и текст примечания изменен соответствующим образом].

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

ATE — автоматизированное испытательное оборудование (automated test equipment);

BOM — перечень поставляемых материалов (bill of materials);

COTS — коммерческий, серийно выпускаемый (commercial off the shelf);

HDL — язык описания аппаратных средств (hardware description languages);

HPD — HDL-программируемое устройство (HDL-programmed device);

ISA — Международная ассоциация автоматизации (International Society of Automation);

NEMA — национальная ассоциация производителей электротехнической промышленности (national electrical manufacturers association);

ОММ — руководство по эксплуатации и техническому обслуживанию (operation and maintenance manual);

АВПО — анализ видов и последствий отказов (failure modes and effects analysis, FMEA);

АВПКО — анализ видов, последствий и критичности отказов (failure mode effects and criticality analysis, FMECA);

АДО — анализ дерева отказов (fault tree analysis, FTA);

АС — атомная станция (nuclear power plant, NPP);

ПЛИС — программируемая логическая интегральная схема (field programmable gate array, FPGA).

5 Жизненный цикл безопасности аппаратных средств

5.1 Общие положения

Процесс производства СКУ для использования на энергоблоках атомных станций изложен в МЭК 61513, который вводит понятие жизненного цикла безопасности системы. Это инструмент, при помощи которого можно осуществлять контроль процесса разработки и использование которого позволяет получить свидетельство необходимости подтверждения надлежащего функционирования важных для безопасности систем. Данное понятие включает и определяет объем требований, но не устанавливает жесткий порядок реализации проекта, который следует использовать для изготовления систем (см. рисунок 1).

Понятие жизненного цикла безопасности систем, введенное МЭК 61513, более подробно описано в других стандартах. При разработке ПО следует использовать дополнительную информацию, приведенную в МЭК 60880 (для систем, выполняющих функции категории А) и МЭК 62138 (для систем, выполняющих функции категорий В и С), при разработке HPD — информацию, приведенную в МЭК 62566 (устройства, выполняющие функции категории А) и МЭК 62566-2 (устройства, выполняющие функции категорий В и С), а при разработке аппаратных средств СКУ классов 1, 2 и 3 — информацию, приведенную в МЭК 60987.

Оборудование для контроля и управления, включая компоненты аппаратных средств, разрабатывают в соответствии с циклом, включающим деятельность, направленную на выработку технического задания, проектирование и реализацию, квалификацию, изготовление, комплексирование (интеграцию) и валидацию, наряду с деятельностью по обеспечению качества и верификации.

В большинстве случаев поставщики оборудования для контроля и управления используют ранее разработанные компоненты, и жизненный цикл безопасности аппаратных средств должен быть строго совместим с жизненным циклом безопасности системы. В частности, техническое задание на аппаратные средства должно являться частью или формироваться непосредственно на основании технического задания на систему и проекта системы.

При необходимости разработка отдельных новых компонентов может быть осуществлена параллельно с разработкой проекта АС конкретного типа. В таких случаях разработку и квалификацию выполняют заблаговременно или с некоторыми наложениями параллельно с мероприятиями проекта.

На рисунке 2 показаны взаимосвязи между деятельностью в рамках жизненного цикла безопасности аппаратных средств и деятельностью в рамках жизненного цикла системы.

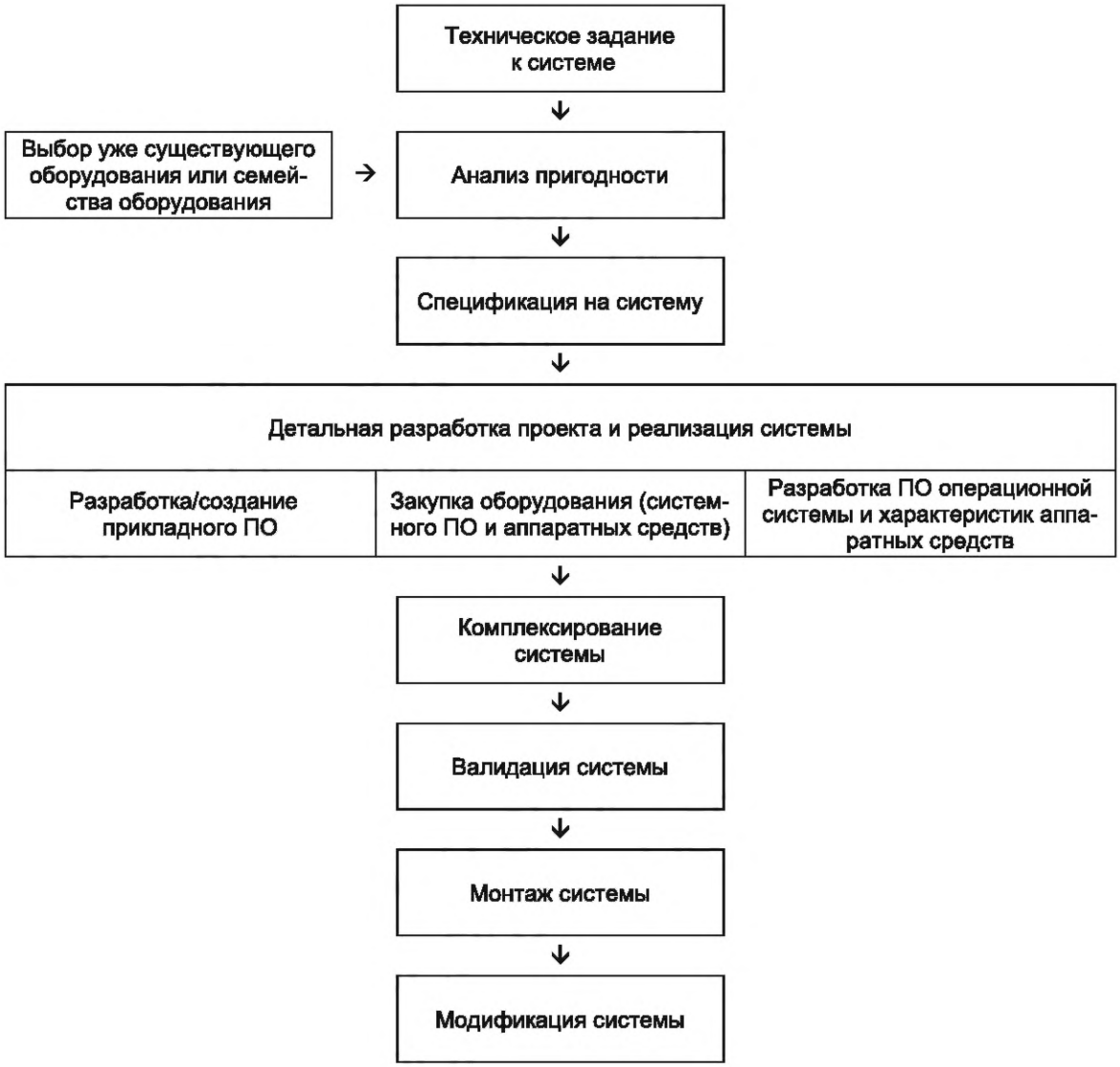
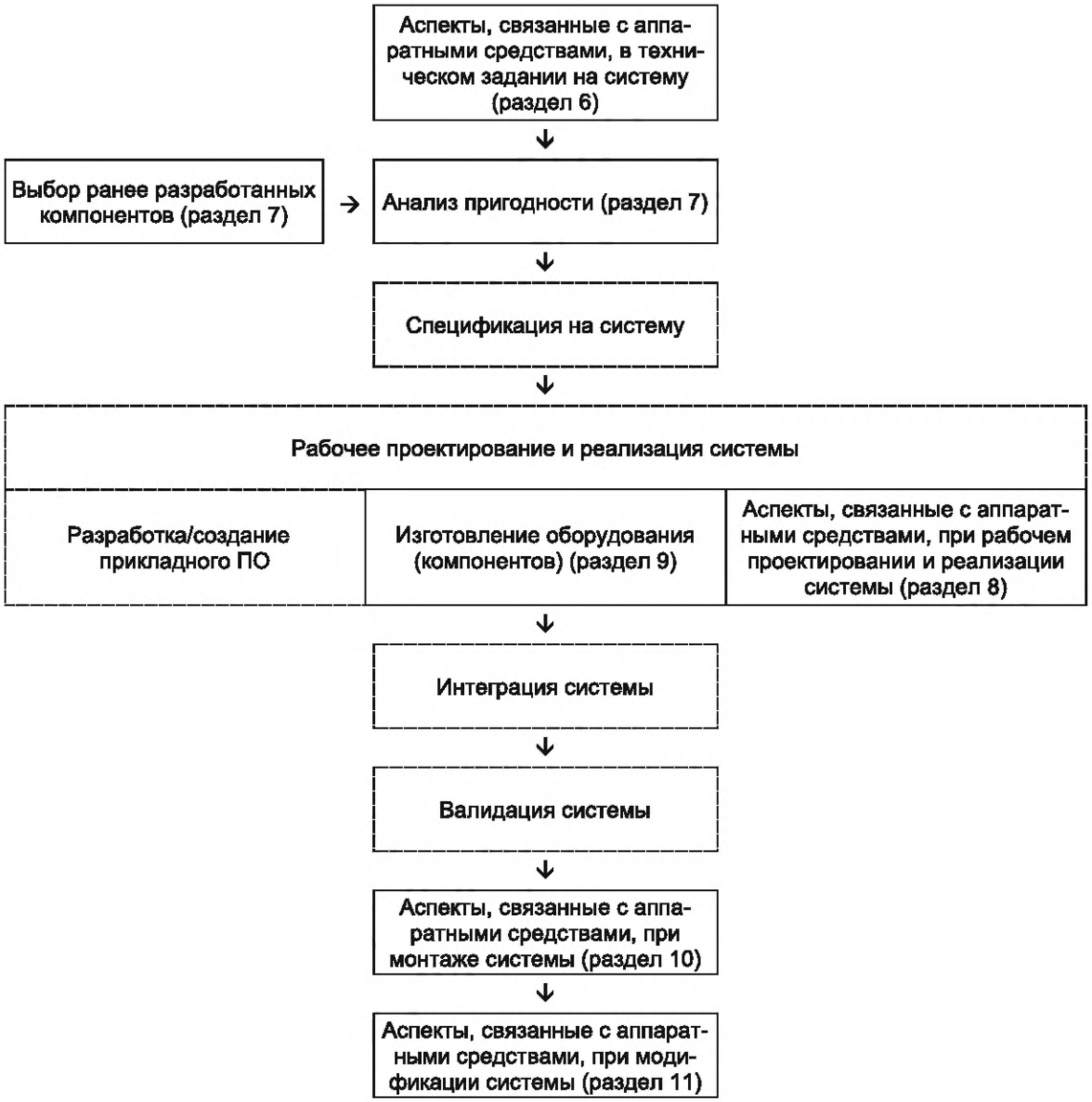


Рисунок 1 — Жизненный цикл безопасности системы
(информативная схема в соответствии с МЭК 61513)



Примечание — Блоки, обведенные тонкими пунктирными линиями, отражают деятельность, связанную с системой, но не рассматриваемую в настоящем стандарте.

Рисунок 2 — Деятельность, относящаяся к аппаратным средствам, в рамках жизненного цикла безопасности системы

К обеспечению жизненного цикла безопасности аппаратных средств также относится следующая дополнительная деятельность по планированию, не представленная на рисунке 2:

- обеспечение качества;
- верификация;
- управление конфигурацией.

В то же время в настоящем стандарте рассматриваются вопросы, связанные с эксплуатацией и техническим обслуживанием, которые не представлены на рисунке 2.

Квалификация на устойчивость к воздействию окружающей среды не представлена на рисунке 2 и не рассматривается в настоящем стандарте. При наличии требования к сейсмостойкости проводят испытания и квалификацию СКУ на устойчивость к воздействию окружающей среды в соответствии с применимыми требованиями IEC/IEEE 60780-323, дополненными требованиями IEC/IEEE 60980-344.

Степень устойчивости к электромагнитным помехам при необходимости следует определять в соответствии с требованиями, установленными в зависимости от среды эксплуатации, и требованиями МЭК 62003. Требования к электромагнитной устойчивости должны соответствовать реалистичным оценкам эксплуатационных условий при всех вероятных наихудших обстоятельствах.

Степень устойчивости к электромагнитным помехам при необходимости определяют в соответствии с применимыми стандартами серии МЭК 61000.

5.2 Жизненный цикл безопасности аппаратных средств СКУ класса 1 и класса 2

5.2.1 Структура проекта аппаратных средств СКУ класса 1 и класса 2

5.2.1.1 Жизненный цикл безопасности аппаратных средств должен быть сопоставим с жизненным циклом безопасности системы.

Проект нового модуля может быть независимым проектом и управляться отдельно от разработки оборудования для контроля и управления даже в тех случаях, когда предполагается интеграция такого модуля. В настоящее время стандартная ситуация заключается в том, что большинство модулей, интегрированных в СКУ, являются ранее разработанными модулями в составе общей совокупности оборудования, предоставляемого поставщиками.

5.2.1.2 Все этапы жизненного цикла безопасности аппаратных средств должны включать точно определенные и задокументированные действия.

5.2.1.3 Все этапы должны быть в определенной степени самостоятельными, но при этом зависимыми от других этапов в части исходных данных, так как выходные данные на каждом этапе, в свою очередь, являются исходными данными для других этапов.

Примечание — Различные этапы проекта в совокупности рассматриваются как общий жизненный цикл безопасности (см. раздел 5 МЭК 61513:2011, в котором приведены требования к жизненным циклам безопасности систем). МЭК 61513 допускает параллельную реализацию этапов проекта при условии, что при интеграции системы это не вызовет негативных последствий для жизненного цикла безопасности системы.

5.2.1.4 Каждый этап должен включать разработку документации для возможности приступить к следующему этапу разработки, учитывая при этом любые допущения или ограничения, которые необходимо применить в отношении оборудования для контроля и управления.

5.2.1.5 Каждый этап должен завершаться проведением верификации (см. 5.2.3).

5.2.1.6 Все работы должны осуществляться в соответствии с графиком, чтобы обеспечить достаточное время для проведения следующих действий:

- обеспечение взаимодействия между этапами разработки аппаратных средств и HPD или ПО, необходимого для совместимости этих компонентов системы;
- разработка документации и проведение испытаний, верификации и действий по обеспечению качества.

5.2.2 Управление качеством аппаратных средств СКУ класса 1 и класса 2

5.2.2.1 План обеспечения качества для аппаратных средств следует разрабатывать в виде отдельного документа (документов) или как часть плана обеспечения качества системы.

5.2.2.2 Все работы по обеспечению качества аппаратных средств, выполняемые в рамках жизненного цикла безопасности аппаратных средств, должны быть включены в план обеспечения качества.

5.2.2.3 План обеспечения качества должен устанавливать требования о выделении достаточных ресурсов (человеческих, финансовых), достаточных средств (запасных частей, устройств для испытания и технического обслуживания и т. д.) и обеспечении достаточных условий (лабораторий, производственных помещений, рабочих мест) для выполнения задач, связанных с каждым этапом жизненного цикла безопасности аппаратных средств.

5.2.2.4 В плане обеспечения качества должно содержаться требование о закреплении каждого вида работ за компетентными лицами.

5.2.2.5 План обеспечения качества должен предусматривать следующие аспекты в той степени, в которой они применимы к любой конкретной системе или разработке:

- аспекты технического задания на систему, связанные с аппаратными средствами;
- выбор ранее разработанных компонентов;
- аспекты рабочего проекта и реализации системы, связанные с аппаратными средствами;
- изготовление оборудования (компонентов);
- аспекты монтажа системы, связанные с аппаратными средствами;
- аспекты модификации системы, связанные с аппаратными средствами.

5.2.2.6 План (планы) обеспечения качества должен содержать информацию об организации, управлении и реализации мероприятий, связанных с обеспечением качества, включая следующие (в применимой степени):

- процесс проектирования;
- контроль комплектности документации;
- контроль инструкций по сборке, монтажу и контроль чертежей;
- процесс закупок товаров и услуг;
- контроль материалов и элементов, используемых для создания аппаратных средств системы;
- мероприятия по управлению качеством, такие как официальные инспекции;
- контроль испытательного оборудования и испытательных средств;
- контроль за обращением/хранением/отгрузкой аппаратных средств;
- процесс испытаний;
- отслеживание несоответствий и связанных с ними корректирующих действий;
- порядок хранения записей по обеспечению качества;
- порядок проведения внутренних и внешних аудитов.

5.2.3 Верификация аппаратных средств СКУ класса 1 и класса 2

5.2.3.1 Общие требования к аппаратным средствам СКУ класса 1 и класса 2

Процессы разработки рабочего проекта и реализации должны включать официальные проверки соответствия результатов каждого этапа разработки аппаратных средств требованиям, обусловленным предыдущим этапом.

Примечание — Предполагается, что процесс верификации аппаратных средств в целом начинается с верификации технического задания на аппаратные средства на предмет соответствия техническому заданию на систему и завершается, когда HPD и ПО системы интегрированы в аппаратные средства. Требования к этапам интеграции аппаратных средств, ПО и HPD приведены в МЭК 60880 и МЭК 62138, а также в МЭК 62566 и МЭК 62566-2 соответственно.

5.2.3.2 План верификации аппаратных средств СКУ класса 1 и класса 2

5.2.3.2.1 План верификации должен быть разработан с целью определения подхода, который будет использован для верификации проекта аппаратных средств и для контроля правильной реализации мероприятий по верификации. Данный план может входить в состав плана по верификации в целом.

5.2.3.2.2 План должен быть разработан прежде, чем будет инициирована деятельность по верификации.

5.2.3.2.3 План (планы) должен содержать информацию о персонале и организации, проводящих верификацию, организационной структуре, методах проведения верификации, уровне проводимой верификации, графике и о прочих существенных аспектах, относящихся к верификации.

5.2.3.2.4 Мероприятия по верификации следует проводить только после предъявления проектировщиками на верификацию результатов проектирования (документации, компонентов) и прохождения контроля комплектности требуемых документов.

Может быть проведена неофициальная предварительная верификация параллельно с процессом проектирования с целью выявления и устранения ошибок в максимально кратчайшие сроки (при условии обеспечения адекватных механизмов контроля комплектности документов).

5.2.3.2.5 После предъявления на верификацию корректировку проекта необходимо проводить только при условии гарантии, что все последующие изменения в проекте аппаратных средств надлежащим образом верифицированы (например, в соответствии с требованиями, приведенными в разделе 11).

5.2.3.3 Независимость верификации аппаратных средств СКУ класса 1 и класса 2

5.2.3.3.1 План верификации должен быть разработан и выполнен лицами, не принимавшими участие в работах по проектированию.

5.2.3.3.2 Персонал, выполняющий верификацию систем класса 1, должен быть административно независимым от проектировщиков аппаратных средств, например относиться к различным подразделениям одной организации или к различным организациям.

5.2.3.3.3 Персоналом, выполняющим верификацию, могут быть только технически компетентные лица.

5.2.3.3.4 Верификацию необходимо выполнять в соответствии с задокументированными процедурами.

5.2.3.3.5 Любые результаты верификации и отклики команды проектировщиков на эти результаты должны быть официально задокументированы.

5.2.3.3.6 Если для систем класса 1 используют ATE, проводящее испытания в автоматическом режиме, должна быть обеспечена независимость между:

- проектировщиками аппаратных средств и разработчиками программы испытаний;
- проектировщиками аппаратных средств и работниками, отвечающими за проведение испытаний и обрабатывающими их результаты.

5.2.3.3.7 Если для систем класса 2 используют ATE, проводящее испытания в автоматическом режиме, должна быть обеспечена независимость между:

- проектировщиками аппаратных средств и разработчиками программы испытаний;
- проектировщиками аппаратных средств и работниками, проводящими обработку результатов испытаний.

5.2.3.4 Методы верификации аппаратных средств СКУ класса 1 и класса 2

5.2.3.4.1 Основания для выбора метода (методов) верификации, предлагаемого(ых) для использования, должны быть достаточно подробно задокументированы, чтобы обеспечить возможность контроля со стороны персонала, не вовлеченного напрямую в мероприятия по проектированию и верификации.

Примечание — Типичными примерами методов верификации являются критический обзор, аудит, анализ, испытания, проводимые вручную или с использованием ATE.

5.2.3.4.2 При выборе приемлемого метода верификации необходимо учитывать следующие факторы:

- классификацию систем по безопасности (например, для аппаратных средств СКУ класса 1 требуются наиболее строгие методики);
- предусмотренные документацией обзоры и испытания, которые необходимо будет выполнить в отношении интегрированных аппаратных средств, ПО и HPD в рамках верификации и валидации системы, с тем чтобы исключить подобные мероприятия из верификации и валидации аппаратных средств и, таким образом, избежать неэффективного использования ресурсов вследствие дублирования действий;
- выполненные ранее работы по верификации в отношении аппаратных средств или систем, включающих аппаратные средства (в тех случаях, когда оборудование было ранее квалифицировано должным образом);
- проектные характеристики системы, например размер, уровень новизны использованных принципов проектирования, типы отказов и сложность;
- вспомогательные данные, которые могут быть получены из иных источников, в том числе данные, полученные в процессе обеспечения качества и квалификации на внешние воздействия.

5.2.3.4.3 Должны быть доступны средства и методы испытаний подсистем и компонентов, позволяющие обеспечить полноту их испытаний.

5.2.3.4.4 В обоснованных случаях следует использовать ATE для повышения полноты испытаний и стабильности их условий.

5.2.3.4.5 Испытательные средства, используемые в процессе верификации или испытаний, должны быть откалиброваны для подтверждения их точности в тех случаях, когда критерии успешности испытаний зависят от измеряемых величин. При этом процедуры должны гарантировать использование только откалиброванных средств измерения.

5.2.3.4.6 Программные испытательные средства должны пройти обязательную валидацию до их использования и подлежать контролю конфигурации.

Примечание — Валидация программных испытательных средств основывается на пользовательской документации и соответствии требованиям к испытаниям.

5.2.3.4.7 Результаты любых официальных испытаний должны быть задокументированы (неофициальные испытания могут быть проведены в процессе проектирования в качестве предваряющих официальные испытания). Поддающиеся аудиту записи об официальных испытаниях должны быть доступны и достаточны для подтверждения того, что все испытания были выполнены и все несоответствия устранены.

5.2.3.5 Документация по верификации аппаратных средств СКУ класса 1 и класса 2

5.2.3.5.1 Поддающиеся аудиту записи, относящиеся к деятельности по верификации, должны включать план проведения верификации, описание процедур испытаний, результаты испытаний, записи по изменениям в проекте и документацию по любым несоответствиям, выявленным в процессе верификации аппаратных средств (наряду с записями, демонстрирующими, каким образом было устранено каждое несоответствие).

5.2.3.5.2 Процедуры испытаний должны быть описаны в виде пошаговой инструкции к верификации аппаратных средств, содержащей также подробную информацию об испытательной установке.

5.2.3.5.3 Процедуры испытаний должны включать однозначно сформулированные критерии успешного/неуспешного прохождения испытания.

5.2.3.5.4 Если испытание проводят с использованием программного обеспечения, то версия ПО должна быть указана в документации по верификации.

5.2.3.6 Управление несоответствиями при верификации аппаратных средств СКУ класса 1 и класса 2

5.2.3.6.1 Несоответствия, выявленные в процессе верификации, должны быть официально задокументированы и переданы соответствующему персоналу для принятия решения.

5.2.3.6.2 Ответ должен быть официальным образом задокументирован, чтобы можно было проследить, все ли несоответствия оценены и все ли обнаруженные недостатки проекта скорректированы или признаны допустимыми.

5.2.3.6.3 В случаях признания недостатков проекта допустимыми данная информация должна быть полностью отражена в документации системы.

5.3 Жизненный цикл безопасности аппаратных средств СКУ класса 3

5.3.1 Структура проекта и управление качеством аппаратных средств СКУ класса 3

5.3.1.1 Жизненный цикл безопасности аппаратных средств должен быть сопоставим с жизненным циклом безопасности всей системы.

Проект разработки нового модуля может быть независимым проектом и управляться отдельно от разработки оборудования для контроля и управления в тех случаях, когда предполагается интеграция такого модуля. В настоящее время типична ситуация, когда большинство модулей, интегрированных в СКУ, являются ранее разработанными модулями в составе общего семейства поставляемого оборудования для контроля и управления.

5.3.1.2 Все этапы должны быть в определенной степени самостоятельными, но при этом зависимыми от других этапов в части исходных данных, так как выходные данные на каждом этапе, в свою очередь, являются исходными данными для других этапов.

Примечание — Различные этапы проекта в совокупности рассматриваются как общий жизненный цикл безопасности (см. раздел 6 МЭК 61513:2011, в котором приведены требования к жизненным циклам безопасности систем). МЭК 61513 допускает параллельную реализацию этапов проекта, при условии, что при интеграции системы это не вызовет негативных последствий для жизненного цикла безопасности системы.

5.3.1.3 Каждый этап должен включать разработку документации для возможности приступить к следующему этапу разработки, учитывая при этом любые допущения или ограничения, которые необходимо применить в отношении оборудования для контроля и управления.

5.3.1.4 План обеспечения качества для аппаратных средств должен быть разработан в виде отдельного документа (документов) или как часть плана обеспечения качества системы.

5.3.1.5 План обеспечения качества должен предусматривать следующие аспекты в той степени, в которой они применимы к любой конкретной системе или разработке:

- аспекты технического задания на систему, связанные с аппаратными средствами;
- выбор ранее разработанных компонентов;
- аспекты рабочего проекта и реализации системы, связанные с аппаратными средствами;
- изготовление оборудования (компонентов);
- аспекты монтажа системы, связанные с аппаратными средствами;
- аспекты модификации системы, связанные с аппаратными средствами.

5.3.2 Верификация аппаратных средств СКУ класса 3

5.3.2.1 Процесс проектирования и реализации должен включать проверку соответствия результатов каждого этапа проектирования и реализации аппаратных средств требованиям, обусловленным предыдущим этапом.

Примечание — Предполагается, что процесс верификации аппаратных средств в целом начинается с верификации технического задания на аппаратные средства на предмет соответствия техническому заданию на систему и завершается, когда HPD и ПО системы интегрированы в аппаратные средства. Требования к этапам интеграции аппаратных средств, ПО и HPD приведены в МЭК 60880 и МЭК 62138, а также в МЭК 62566 и МЭК 62566-2 соответственно.

5.3.2.2 Несоответствия, выявленные в процессе верификации, должны быть официально задокументированы и переданы соответствующему персоналу для принятия решения.

5.3.2.3 Поддающиеся аудиту записи, относящиеся к деятельности по верификации, должны включать план проведения верификации, описание процедур испытаний, результаты испытаний, записи по изменениям в проекте, а также решения, принятые по выявленным несоответствиям.

6 Аспекты аппаратных средств в требованиях технического задания СКУ

6.1 Аспекты аппаратных средств в требованиях технического задания СКУ класса 1 и класса 2

6.1.1 Общие требования к аппаратным средствам СКУ класса 1 и класса 2

6.1.1.1 Требования к аппаратным средствам должны быть изложены в техническом задании на аппаратные средства или в составе спецификации более общего характера.

6.1.1.2 Требования к аппаратным средствам должны соответствовать техническому заданию на систему (см. МЭК 61513:2011, раздел 6).

Техническое задание на систему представляет собой описание аспектов, относящихся к аппаратным средствам и интегрированным системам аппаратных средств/ПО/HPD, и определяет цели проектирования системы, а также функции, которые должна выполнять система. Система может быть целиком спроектирована для конкретного случая применения или может быть создана на основе общего семейства оборудования, скомпонованного для конкретного проекта.

В техническом задании на аппаратные средства указывают их функции и требуемые функциональные характеристики, устанавливают требования к проекту аппаратных средств, требования к их надежности и к условиям окружающей среды, в которых аппаратные средства будут эксплуатироваться.

6.1.1.3 Требования к аппаратным средствам должны быть представлены такими способами или методами, формат которых не препятствует удобочитаемости.

6.1.1.4 Требования к аппаратным средствам должны быть выражены в форме, не допускающей двоякого толкования, поддаваться проверке путем испытаний, подтверждению путем верификации и должны быть выполнимыми.

6.1.1.5 Требования к аппаратным средствам должны в общем определять, что должно быть ими выполнено и каким образом это должно быть выполнено.

Использование ранее разработанных компонентов позволяет осуществлять восходящее проектирование аппаратных средств.

6.1.2 Функциональные и эксплуатационные требования к аппаратным средствам СКУ класса 1 и класса 2

6.1.2.1 Функциональные и эксплуатационные требования к аппаратным средствам должны соответствовать функциональным и эксплуатационным требованиям к системе.

6.1.2.2 Функциональные и эксплуатационные требования к аппаратным средствам в сочетании с требованиями к элементам аппаратных средств или программируемым цифровым элементам (в той мере, которая необходима для учета всех требований к аппаратным средствам) должны быть верифицированы на соответствие требованиям к системе.

6.1.2.3 Функциональные требования к аппаратным средствам должны включать (помимо прочего):

- назначение аппаратных средств системы в целом и каждого отдельного узла аппаратных средств;
- количество и типы датчиков и исполнительных механизмов, которые должны быть подключены к системе;
- количество и типы устройств человеко-машинного интерфейса, таких как дисплеи, принтеры и клавиатуры.

6.1.2.4 Каждый поставляемый компонент или подсистема, которые подлежат интеграции в систему, должны:

- сопровождаться спецификацией, в которой рассмотрены все аспекты безопасности эксплуатации данного элемента, или
- сопровождаться анализом, в котором определены проектные характеристики аппаратных средств компонента в пределах, необходимых для подтверждения его пригодности.

6.1.2.5 Требования к эксплуатационным характеристикам аппаратных средств должны включать (применительно к каждому конкретному использованию):

- необходимую скорость приема данных;
- необходимую мощность для обработки данных;
- необходимую вычислительную мощность;
- необходимые интерфейсы обмена данными (протоколы, скорости передачи данных);
- требуемую точность вычислений и преобразований данных;
- необходимую способность к подавлению помех сигналам;
- необходимые времена отклика;
- ограничения физических размеров;
- географические требования (например, длина линий передачи данных);
- необходимый уровень резервной мощности (при необходимости);
- требования к внешним условиям при эксплуатации;
- требования к источникам электропитания.

6.1.2.6 Ограничения, касающиеся интерфейсов аппаратных средств с другими системами, должны быть указаны в техническом задании на аппаратные средства или в документе более широкой области применения.

В МЭК 61513:2011 (6.2.2.3.2, 6.2.2.4, 6.2.2.5, 6.2.3.3.3 и 6.2.3.3.4) приведены требования к интерфейсу системы, направленные на обеспечение правильной интеграции и предотвращение распространения отказов через интерфейсы системы.

6.1.2.7 Должны быть определены любые ограничения, накладываемые на проект аппаратных средств проектом системы или проектом ПО/HPD.

6.1.3 Требования к надежности аппаратных средств СКУ класса 1 и класса 2

6.1.3.1 Требования к надежности аппаратных средств должны быть определены и соответствовать требованиям к надежности системы в целом.

Примечание — Надежность аппаратных средств в данном контексте относится к случайным отказам, а не к систематическим отказам.

6.1.3.2 Требования к надежности/пригодности аппаратных средств должны включать описание типов отказов, которые аппаратные средства должны выдерживать без потери функций или с определенной ограниченной потерей функций.

6.1.3.3 Требования к аппаратным средствам должны устанавливать целевые значения параметров надежности, таким как средняя наработка на выявленный отказ, средняя наработка на невыявленный отказ, средняя наработка до ремонта (для выявленных отказов).

6.1.3.4 Любое требование, касающееся заявленной надежности, соответствие которому должно быть подтверждено подробным анализом, следует приводить с указанием необходимого уровня анализа, т. е. анализа узла, модуля или компонента.

6.1.3.5 Должны быть установлены требования к техническому обслуживанию в целях обеспечения необходимой надежности в течение жизненного цикла СКУ.

6.1.3.6 Требования к техническому обслуживанию должны касаться следующих вопросов (насколько применимо к конкретной системе):

- требования к работе системы во время проведения технического обслуживания аппаратных средств;
- замена расходных материалов, например воздушных фильтров, аккумуляторов;
- любые требования по регулярной замене подсистем, модулей и/или компонентов;
- любые требования по проведению периодических испытаний с указанием их периодичности;
- меры, направленные на предотвращение ошибок при техническом обслуживании, которые потенциально могут привести к отказу по общей причине;
- объем мероприятий по повторной валидации системы (например, испытания), необходимой после работ по техническому обслуживанию аппаратных средств.

6.1.3.7 Требования к техническому обслуживанию должны быть установлены на этапе разработки технического задания на аппаратные средства, а в тех случаях, когда они не могут быть детально определены на этом этапе, они должны быть окончательно сформулированы на более позднем этапе, но до монтажа системы.

6.1.4 Требования к условиям окружающей среды для аппаратных средств СКУ класса 1 и класса 2

6.1.4.1 Требования к условиям окружающей среды для аппаратных средств должны содержать ограничения, устанавливаемые для СКУ, и указывать соответствующие уровни физических параметров, которые следует учитывать в применимых случаях.

Примечание — Типичные ограничения включают климатические условия, старение, сейсмические условия, химические воздействия, электроснабжение, электромагнитную совместимость и радиационные условия.

6.1.4.2 Диапазоны нормальных и экстремальных условий окружающей среды, которые должна выдерживать система, определяют в соответствии с ограничениями, обусловленными рамками проекта АС (см. МЭК 61513:2011, 5.2.4).

6.1.4.3 Должны быть учтены любые специфические требования, касающиеся хранения, монтажа и ввода в эксплуатацию аппаратных средств.

6.1.5 Требования к изготовлению аппаратных средств СКУ класса 1 и класса 2

Требования к аппаратным средствам должны определять, в частности:

- перечень запрещенных к использованию материалов, а также требования к особым материалам, которые будут использованы;
- специфические виды производственных процессов;
- минимальные критерии приемлемости в соответствии с IPC-A-610 (см. 9.1.6.4).

6.1.6 Требования к документации для аппаратных средств СКУ класса 1 и класса 2

Требования к документации на аппаратные средства должны быть определены в составе требований к документации на СКУ (см. МЭК 61513).

В приложении А приведена стандартная документация для каждого из основных разделов настоящего стандарта.

6.2 Аспекты аппаратных средств в требованиях технического задания СКУ класса 3

6.2.1 Общие требования к аппаратным средствам СКУ класса 3

6.2.1.1 Требования к аппаратным средствам должны быть изложены в техническом задании на аппаратные средства или в составе спецификации более общего характера.

6.2.1.2 Должно быть обеспечено соответствие технического задания на аппаратные средства требованиям, изложенным в техническом задании на систему, в части:

- функциональности;
- надежности;
- условий окружающей среды при эксплуатации;
- изготовления [конструкционные материалы, запрещенные к использованию при изготовлении, минимальный уровень критериев приемлемости по IPC-A-610 (см. 9.2.5), взаимозаменяемость].

6.2.1.3 Каждый компонент или подсистема, полученные от поставщика, которые предстоит интегрировать в систему, должны быть подвергнуты анализу с целью установить, в должной ли степени проектные характеристики аппаратных средств компонента подтверждают его пригодность, как описано в 7.2.

6.2.2 Надежность аппаратных средств СКУ класса 3

На случай, если анализ надежности системы требует дополнительных доказательств, в техническом задании на аппаратные средства должно быть предусмотрено требование о проведении анализа на возможность отказов аппаратных средств.

6.2.3 Требования к параметрам окружающей среды для аппаратных средств СКУ класса 3

Требования к параметрам окружающей среды должны устанавливать ограничения, накладываемые на СКУ, и указывать соответствующие диапазоны физических параметров, которые следует учитывать, если это необходимо.

Примечание — Типичные ограничения относятся к климатическим условиям и электрооборудованию.

6.2.4 Требования к документации на аппаратные средства СКУ класса 3

Требования к документации на аппаратные средства должны быть установлены в составе требований к документации на СКУ (см. МЭК 61513).

Типичный перечень документов, касающихся каждого из основных разделов настоящего стандарта, приведен в приложении А.

7 Выбор ранее разработанных компонентов аппаратных средств

7.1 Выбор ранее разработанных компонентов аппаратных средств СКУ класса 1 и класса 2

7.1.1 Анализ пригодности должен быть выполнен и задокументирован для подтверждения того, что ранее разработанные компоненты, используемые в составе оборудования, удовлетворяют установленным требованиям, приведенным в 6.1. Данный анализ может быть выполнен в рамках общего анализа пригодности.

7.1.2 В дополнение к указанному анализу пригодности должны быть предоставлены свидетельства, подтверждающие качество, основанные:

- на идентифицирующих данных, типе исполнения;
- изменениях с течением времени, задокументированных соответствующим образом;
- записях по управлению качеством;
- типовых испытаниях, проведенных изготовителем;
- применяемых руководствах или стандартах;
- эксплуатационном опыте изготовителя.

7.1.3 В тех случаях, когда анализ пригодности или свидетельства, подтверждающие качество, не обеспечивают полной информации, должны быть проведены мероприятия, компенсирующие этот недостаток, например испытания, анализ, приведение дополнительных обоснований.

7.1.4 Если в результате анализа пригодности выявлены несоответствия, то они должны быть устранены путем изменения проекта аппаратных средств или проекта системы (при условии, что не будут нарушены требования ядерной безопасности) или компонент должен быть забракован.

7.1.5 Конструкция ранее разработанного компонента должна полностью удовлетворять всем требованиям к техническому обслуживанию, установленным на основании технического задания на аппаратные средства.

Примечание — Данные требования относятся к процедурам эксплуатационных испытаний, калибровке, наладке, регулярным заменам и текущему ремонту.

7.1.6 В тех случаях, когда надежность аппаратных средств недостаточна для достижения необходимых показателей, должны быть приняты компенсирующие меры.

Примечание — Такие меры могут включать усовершенствование конструкции или изменения, относящиеся к эксплуатации (например, увеличение частоты периодических испытаний).

7.1.7 К такой мере, как увеличение частоты периодических испытаний, следует прибегать с осторожностью, поскольку любые принудительные вмешательства в работу установленного оборудования неизбежно приводят к риску прямого или косвенного внесения ошибок (например, общие последствия периодических испытаний могут негативно повлиять на безопасность). Идеальным вариантом является проведение испытаний, когда возможные нарушения процедуры испытаний не могут повлиять на безопасность, например во время простоев или когда испытуемое оборудование изолировано от остальной установки.

7.1.8 Должна быть проведена оценка проекта с точки зрения риска ошибок персонала в процессе эксплуатации и технического обслуживания оборудования (см. 8.1.4.3).

7.2 Выбор ранее разработанных компонентов аппаратных средств СКУ класса 3

7.2.1 Анализ пригодности должен быть выполнен и задокументирован для подтверждения того, что ранее разработанные компоненты, используемые в составе оборудования, удовлетворяют установленным требованиям, указанным в 6.1. Данный анализ может быть выполнен в рамках общего анализа пригодности.

7.2.2 В дополнение к указанному анализу пригодности должны быть предоставлены свидетельства, подтверждающие качество, основанные:

- на эксплуатационном опыте изготовителя; и/или
- данных, поставляемых изготовителями электронных модулей (характер и результаты испытаний по завершении изготовления, опыт эксплуатации, испытания образцов, результаты аудитов, техники обращения, сертификаты); и/или
- типовых испытаниях, проведенных изготовителем.

7.2.3 Если предоставлены свидетельства, основанные на эксплуатационном опыте изготовителя, они должны быть официально оформлены и основываться:

- на результатах инспекционного контроля поставленных компонентов, выполненного на одной из последовательно выпускаемых партий продукции и позволяющего верифицировать соответствие партии предъявляемым требованиям и выявленные отклонения; и/или
- результатах испытаний образцов; и/или
- результатах эксплуатации, демонстрирующих дефекты компонентов модулей, выявленные в ходе контроля, проведенного после завершения изготовления или при возврате заказчиком изделия для ремонта.

8 Аспекты аппаратных средств при разработке и реализации рабочего проекта СКУ

8.1 Аспекты аппаратных средств при разработке и реализации рабочего проекта СКУ класса 1 и класса 2

8.1.1 Общие требования к аппаратным средствам СКУ класса 1 и класса 2

8.1.1.1 Источником исходных данных для рассмотрения аспектов аппаратных средств на этапе разработки и реализации проекта системы должно быть техническое задание на аппаратные средства.

8.1.1.2 Процесс проектирования должен проходить этапы разработки проекта, отражаемые в плане обеспечения качества (см. 5.2.2), результатом чего является изготовление аппаратных средств, удовлетворяющих техническому заданию на аппаратные средства.

На более общем уровне работ по проектированию можно рассматривать общий проект аппаратных средств, состоящий из анализа различных вариантов проектных решений в целях определения архитектуры аппаратных средств системы, имея в виду входящие в нее подсистемы и модули.

После разработки общего проекта аппаратных средств обычно следует разработка рабочего (детального) проекта, состоящего из одного или более уровней.

8.1.1.3 Разработка рабочего проекта заключается в расширении общего проекта, направленном на создание проектов подсистем, модулей и компонентов настолько подробных, что описание проекта аппаратных средств становится достаточным для его реализации.

Могут быть созданы опытные образцы аппаратных средств не только в целях демонстрации успешного взаимодействия между их модулями, но также для проверки совместимости аппаратных средств, ПО и HPD.

8.1.1.4 Если проектирование проводят в один этап, то этот этап должен включать разработку рабочего проекта аппаратных средств.

8.1.2 Мероприятия по проектированию аппаратных средств СКУ класса 1 и класса 2

8.1.2.1 На требования к эксплуатационным характеристикам системы, зависящим от эксплуатационных характеристик аппаратных средств, очевидно влияет проект аппаратных средств, а потому путем анализа или испытаний необходимо получить свидетельство соответствия проекта аппаратных средств данным требованиям (см. 6.1.2.5).

8.1.2.2 Любые отклонения от требований к аппаратным средствам должны быть устранены путем внесения изменений в проект или путем повторного анализа требований (см. 5.2.3.6).

8.1.2.3 Должны быть определены испытания, необходимые для демонстрации того, что необходимые эксплуатационные характеристики достигнуты.

8.1.2.4 Такие испытания могут быть проведены для отдельных аппаратных средств или, когда аппаратные средства интегрированы с ПО и/или HPD, т. е. на этапе комплексирования системы.

8.1.2.5 Следует определить, какие работы по техническому обслуживанию необходимы, чтобы удостовериться в том, что требования к эксплуатационным характеристикам и надежности удовлетворяются в течение срока эксплуатации оборудования. К таким работам могут относиться периодические

испытания, калибровка приборов, ремонт, предупредительное и корректирующее техническое обслуживание. Все такие работы должны быть задокументированы как процедуры технического обслуживания.

8.1.2.6 Работы по техническому обслуживанию необходимо выполнять в той мере, которая дает достаточную уверенность в правильной работе оборудования, а также снижает до минимума влияние персонала и принудительные вмешательства в работу системы, что позволяет уменьшить вероятность дефектов, происходящих вследствие работ по техническому обслуживанию.

8.1.2.7 Для оборудования с резервированной системой или несколькими системами, предназначенными для выполнения функции безопасности, при анализе следует учитывать возможные отказы по общей причине, связанные с аппаратными средствами.

Возможными причинами возникновения таких отказов, связанных с аппаратными средствами, являются:

- работы по техническому обслуживанию нескольких компонентов оборудования, выполняемые одновременно или последовательно (в особенности, когда такие работы могут стать причиной отказов аппаратных средств);
- периодические испытания;
- скрытые дефекты проекта аппаратных средств, не выявленные в течение жизненного цикла разработки.

8.1.3 Надежность аппаратных средств СКУ класса 1 и класса 2

8.1.3.1 При необходимости подтверждения выводов анализа безопасности, проведенного на уровне системы, следует во время проектирования провести анализ вероятности отказов аппаратных средств.

8.1.3.2 Метод, используемый для проведения анализа надежности аппаратных средств, выбирают в соответствии с целью такого анализа.

Требования к надежности устанавливают в техническом задании на аппаратные средства в соответствии с 6.1.3.

Методы, которые могут быть использованы для анализа надежности аппаратных средств, включают:

- АДО, направленный на выявление и анализ условий и факторов, становящихся причиной или способствующих возникновению определенного нежелательного события (данная методика приведена в МЭК 61025);
- АВПО, идентифицирующий отказы, которые имеют значимые последствия, влияющие на эксплуатационные характеристики системы, например на надежность, безопасность. В МЭК 60812, который описывает ряд методик проведения АВПО и АВПКО, даны рекомендации по применению данных методик в соответствии с определенными целями;
- расчет значений частоты отказов, используемых в качестве исходных данных для АВПО или АВПКО, который применяют при различии между фактическими и стандартными условиями окружающей среды, с последующей корректировкой расчетных данных в соответствии с рекомендациями, приведенными, например, в МЭК 61709.

8.1.3.3 Для оборудования класса 1 следует использовать методы АДО или АВПО в сочетании с данными об отказах компонента для получения расчетных значений надежности аппаратных средств системы (см. IEC 61513), за исключением случаев, когда имеется достаточно данных из опыта эксплуатации для обеспечения высокого уровня уверенности в том, что целевые значения надежности достигнуты.

8.1.3.4 Для оборудования класса 2 надежность аппаратных средств системы следует определять:

- методами АДО или АВПО в сочетании с данными об отказах компонента;
- путем обоснования достаточной надежности, основанного на качественных аргументах, особенно в тех случаях, когда к надежности аппаратных средств системы не предъявляют чрезмерно строгие требования (например, когда речь идет о таких факторах, как качество компонентов, резервирование аппаратных средств, эксплуатационный опыт, отношение выявленных отказов аппаратных средств к скрытым отказам аппаратных средств).

8.1.3.5 Проект аппаратных средств должен способствовать минимизации возможного воздействия на ядерную безопасность следующих факторов:

- работы по техническому обслуживанию;
- отказ системы в связи со случайными дефектами;
- отказ аппаратных средств в связи с условиями окружающей среды.

8.1.3.6 Если расчетная надежность аппаратных средств не соответствует ожидаемым показателям, то следует провести компенсирующие действия, заключающиеся в усовершенствовании проекта или введении изменений в эксплуатационную процедуру (таких, как увеличение частоты периодических испытаний).

При выборе такого компенсирующего действия, как увеличение частоты периодических испытаний, необходимо проявлять осторожность, так как любые действия, связанные с нарушением целостности оборудования работающей АС, характеризуются повышенным риском, связанным с введением или провоцированием дефектов (то есть суммарное общее воздействие периодических испытаний на безопасность может быть отрицательным). Идеальным вариантом является проведение всех испытаний тогда, когда возможные нарушения, возникающие в процессе испытаний, не могут повлиять на ядерную безопасность, например во время останова энергоблока или когда испытуемое оборудование отключено от работающей АС.

При вероятностной оценке безопасности АС расчетные значения параметров надежности аппаратных средств (например, полученные методом АДО) могут быть использованы и таким образом могут внести свой вклад в точность расчетов надежности АС в целом.

8.1.4 Техническое обслуживание аппаратных средств СКУ класса 1 и класса 2

8.1.4.1 Проектом аппаратных средств должны быть учтены любые конкретные требования к техническому обслуживанию, включенные в техническое задание на аппаратные средства.

8.1.4.2 Все электронные модули, входящие в состав оборудования, должны быть идентифицированы как пригодные для ремонта или не подлежащие ремонту.

8.1.4.3 Кроме того, в тех случаях, когда это возможно, проект должен предусматривать способы снижения риска появления дефектов вследствие работ по техническому обслуживание. К таким способам можно отнести:

- легкий доступ к компонентам, которые могут подлежать замене как расходные материалы или в результате отказов;
- четкая идентификация заменяемых компонентов, чтобы технический персонал мог легко проверить правильность замены компонентов;
- использование компонентов, которые можно заменять без нарушения целостности технологической кабельной проводки АС;
- обеспечение достаточного расстояния между клеммными блоками;
- обеспечение достаточного количества специальных клемм, используемых во время работ по калибровке/испытаниям (чтобы отсутствовала необходимость отключения проводных соединений оборудования АС при проведении таких работ);
- включение в проект аппаратных средств структурированной компоновочной схемы с четкой маркировкой для снижения вероятности ошибок при техническом обслуживании.

8.1.5 Отказы питания аппаратных средств СКУ класса 1 и класса 2

8.1.5.1 В той мере, в какой это требуется в соответствии с техническим заданием на аппаратные средства, СКУ должна быть спроектирована устойчивой к последствиям кратковременных перебоев питания и возможным изменениям в сети (напряжение/частота).

8.1.5.2 Должны быть предусмотрены системные средства для уведомления операторов и технического персонала о таких колебаниях мощности (эту функцию не обязательно назначают аппаратным средствам, и поэтому данный аспект может не входить в область применения настоящего стандарта).

8.1.6 Проектная документация для аппаратных средств СКУ класса 1 и класса 2

8.1.6.1 Проектная документация на аппаратные средства должна содержать проект аппаратных средств и описание способов, с помощью которых были удовлетворены требования к аппаратным средствам.

8.1.6.2 Должны быть использованы стандартные формы проектной документации на аппаратные средства и автоматизированные средства проектирования аппаратных средств.

8.1.6.3 Должна быть соблюдена иерархия проектных документов, относящихся к аппаратным средствам СКУ, включающих ряд уровней документации.

8.1.6.4 Проектная документация на аппаратные средства на каждом уровне должна устанавливать аспекты проектирования, относящиеся к данному уровню, и определять требования к аппаратным средствам для более низких уровней или учитывать характеристики аппаратных средств более низкого уровня.

8.1.6.5 Проектная документация на аппаратные средства должна определять архитектуру аппаратных средств, то есть структуру и связи между разными частями системы.

8.1.6.6 Проектная документация на аппаратные средства должна включать общую компоновочную схему аппаратных средств с блок-схемами подсистем и модулей нижних уровней.

8.1.6.7 Проектная документация на аппаратные средства должна также включать требования к аппаратным средствам для разработки детального (рабочего) проекта аппаратных средств, такие как:

- количество и типы центральных процессорных устройств и других процессоров;
- требования к запоминающим устройствам аппаратных средств;
- количество и типы HPD;
- количество и типы интерфейсов;
- количество и типы линий и шин передачи данных.

8.1.6.8 По завершении проектирования и реализации аппаратных средств должна быть сформирована проектная документация на аппаратные средства, включающая полное и завершенное описание как особенностей проекта до нижнего уровня, так и возможностей, ограничений и иных характеристик оборудования.

8.1.6.9 Документация, завершающая проектирование аппаратных средств, должна включать следующую информацию:

- обзор проекта;
- кросс-ссылки на подтверждающие проектные документы;
- описание разделения аппаратных средств на подсистемы аппаратных средств;
- описание каждой подсистемы, касающееся ее основных модулей и компонентов (с использованием блок-схем, схем подключений);
- описание в установленном порядке интерфейсов аппаратных подсистем, которое должно отражать логические, физические, электрические и другие аспекты;
- описание интерфейсов аппаратных средств СКУ. Должны быть описаны интерфейсы с любыми другими системами, как размещенными на площадке АС, так и находящимися за ее пределами, с указанием конкретных интерфейсов и соответствующих требований к аппаратным средствам;
- описание физической компоновки оборудования со схемами;
- описание условий окружающей среды при использовании и хранении;
- инструкции по техническому обслуживанию, включая определение необходимых действий (например, замена компонентов), требуемых для поддержания указанного квалифицированного срока службы;
- описание характеристик надежности и безопасности оборудования;
- требования к техническому обслуживанию.

8.2 Аспекты аппаратных средств при разработке и реализации рабочего проекта СКУ класса 3

8.2.1 Общие требования к аппаратным средствам СКУ класса 3

8.2.1.1 Источником исходных данных на этапе рассмотрения аспектов аппаратных средств при разработке и реализации рабочего проекта системы должно быть техническое задание на аппаратные средства.

8.2.1.2 Проектная документация на аппаратные средства должна содержать проект аппаратных средств и описание способов, с помощью которых были удовлетворены требования к аппаратным средствам.

8.2.1.3 По завершении разработки проекта должна быть оформлена необходимая проектная документация на аппаратные средства, включающая полное завершенное описание проекта, а также функциональных возможностей, ограничений и иных характеристик аппаратных средств.

8.2.2 Надежность аппаратных средств СКУ класса 3

При необходимости содействия анализу надежности на уровне системы в процессе проектирования должен быть выполнен анализ вероятности отказов аппаратных средств.

8.2.3 Техническое обслуживание аппаратных средств СКУ класса 3

8.2.3.1 Проект аппаратных средств должен учитывать любые конкретные требования к техническому обслуживанию, содержащиеся в техническом задании на аппаратные средства.

8.2.3.2 Все электронные модули, входящие в состав оборудования, должны быть идентифицированы как пригодные для ремонта или не подлежащие ремонту.

9 Изготовление оборудования (компонентов) аппаратных средств

9.1 Изготовление оборудования (компонентов) аппаратных средств СКУ класса 1 и класса 2

9.1.1 Управление качеством при изготовлении оборудования (компонентов) аппаратных средств СКУ класса 1 и класса 2

9.1.1.1 Работы по производству компонентов должны быть включены в план по обеспечению качества или, если это не сделано, должны рассматриваться в отдельном плане по обеспечению качества при изготовлении.

9.1.1.2 Мероприятия, относящиеся к изготовлению, проводимые при проектировании (такие, как оценка процесса производства при квалификации оборудования), должны быть включены в план обеспечения качества.

Примечание — К аппаратным средствам, изготавливаемым на этапе производства, на которые распространяются положения настоящего раздела, относятся отдельные модули, сборочные узлы или оборудование в целом.

9.1.1.3 Основным соображением при определении процессов изготовления, включенным в план обеспечения качества, должна быть уверенность в том, что процесс изготовления не ухудшит способность изделия выполнять функции безопасности.

9.1.1.4 Для работ по изготовлению должны быть определены процедуры и разработаны инструкции. Данные работы включают процессы изготовления и их контроль, инспекционный контроль и испытания, осуществление независимого надзора за качеством и экспертизы, маркирование, обращение с изделием, упаковку, хранение и доставку.

9.1.1.5 Должны быть определены объем и подробное содержание процедур и рабочих инструкций, необходимых для осуществления деятельности по изготовлению, чтобы обеспечить:

- соответствие изготовленных изделий описанию и спецификации, сформированным на этапах проектирования и реализации;
- соответствие изготовленных изделий требованиям, соответствие которым было продемонстрировано исходной моделью при осуществлении программы по квалификации.

9.1.1.6 Если аппаратные средства включают компоненты, поставляемые внешними поставщиками, то оценка и отбор таких поставщиков должны основываться на их способности изготавливать и поставлять данные изделия в соответствии с описанием и спецификацией на изделия, включая требования по 9.1 и требования, установленные в плане обеспечения качества.

9.1.1.7 В тех случаях, когда проектировщик СКУ принимает решение о передаче в субподряд какого-либо процесса, влияющего на соответствие изделия установленным требованиям, должен быть обеспечен контроль за таким процессом. Тип и степень контроля за переданными в субподряд процессами должны быть определены в плане обеспечения качества.

9.1.1.8 Критерии отбора, оценки и повторной оценки внешних поставщиков и субподрядчиков должны быть определены и задокументированы (например, общая информация, такая как сфера деятельности, объем поставок, технические возможности и производственные мощности, организация обеспечения качества, наличие системного и технического аудита, финансовое положение, поведение на рынке).

9.1.1.9 Управление качеством производственных процессов должно пройти независимую сертификацию на соответствие признанным международным стандартам аккредитованными органами (например, представителями международного реестра сертифицированных аудиторов по схеме, установленной ИСО 9001).

9.1.1.10 Должно быть определено, каким образом предупреждается использование в производственном процессе изделий с истекшим сроком годности.

9.1.2 Обучение персонала, участвующего в изготовлении аппаратных средств СКУ класса 1 и класса 2

9.1.2.1 Необходимые компетенции персонала, выполняющего любые виды работ по изготовлению и контролю:

- должны быть установлены, задокументированы и должны поддерживаться на необходимом уровне; или

- в других случаях для достижения необходимой компетенции следует проводить обучение или иные подобные мероприятия. Эффективность обучения и иных мероприятий должна быть оценена и подтверждена документально.

9.1.2.2 Обучение персонала должно быть направлено на осознание актуальности и важности выполняемых им работ и информирование относительно того, какой вклад вносит их деятельность в достижение должного качества и безопасности. Кроме того, необходимо вести соответствующие записи, фиксирующие процесс обучения, тренинги, накопление навыков и опыта.

9.1.3 Планирование и организация работ по изготовлению аппаратных средств СКУ класса 1 и класса 2

9.1.3.1 План обеспечения качества при изготовлении должен быть доступен в момент начала этапа изготовления и должен поддерживаться в актуальном состоянии на протяжении всей работы по проекту.

9.1.3.2 Необходимо поддерживать взаимодействие между различными группами, вовлеченными в проектирование, реализацию и изготовление, в целях обеспечения эффективной коммуникации, четкого определения и распределения ответственности за все аспекты оборудования, относящиеся к процессу изготовления.

9.1.3.3 Должны быть реализованы эффективные механизмы коммуникации с заказчиками или проверяющими лицами с тем, чтобы определить и запланировать этапы изготовления, а также соответствующие инспекции, аудиты или средства контроля.

9.1.4 Исходные данные для изготовления аппаратных средств СКУ класса 1 и класса 2

9.1.4.1 Исходные данные для изготовления, включая критерии приемки изделия, должны быть определены на этапе проектирования и реализации в целях предоставления надлежащей информации для изготовления, испытаний и управления качеством.

9.1.4.2 Исходные данные должны включать следующую информацию:

- необходимость обеспечения независимости между работами по изготовлению и официальным описанием их содержания;
- любые требования к получению согласия заказчика с изменениями в процессе изготовления, связанными со сменой поставщиков компонентов или расходных материалов;
- любые требования к получению согласия заказчика с заменой компонентов или расходных материалов в процессе изготовления (например, припоев);
- необходимость специального обучения в связи с изготовлением оборудования, предназначенного для использования в ядерной отрасли.

9.1.4.3 Должны быть учтены любые требования, установленные в процессе проектирования, влияющие на процесс изготовления. К ним относятся любые законодательные или нормативные требования, применимые к изготавливаемой продукции, а также физические и технические характеристики.

Примечание — Могут быть использованы общепринятые промышленные стандарты с учетом класса безопасности функций, реализуемых компонентами аппаратных средств (например, промышленные стандарты ИСО и ISA, стандарты NEMA по защитным оболочкам и ограждениям, стандарты, регламентирующие классы пожарной безопасности, стандарты по материальным процессам, стандарты по методам формирования проводных соединений и т. д.).

9.1.4.4 Исходные документы должны быть критически оценены до начала работ по изготовлению.

9.1.4.5 Критическая оценка исходных документов должна показать, что требования к изделию определены и могут быть соблюдены.

9.1.4.6 Результаты критической оценки исходных документов должны быть задокументированы.

9.1.5 Закупки и комплектация при изготовлении аппаратных средств СКУ класса 1 и класса 2

9.1.5.1 Процесс комплектации коммерчески доступных компонентов для аппаратных средств СКУ класса 1 и класса 2

9.1.5.1.1 Необходимо продемонстрировать или засвидетельствовать другим подходящим способом, что все компоненты оборудования, включая платы и кожухи электронных компонентов, удовлетворяют предъявленным требованиям (например, функциональности, устойчивости к условиям среды, надежности и сроку службы).

9.1.5.1.2 Необходимо продемонстрировать, что выбранные компоненты соответствуют ожидаемым характеристикам и качеству и их выбор осуществлен в соответствии с требованиями, приведенными в 7.1.

9.1.5.2 Процесс комплектации элементов, используемых в оборудовании для СКУ класса 1 и класса 2

9.1.5.2.1 Вид и степень контроля, реализуемого в отношении поставщика или субподрядчика, а также закупаемого элемента, должны быть определены и закреплены на уровне договора, заключаемого с поставщиком.

9.1.5.2.2 Когда закупаемый элемент имеет встроенные программируемые электронные компоненты или состоит из них, должны быть установлены дополнительные требования для обеспечения жесткого управления конфигурацией и контроля версий аппаратных средств, ПО и HPD, основанные как на утвержденной квалификации, так и на записях по изготовлению. Производитель должен предоставить все сведения о любых изменениях и обеспечить оценку их влияния на безопасность.

9.1.5.2.3 Необходимо вести записи о результатах контроля и любых действиях, потребовавшихся в связи с оценкой.

9.1.5.2.4 Информация о закупках должна содержать описание элемента, который следует закупить или получить по договору субподряда, а также (в применимых случаях):

- технические условия (например, схемы, чертежи, программы контроля, программы испытаний),
- требования к приемке (например, процессы, процедуры, продукция и оборудование),
- требования к квалификации персонала;
- требования к системе управления качеством.

9.1.5.3 Верификация закупленных или приобретенных по договору субподряда элементов для СКУ класса 1 и класса 2

9.1.5.3.1 Должны быть определены и проведены инспекционные или иные мероприятия, чтобы подтвердить, что закупленный элемент, а также необходимая сопутствующая документация удовлетворяют установленным закупочным требованиям (см. 5.2.3).

9.1.5.3.2 Если верификацию предполагается проводить на территории поставщика или субподрядчика, то порядок и методы верификации должны быть указаны в информации о закупке. Должны быть установлены требования к подготовке и принятию плана (планов) заводских приемочных испытаний, требования к надзору и непосредственному наблюдению за проведением приемочных испытаний, требования к мероприятиям по конечному заводскому контролю и инспекции (например, указать ранее выявленные несоответствия и подтвердить их устранение до отгрузки на площадку).

9.1.5.3.3 Порядок проведения верификации должен содержать положения, относящиеся к мероприятиям по отслеживанию и контролю, таким как выборочные испытания, наблюдения на площадке или приостановка работ.

9.1.5.3.4 Должен быть обеспечен строгий контроль качества поступающих элементов, включая использование таможенных складов (в применимых случаях). Контроль поступающих изделий должен включать неразрушающий контроль (например, визуальный) и, в применимых случаях, интрузивный контроль, такой как электроиспытания и испытания на функциональное поведение.

9.1.5.3.5 Должны быть составлены отчеты по контролю, включающие результаты проведенных инспекций. Данные отчеты также должны обеспечивать отслеживаемость всех компонентов (производитель, номер партии).

9.1.6 Изготовление аппаратных средств СКУ класса 1 и класса 2

9.1.6.1 Контроль при изготовлении аппаратных средств СКУ класса 1 и класса 2

9.1.6.1.1 Планирование и изготовление следует проводить в контролируемых условиях.

Контролируемые условия должны включать (если применимо):

- наличие информации, описывающей характеристики изделия;
- наличие рабочих инструкций;
- наличие инструкций по качеству;
- использование и доступность подходящего оборудования и средств;
- прослеживаемость частей компонентов, внесенных в спецификацию (BOM);
- записи по срокам и распределению ответственности для персонала, участвующего в производственных операциях;
- реализацию мероприятий по выпуску, доставке, а также мероприятий, реализуемых после доставки.

9.1.6.1.2 Процессы сборки электронных модулей должны быть точно описаны.

9.1.6.1.3 Для каждого шага должна быть представлена по меньшей мере следующая информация:

- выполняемая операция;

- используемые инструменты и средства;
- данные для верификации инструментов (критерии, процессы, способы, частота проведения);
- данные проведенных верификаций (объем выборки, санкционные меры в случае обнаружения несоответствий);
- необходимый уровень подготовки операторов;
- помещения, выделенные для изготовления аппаратных средств (уровень чистоты, температура, влажность, защита от электростатических разрядов);
- применяемые стандарты.

9.1.6.2 Определение и контроль условий окружающей среды при изготовлении аппаратных средств СКУ класса 1 и класса 2

9.1.6.2.1 Требования к условиям окружающей среды в зонах изготовления и контроля изготовленных аппаратных средств должны быть определены и задокументированы.

9.1.6.2.2 Должны быть определены и задокументированы условия доступа в зоны, такие как права на доступ, требования к процедурам доступа и к одежде.

9.1.6.2.3 Должны быть разработаны и задокументированы планы по контролю условий окружающей среды в производственных помещениях и в зонах доступа к ним (например, запыленность атмосферы, создание инертной среды, регулировка температуры или влажности, контроль химического состава воды, контроль электростатических разрядов).

9.1.6.3 Валидация процессов изготовления аппаратных средств СКУ класса 1 и класса 2

9.1.6.3.1 Должны быть утверждены особые процессы обеспечения производства в тех случаях, когда результат обеспечения не может быть верифицирован путем последующего контроля или измерения, и вследствие этого недостачи могут быть выявлены только при использовании или после доставки изделия.

9.1.6.3.2 Должна быть продемонстрирована надежность данных процессов с точки зрения получения запланированных и стабильных результатов.

Должны быть установлены составляющие данных процессов, включая (если применимо):

- определенные критерии для анализа и утверждения процессов;
- одобрение оборудования и квалификации персонала;
- использование конкретных методов и процедур;
- требования к записям и валидации;
- обращение с дефектными деталями, включая возможные последствия для процесса изготовления.

9.1.6.4 Оценка приемлемости и воспроизводимости изготовленного оборудования СКУ класса 1 и класса 2

9.1.6.4.1 Произведенное оборудование должно быть оценено и признано заказчиком пригодным к использованию.

9.1.6.4.2 Признание пригодности должно основываться на управлении обеспечением качества, общем процессе квалификации аппаратных средств и успешных результатах квалификации компонентов, модулей или оборудования, которые, как правило, являются первыми в своем роде.

9.1.6.4.3 Проектировщик СКУ должен иметь возможность воспроизвести спроектированное оборудование путем изготовления и сборки на своем предприятии либо путем изготовления и сборки субподрядчиком.

9.1.6.4.4 Оценка производства должна основываться на исследованиях организации производственного процесса и технических средств, используемых изготовителем СКУ для производства изделий.

9.1.6.4.5 При внесении изменений в процесс изготовления после квалификации первого изготовленного элемента проектировщиком оборудования СКУ должен быть проведен анализ последствий таких изменений и дана оценка результатов этого анализа с целью принятия решения о необходимости проведения новой квалификации или неизменности результатов предыдущей квалификации.

9.1.6.4.6 Контроль размеров и отбор образцов для выборочного контроля должны удовлетворять требованиям ИСО 28590.

9.1.6.4.7 При приемке сборочных узлов следует применять критерии в соответствии с IPC-A-610.

9.1.6.4.8 Минимальные критерии приемки сборочных узлов должны соответствовать классу 2 по IPC-A-610.

9.1.6.4.9 Для электронных сборочных узлов класса безопасности 1 следует использовать критерии приемлемости, соответствующие классу 3 по IPC-A-610.

Настоящее положение носит рекомендательный характер, допуская ситуации, при которых требуется использовать существующие электронные платы такими, какими они спроектированы ранее. С другой стороны, любые новые проекты электронных компонентов обычно не сталкиваются с трудностями с точки зрения их соответствия критериям класса 3 по IPC-A-610.

9.1.6.4.10 Уровень согласно IPC-A-610, которому соответствуют электронные компоненты, должен быть задокументирован.

9.1.6.4.11 Персонал должен пройти обучение для ознакомления со стандартом IPC-A-610.

Официальной аттестации персонала, выполняющего изготовление и контроль, на знание положений IPC-A-610 настоящим стандартом не требуется.

9.1.6.4.12 Электронные компоненты должны подлежать контролю, предусматривающему:

- проверку доставленных компонентов на соответствие идентификации (маркировка на компонентах или катушках);
- верификацию соответствия компонентов заказу (производитель, коммерческое наименование, код даты или дата изготовления);
- верификацию компонентов на отсутствие повреждений (например, повреждения при ударной нагрузке, окисление и т. д.).

9.1.6.4.13 Коммерчески доступные компоненты, более не распространяемые официальными дистрибьюторами, компоненты от изготовителей, имеющих негативные отзывы пользователей, или компоненты, сопровождаемые недостаточно подробной документацией, должны быть подвергнуты функциональным испытаниям и охарактеризованы с целью подтверждения того, что они в состоянии выполнять свои функции при всех предусмотренных условиях (например, температура, напряжение, ток и т. д.), включая граничные условия.

Примечания

1 Контроль компонентов может быть осуществлен путем описания характеристик и проведения испытаний каждой партии (например, с общим кодом даты).

2 Компоненты, более не поставляемые официальными дистрибьюторами, как правило, распространяются через посредников. Посредник является независимым продавцом, не имеющим контрактных соглашений с оригинальным изготовителем компонентов и не выполняющим проектирование компонентов.

9.1.6.4.14 Услугами посредников следует пользоваться только в тех случаях, когда компоненты более не распространяются официальными дистрибьюторами.

9.1.6.4.15 Для оборудования класса 1 качество компонентов, приобретенных у посредника, должно быть доказано путем подтверждения соответствующей репутации и принимаемых мер по обеспечению качества.

9.1.6.4.16 Электронные сборочные узлы должны подлежать контролю, предусматривающему:

- проверку поставленных элементов на соответствие идентификации;
- проверку сертификата соответствия IPC-A-610 и соответствующего класса (может быть заменена визуальной проверкой соответствия электронного сборочного узла);
- проверку габаритных размеров, лакокрасочного покрытия, положения соединителей и креплений, а также первичных компонентов электронного сборочного узла на соответствие спецификации;
- проверку правильного функционирования электронного сборочного узла в соответствии с его спецификацией путем проведения функциональных испытаний. Функциональные испытания должны быть направлены по меньшей мере на верификацию всех первичных функций электронного сборочного узла и его критических характеристик. Данные испытания могут быть проведены как для отдельного электронного сборочного узла, так и для партии сборочных узлов;
- проверку наличия корректных версий аппаратных средств, ПО и HPD, проводимую подходящими способами.

9.1.6.4.17 Проверки следует проводить в соответствии с процедурами испытаний и в применимых случаях с использованием точно идентифицированного ПО.

9.1.6.4.18 Процедуры испытаний должны в частности обеспечивать верификацию:

- заданных значений;
- функционирования электромеханических компонентов;
- корректности функционирования во всех эксплуатационных режимах;
- корректности работы схем самотестирования и сигнализации (в тех случаях, когда это возможно);
- соответствия первичных статических и динамических электрических характеристик.

9.1.6.5 Контроль средств изготовления, контрольных и измерительных устройств при изготовлении аппаратных средств СКУ класса 1 и класса 2

9.1.6.5.1 Должны быть определены средства, необходимые для изготовления аппаратных средств.

9.1.6.5.2 Должны быть определены процессы контроля и измерений, которым следует подвергать готовые изделия с целью подтверждения их соответствия предъявляемым требованиям.

9.1.6.5.3 Должны быть установлены способы подтверждения того, что изготовление, контроль и измерения выполнены таким образом, который удовлетворяет требованиям к изготовлению, контролю и измерению.

9.1.6.5.4 При необходимости подтверждения достоверности результатов инструменты и измерительные устройства должны:

- проходить поверку и калибровку через определенные промежутки времени или перед использованием с применением для этого эталонов или установленных зарегистрированных опорных значений, предназначенных для поверки или калибровки;
- быть настроенными или проходить перенастройку при необходимости;
- иметь идентификацию, подтверждающую статус поверки;
- быть защищенными от изменения настроек, приводящих к получению недостоверных результатов измерений;
- быть защищенными от повреждений и ухудшения характеристик при использовании, техническом обслуживании и хранении.

9.1.6.5.5 Процедуры обеспечения качества должны гарантировать, что в случае признания несоответствия изготовленного оборудования установленным требованиям вследствие ошибок в процессе изготовления предприняты адекватные корректирующие действия.

9.1.6.5.6 Необходимо вести записи о результатах калибровки инструментов, используемых при изготовлении, верификации, а также о результатах предпринятых корректирующих действий.

9.1.6.5.7 Если для проведения контроля и измерений используют устройства, включающие ПО, то должно быть подтверждено соответствие устройства предусмотренному назначению. Подтверждение должно быть получено до первого использования устройства, и при необходимости соответствие подтверждают повторно.

Примечание — Подтверждение способности компьютерного ПО удовлетворять предусмотренному назначению, как правило, подразумевает верификацию и управление конфигурацией для поддержания его в пригодном к использованию состоянии.

9.1.6.6 Идентификация и прослеживаемость изделий для СКУ класса 1 и класса 2

9.1.6.6.1 В течение всего периода реализации необходимо осуществлять идентификацию изготовляемой системы, а также компонентов и материалов, используемых для ее изготовления, применяя для этого подходящие методы.

9.1.6.6.2 Статус изготовляемой системы следует контролировать на протяжении всего цикла изготовления.

9.1.6.6.3 Необходимо использовать уникальную идентификацию системы и ее составных частей, а также вести записи о вносимых изменениях в целях обеспечения прослеживаемости.

9.1.6.6.4 Должна быть составлена заключительная часть отчета об изготовлении для каждой единицы оборудования и/или сборочного узла с целью определения его конфигурации, включающая описание оборудования, составляющих его сборочных узлов, компонентов и версий. Такие документы, как правило, включают перечень составных частей сборочных узлов, планов, чертежей, схем, технических данных, ссылок на подробные документы нижнего уровня и операторов с тем, чтобы обеспечить исчерпывающее описание версии системы и/или сборочных узлов.

9.1.6.7 Защита и хранение изделий для СКУ класса 1 и класса 2

9.1.6.7.1 Система и входящие в нее части должны быть защищены во время работ по сборке, чтобы обеспечить поддержание соответствия требованиям. Защита должна предусматривать идентификацию и в применимых случаях надлежащее обращение, упаковку, условия хранения и защиты до приемочных испытаний оборудования.

9.1.6.7.2 Условия хранения компонентов, предназначенных для изготовления электронных модулей, должны предупреждать ухудшение их надежности.

9.1.6.7.3 Защиту от электростатических разрядов обеспечивают следующими способами:

- специальной упаковкой чувствительных компонентов (антистатической упаковкой) с четко различимым знаком, обозначающим опасность электростатических разрядов для упакованного изделия;

- целенаправленной защитой электронных модулей;
- снижением числа возможных источников электростатических разрядов (например, путем использования антистатических браслетов, надлежащим образом организованной защиты рабочих мест для упаковки и распаковки компонентов, использования токопроводящих материалов для покрытий пола);
- повышением осведомленности и обучением персонала.

9.1.6.7.4 Условия хранения (длительность, параметры окружающей среды) должны быть совместимы:

- со спецификацией на упаковку и защиту компонентов (например, антистатические ленты, пакеты из материалов, защищающих от влаги);
- с рекомендациями изготовителя компонентов, в частности для компонентов с ограниченным сроком годности (например, электролитические конденсаторы) или чувствительным к проникновению влаги.

9.1.6.8 Достаточность инструментов и навыков персонала при изготовлении СКУ класса 1 и класса 2

9.1.6.8.1 Требования к техническому обслуживанию инструментов и иных средств, используемых во время изготовления, испытаний и валидации, должны быть определены в процессе планирования деятельности по изготовлению и соответствовать классу безопасности функций, выполняемых компонентами.

9.1.6.8.2 Должны быть определены требования к поддержанию профессиональных навыков персонала, вовлеченного в изготовление, испытания и валидацию.

9.1.6.9 Принятие решений и контроль в случае обнаружения несоответствий при изготовлении СКУ класса 1 и класса 2

9.1.6.9.1 Несоответствия производственного процесса, выявленные во время квалификационных испытаний на внешние воздействия, верификации или изготовления, должны быть определены и зарегистрированы в соответствии с планом обеспечения качества (см. 5.2.2).

9.1.6.9.2 Необходимые изменения и принятые решения должны быть определены и зарегистрированы таким образом, чтобы их могли легко проверить третьи лица. Соответствующие записи должны отражать характер изменений, включать анализ воздействия, а также соответствующие обоснования и подтверждения.

9.1.6.9.3 Должны быть обеспечены средства контроля на производственной линии в целях проверки того, что модификации были надлежащим образом учтены, а средства контроля и процедуры испытаний были надлежащим образом адаптированы (изготовлены, идентифицированы и прошли приемочные испытания).

9.2 Изготовление оборудования (компонентов) аппаратных средств СКУ класса 3

9.2.1 Управление качеством при изготовлении оборудования (компонентов) аппаратных средств СКУ класса 3

9.2.1.1 Должны быть определены критерии отбора, оценки и повторной оценки внешних поставщиков или субподрядчиков (сфера деятельности, объем поставок, технические компетенции и производственные мощности, организация обеспечения качества, системные и технические аудиты, финансовое положение, поведение на рынке).

9.2.1.2 Управление качеством производственных процессов должно пройти независимую сертификацию на соответствие признанным международным стандартам аккредитованными органами (например, представителями международного реестра сертифицированных аудиторов по схеме, установленной ИСО 9001).

9.2.2 Обучение персонала, участвующего в изготовлении аппаратных средств СКУ класса 3

Необходимые компетенции персонала, выполняющего любые виды работ по изготовлению и контролю, должны быть определены, задокументированы и поддерживаться на должном уровне.

9.2.3 Исходные данные для изготовления аппаратных средств СКУ класса 3

9.2.3.1 Исходные данные для изготовления аппаратных средств должны быть определены на этапе проектирования и реализации в целях предоставления надлежащей информации для изготовления и управления качеством, включая информацию о критериях приемки изделия.

9.2.3.2 Исходные данные должны включать следующую информацию:

- необходимость обеспечения независимости между проведением работ по изготовлению и официальным описанием их содержания;

- любые требования к получению согласия заказчика с изменениями в процессе изготовления, связанными со сменой поставщиков компонентов или расходных материалов;

- любые требования к получению согласия заказчика с заменой компонентов или расходных материалов в процессе изготовления (например, припоев).

9.2.3.3 Ознакомление с исходными документами должно быть выполнено до начала работ по изготовлению.

9.2.3.4 При ознакомлении с исходными документами должно быть подтверждено, что требования к изделию определены и могут быть удовлетворены.

9.2.3.5 Результаты ознакомления с исходными документами и комментарии по данным результатам должны быть зафиксированы.

9.2.4 Закупки и комплектация при изготовлении аппаратных средств СКУ класса 3

9.2.4.1 Процесс комплектации коммерчески доступных компонентов для СКУ класса 3

Должны быть предоставлены достаточные свидетельства того, что все компоненты оборудования, включая платы и кожухи электронных компонентов, удовлетворяют предъявляемым требованиям (функциональность, устойчивость к условиям окружающей среды, надежность и срок службы), а их отбор осуществлен так, как описано в 7.2.

9.2.4.2 Процесс закупки элементов для оборудования СКУ класса 3

9.2.4.2.1 Вид и степень контроля, реализуемого в отношении поставщика или субподрядчика, а также закупаемого элемента, должны быть определены и закреплены на уровне договора, заключаемого с поставщиком.

9.2.4.2.2 Когда закупаемый элемент имеет встроенные программируемые электронные компоненты или состоит из них, должны быть установлены дополнительные требования, касающиеся внесения изменений в управление конфигурацией и контроля версий аппаратных средств, ПО и HPD, основанные как на утвержденной квалификации, так и на записях по изготовлению. Изготовитель должен предоставить все сведения о любых изменениях.

9.2.4.3 Верификация закупленных или приобретенных по договору субподряда элементов для СКУ класса 3

Должны быть определены и реализованы инспекция или иные мероприятия в целях получения гарантии, что закупленный элемент, включая сопутствующую документацию, удовлетворяет установленным требованиям к закупке (см. 5.3.2).

9.2.5 Оценка электронных модулей для аппаратных средств СКУ класса 3

9.2.5.1 Критерии приемки электронных сборочных узлов должны соответствовать IPC-A-610.

9.2.5.2 Минимальные критерии приемки сборочных узлов должны соответствовать классу 2 по IPC-A-610.

9.2.5.3 Уровень согласно IPC-A-610, которому соответствуют электронные сборочные узлы, должен быть задокументирован.

9.2.5.4 Персонал должен пройти обучение для ознакомления с документом IPC-A-610.

Настоящий стандарт не устанавливает требование официальной аттестации персонала, выполняющего изготовление и контроль, на соответствие документу IPC-A-610.

9.2.5.5 Электронные компоненты должны подлежать контролю, предусматривающему:

- проверку доставленных компонентов на соответствие идентификации (маркировка на компонентах или катушках);

- проверку соответствия компонентов заказу (производитель, коммерческое наименование, код даты или дата изготовления);

- проверку компонентов на отсутствие повреждений (например, повреждения при ударной нагрузке, окисление и т. д.).

9.2.5.6 Коммерчески доступные компоненты, более не распространяемые официальными дистрибьюторами, компоненты от изготовителей, имеющих негативные отзывы пользователей, или компоненты, сопровождаемые недостаточно подробной документацией, должны быть подвергнуты функциональным испытаниям и охарактеризованы с целью подтверждения того, что они в состоянии выполнять свои функции при всех предусмотренных условиях (например, температура, напряжение, ток и т. д.), включая граничные условия.

Примечания

1 Контроль компонентов может быть осуществлен путем описания характеристик и проведения испытаний каждой партии (например, с общим кодом даты).

2 Компоненты, более не поставляемые официальными дистрибьюторами, как правило, распространяются через посредников. Посредник является независимым продавцом, не имеющим контрактных соглашений с оригинальным изготовителем компонентов и не выполняющим проектирование компонентов.

9.2.5.7 Услугами посредников следует пользоваться только для приобретения компонентов, более не распространяемых официальными дистрибьюторами.

9.2.5.8 Электронные сборочные узлы должны подлежать контролю, предусматривающему:

- проверку поставленных элементов на соответствие идентификации;
- проверку сертификата соответствия IPC-A-610 и соответствующего класса (может быть заменена визуальной проверкой соответствия электронного сборочного узла);
- проверку габаритных размеров, лакокрасочного покрытия, положения соединителей и креплений, а также первичных компонентов электронного сборочного узла на соответствие спецификации;
- проверку правильного функционирования электронного сборочного узла в соответствии с его спецификацией путем проведения функциональных испытаний. Функциональные испытания должны быть направлены по меньшей мере на верификацию всех первичных функций электронного сборочного узла и его критических характеристик. Данные испытания могут быть проведены как для отдельного электронного сборочного узла, так и для партии сборочных узлов;
- проверку наличия корректных версий аппаратных средств, ПО и HPD, проводимую подходящими способами.

Контроль электронных сборочных узлов осуществляют путем осмотра и проведения необходимых измерений.

9.2.5.9 Должны быть составлены отчеты по контролю, включающие результаты проведенных проверок. Данные отчеты также должны обеспечивать прослеживаемость всех компонентов (изготовитель, номер партии).

9.2.6 Идентификация и прослеживаемость аппаратных средств СКУ класса 3

9.2.6.1 Идентификацию изготовленной системы, в том числе компонентов и материалов, использованных для ее изготовления, следует осуществлять с применением пригодных средств на протяжении всего периода реализации изделия.

9.2.6.2 Производственная документация должна описывать работы по изготовлению, хранению, инспекционному контролю и испытаниям и включать свидетельства того, что требования, приведенные в 9.2, соблюдены.

9.2.7 Защита и хранение компонентов аппаратных средств СКУ класса 3

9.2.7.1 Хранение компонентов, предназначенных для изготовления электронных модулей, должно быть организовано таким образом, чтобы не происходило ухудшение надежности компонентов.

9.2.7.2 Защиту компонентов от электростатических разрядов обеспечивают:

- специальной упаковкой чувствительных компонентов (антистатическая упаковка) с четко различимым обозначением, указывающим на опасность электростатических разрядов;
- специальной упаковкой электронных модулей;
- уменьшением числа возможных источников электростатических разрядов (например, путем использования антистатических браслетов, обеспечения надлежащим образом защищенных рабочих мест для упаковки и распаковки, покрытий пола из токопроводящего материала);
- повышением осведомленности и профессиональной подготовки персонала.

9.2.7.3 Условия хранения (длительность, параметры окружающей среды) должны быть совместимы:

- со спецификацией на упаковку и защиту компонентов (например, антистатические ленты, герметичные пакеты, защищающие от влаги);
- с рекомендациями изготовителя компонентов, особенно компонентов с ограниченным сроком годности (например, электролитических конденсаторов) или чувствительным к пребыванию во влажной атмосфере.

9.2.8 Изготовление электронных модулей для аппаратных средств СКУ класса 3

9.2.8.1 Процессы, используемые для сборки электронных модулей, должны быть точно описаны.

9.2.8.2 Для каждого этапа должна быть представлена по меньшей мере следующая информация:

- выполняемая операция;
- используемые инструменты и изделия;
- требования к верификации инструментов (критерии, процессы, способы, периодичность);
- требования к верификации изделий (объем выборки для испытаний, меры, принимаемые в случае обнаружения несоответствий);

- необходимый уровень профессиональной подготовки операторов;
- помещения, в которых следует осуществлять процесс изготовления (уровень чистоты, температура, влажность, защита от электростатического разряда);
- применяемые стандарты.

9.2.8.3 Должен быть установлен способ, позволяющий избегать использование изделий с истекшим сроком годности в процессе изготовления модулей.

9.2.8.4 При внесении изменений в процесс изготовления после квалификации первого изготовленного элемента проектировщиком оборудования СКУ должен быть проведен анализ влияния этих изменений и дано заключение о необходимости проведения новой квалификации или возможности использования результатов предыдущей квалификации вследствие их неизменности.

10 Аспекты аппаратных средств СКУ при монтаже системы

10.1 Основные положения

Настоящий раздел применим для систем всех классов безопасности.

Требования настоящего раздела к монтажу и вводу в эксплуатацию взаимосвязаны с требованиями к монтажу системы в целом, ее интеграции на площадке и вводу в эксплуатацию, дополняя эти требования, и соответствуют МЭК 61513:2011 (6.2.7) и разделу 7.

10.2 Аспекты аппаратных средств при монтаже должны быть включены в план монтажа системы.

10.3 Упаковку, обращение, транспортирование, хранение и распаковку аппаратных средств необходимо проводить таким образом, чтобы предотвратить нанесение какого-либо ущерба системе.

10.4 Перед распаковкой и монтажом системы необходимо выполнить проверку параметров окружающей среды, в которой будут монтировать систему, чтобы подтвердить их соответствие требованиям к условиям окружающей среды для аппаратных средств, как указано в 6.1.4.

10.5 Должны быть разработаны и представлены надлежащие процедуры и задокументированная информация, позволяющие провести монтаж, подключение кабелей и проводов в соответствии с проектными требованиями (включая требования, относящиеся к квалификации, требования к механическим креплениям, заземлению).

10.6 Указанная информация должна помимо прочего включать идентификацию элементов оборудования.

10.7 Оборудование должно быть смонтировано, подвергнуто автономному испытанию и приведено в рабочее состояние в соответствии с определенными процедурами до подключения к технологическому оборудованию.

10.8 Внутренние соединения оборудования должны быть осуществлены, испытаны и введены в эксплуатацию в качестве системы в соответствии с установленными процедурами до подключения к технологическому процессу.

10.9 Система в целом должна быть подключена к технологическому процессу и подвергнута специальным плановым пусконаладочным испытаниям в соответствии с требованиями, установленными в МЭК 61513.

После завершения монтажа и ввода системы в эксплуатацию, когда подтверждено соответствие всем критериям (или согласованы отклонения), управление системой может быть передано пользователю в соответствии с МЭК 61513.

11 Аспекты аппаратных средств СКУ при модификации

11.1 Основные положения

Настоящий раздел применим для систем всех классов безопасности.

Модификация проекта аппаратных средств может потребоваться для устранения недостатков исполнения или для учета новых или возникших в результате пересмотра требований к рабочим характеристикам системы. Требования настоящего раздела к модификации взаимосвязаны с требованиями к модификации системы в целом, изложенными в МЭК 61513:2011 (6.2.8 и 6.4.7), и дополняют их.

11.2 Изменения конструкции аппаратных средств, которые влияют не только на этап проектирования (за исключением любых изменений, внесенных разработчиками в процессе разработки проекта), следует контролировать в соответствии с задокументированной процедурой.

11.3 Такая процедура внесения изменений в конструкцию должна учитывать любые возможные влияния на другие аспекты проекта системы, такие как другие аппаратные средства, программное обеспечение и компоненты HPD.

11.4 Процедура внесения изменения в проект должна гарантировать, что влияние всех изменений аппаратных средств на процессы верификации, валидации и квалификации аппаратных средств и системы идентифицировано и все необходимые переделки выполнены.

11.5 Модифицированные компоненты должны быть идентифицированы согласно соответствующим процедурам контроля качества.

12 Эксплуатация и техническое обслуживание аппаратных средств

12.1 Основные положения

Настоящий раздел применим для систем всех классов безопасности.

Требования к эксплуатации и техническому обслуживанию, изложенные в настоящем разделе, взаимосвязаны с требованиями к эксплуатации и техническому обслуживанию системы в целом, изложенными в МЭК 61513:2011 и разделе 8, и дополняют их.

12.2 Требования к эксплуатации и техническому обслуживанию аппаратных средств

12.2.1 Для контроля эксплуатации и документирования деятельности по эксплуатации и техническому обслуживанию следует использовать имеющуюся официальную процедуру (или процедуры). При этом необходимо учитывать:

- предупредительные действия, необходимые для снижения вероятности внесения дефектов и возможности получения травм персоналом;
- организационную и эксплуатационную подготовку, необходимую, если деятельность по эксплуатации и техническому обслуживанию может повлиять на работу АС или готовность исполнения функций, важных для безопасности.

12.2.2 Эксплуатацию и техническое обслуживание должен выполнять квалифицированный и уполномоченный персонал в соответствии с задокументированными процедурами.

12.2.3 Процедуры должны предусматривать подтверждение (уполномоченным лицом или путем автоматизированного испытания) того, что в тех случаях, когда задачи могут иметь непосредственное влияние на безопасность, каждая задача была выполнена удовлетворительно.

12.2.4 Вся необходимая информация, такая как время и дата, выполненные замены, должна быть записана.

12.2.5 Записи, связанные с работами по техническому обслуживанию, должны быть доступны для аудита, если это необходимо.

12.2.6 В отношении компонентов, для которых предусмотрена замена только в случае их отказа, может быть использован режим профилактического обслуживания. В этом случае следует применять средства контроля, действие которых основано на наблюдении механизмов старения, чтобы обеспечить замену компонентов до истечения их срока службы.

12.2.7 Запасные части, принадлежащие эксплуатирующей организации, должны храниться на складе, отвечающем всем требованиям к условиям окружающей среды, предъявляемым для хранения данного типа деталей.

12.2.8 Срок хранения запасных частей подлежит контролю и с течением времени может быть изменен по мере необходимости в соответствии с характеристиками старения аппаратных средств.

12.2.9 Должны быть указаны любые действия, необходимые для поддержания состояния готовности запасных частей, такие как периодическая подача питания.

12.2.10 Все запасные части должны подлежать контролю конфигурации и иметь соответствующую идентификационную маркировку или ярлыки.

12.2.11 Поставки запасных частей в будущем должны быть обеспечены, насколько это практически возможно (например, за счет хранения запасных частей, гарантированных поставок или за счет доступа к производственным мощностям).

12.3 Данные об отказах аппаратных средств

12.3.1 Данные об отказах, полученные во время работы оборудования, представляют собой основной источник информации, которую можно использовать для улучшения:

- знаний о надежности компонентов (с учетом реальных условий эксплуатации);

- качества оценки надежности оборудования (путем определения фактических данных о реальных отказах в условиях эксплуатации);
- политики технического обслуживания (за счет оптимизации запасных частей, более эффективных графиков профилактического обслуживания и более строгих требований к подготовке обслуживающего персонала).

12.3.2 Данные об отказах при эксплуатации (полученные из отчетов о техническом обслуживании) должны быть зарегистрированы в банке данных об отказах.

12.3.3 Записи о техническом обслуживании должны содержать следующую информацию (если применимо и известно):

- идентификационные данные системы с неисправным компонентом;
- обстоятельства отказа и последствия отказа;
- идентификационные данные отказавшего компонента;
- расположение компонента в системе;
- описание неисправности, вызвавшей отказ;
- дату вмешательства;
- возраст отказавшего компонента;
- идентификацию лица (лиц), подавшего(их) сообщение;
- идентификацию лица (лиц), выявившего(их) неисправность.

12.3.4 Данные об отказах систем, важных для безопасности, необходимо периодически пересматривать, чтобы гарантировать, что частота отказов компонентов остается в допустимых пределах.

12.3.5 Любые статистически значимые негативные тренды в данных следует экстраполировать, чтобы обеспечить, насколько это практически возможно, что оборудование будет продолжать удовлетворительно работать в будущем до следующей оценки данных об отказах оборудования или до тех пор, пока оборудование не будет заменено (в зависимости от того, какой период наименьший).

12.3.6 Записи о техническом обслуживании должны включать данные о реальных условиях эксплуатации — температуре и влажности.

12.4 Документация по эксплуатации и техническому обслуживанию аппаратных средств

12.4.1 Инструкции по эксплуатации и техническому обслуживанию аппаратных средств должны быть представлены в руководстве по эксплуатации и техническому обслуживанию, которое обычно относится к СКУ в целом.

12.4.2 В руководстве по эксплуатации и техническому обслуживанию должна быть описана политика технического обслуживания используемого оборудования, включая идентификацию аппаратных компонентов, которые требуют регулярной проверки, повторной калибровки или замены.

12.4.3 Руководство по эксплуатации и техническому обслуживанию должно описывать любые соответствующие диагностические процессы, которые необходимо использовать для обнаружения отказа конкретных модулей.

12.4.4 Руководство по эксплуатации и техническому обслуживанию должно описывать процедуру ремонта, то есть:

- способы ремонта или замены различных подсистем, модулей и узлов;
- любые ограничения, которым будет подвергаться система во время ремонта (например, система или части системы, которые должны быть отключены);
- степень, в которой оборудование должно проходить повторную поверку после ремонта.

12.4.5 В дополнение к процедурам планового периодического обслуживания должны быть предусмотрены диагностические процедуры, где это уместно и практически возможно, которые могут быть использованы при изучении причин аномального поведения системы и идентификации отказавших компонентов.

Приложение А
(справочное)

Стандартная документация

В таблице А.1 приведен типичный перечень документов, относящихся к каждому из основных разделов настоящего стандарта, касающихся жизненного цикла безопасности аппаратных средств. Выбор и распределение информации между документами и внутри них может быть сделан в соответствии с дифференцированным подходом согласно классу СКУ.

Таблица А.1 — Стандартная документация

Документ или тематика документа	Ссылки на структурные элементы настоящего стандарта
План обеспечения качества*	5.2.2, 5.3.1
План верификации*	5.2.3.2
Документы технического задания на систему, касающиеся аспектов аппаратных средств	
Техническое задание на аппаратные средства*	6.1, 6,2
Документы, касающиеся выбора ранее разработанных компонентов	
Анализ пригодности ранее разработанных компонентов и подтверждение качества*	7.1.1, 7.1.2, 7.2.1, 7.2.2
Документы рабочего проекта и реализации системы, касающиеся аспектов аппаратных средств	
Проектная документация на аппаратные средства	8.1.6, 8.2.1
Анализы надежности аппаратных средств	8.1.3
Записи по работам, связанным с верификацией/испытаниями	5.2.3.5
Документы, касающиеся отслеживания отклонений	5.2.3.6, 5.3.2
Документы, касающиеся изготовления оборудования (компонентов)	
План обеспечения качества*	9.1.1
Процедуры и рабочие инструкции	9.1.1
Записи по компетенциям персонала	9.1.2, 9.2.2
Критерии отбора, оценки и повторной оценки внешних поставщиков или субподрядчиков	9.1.1
Обзоры исходных документов, формируемых на этапе проектирования	9.1.4, 9.2.3
Отчеты по контролю	9.2.5.9
Требования к условиям окружающей среды в зонах производства и осуществления контроля	9.1.6.2
Записи по результатам калибровки, поверки заводских измерительных приборов и предпринятых корректирующих действиях	9.1.6.5
Заключение производственного отчета	9.1.6.6.4
Записи о несоответствиях при изготовлении	9.1.6.9
Документы, касающиеся аспектов аппаратных средств, связанные с монтажом системы	
Планы монтажа*	10.2
Процедуры монтажа, прокладки кабелей и проводов*	10.5

Окончание таблицы А.1

Документ или тематика документа	Ссылки на структурные элементы настоящего стандарта
Процедура испытаний на площадке*	10.7, 10.8
Документы, касающиеся эксплуатации и технического обслуживания	
Руководство по эксплуатации и техническому обслуживанию*	12.4
Записи, формируемые при проведении технического обслуживания*	12.2
Банк данных об отказах	12.3
* Данные документы могут быть опущены, если информация, которая должна в них содержаться, включена в документы на систему.	

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC/IEEE 60780-323	—	*
IEC 60812	MOD	ГОСТ Р 27.303—2021 (МЭК 60812:2018) «Надежность в технике. Анализ видов и последствий отказов»
IEC 60880	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
IEC/IEEE 60980-344	—	*
IEC 61000 (all parts)	—	*, 1)
IEC 61025	NEQ	ГОСТ Р 27.302—2009 «Надежность в технике. Анализ дерева неисправностей»
IEC 61513:2011	IDT	ГОСТ Р МЭК 61513—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 61709	—	*
IEC 62003	—	*
IEC 62138:2018	IDT	ГОСТ Р МЭК 62138—2021 «Программное обеспечение систем контроля и управления атомной станции, выполняющих функции безопасности категорий В и С. Общие требования»
IEC 62566:2012	—	*
IEC 62566-2	—	*
ISO 28590	MOD	ГОСТ Р 50779.70—2018 (ИСО 28590:2017) «Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Введение в стандарты серии ГОСТ Р ИСО 2859»
IPC-A-610	—	**

1) IEC 61000 состоит из шести частей, каждая из которых представляет собой серию стандартов (в общем более 100). В Российской Федерации действуют 32 межгосударственных стандарта, гармонизированных с разными стандартами серии IEC 61000 с идентичной степенью соответствия: ГОСТ IEC 61000-3-2—2021, ГОСТ IEC 61000-3-3—2015, ГОСТ IEC 61000-3-11—2022, ГОСТ IEC 61000-3-12—2016, ГОСТ IEC 61000-4-3—2016, ГОСТ IEC 61000-4-4—2016, ГОСТ IEC 61000-4-5—2017, ГОСТ IEC 61000-4-8—2013, ГОСТ IEC 61000-4-9—2013, ГОСТ IEC 61000-4-10—2014, ГОСТ IEC 61000-4-12—2016, ГОСТ IEC 61000-4-13—2016, ГОСТ IEC 61000-4-14—2016, ГОСТ IEC 61000-4-18—2016, ГОСТ IEC 61000-4-20—2014, ГОСТ IEC 61000-4-27—2016, ГОСТ IEC 61000-4-29—2016, ГОСТ IEC 61000-4-30—2017, ГОСТ IEC 61000-4-31—2019, ГОСТ IEC 61000-4-34—2016, ГОСТ IEC 61000-4-39—2019, ГОСТ IEC 61000-6-3—2016, ГОСТ IEC 61000-6-4—2016, ГОСТ IEC 61000-6-5—2017, ГОСТ IEC 61000-6-7—2019, ГОСТ IEC/TR 61000-1-5—2017, ГОСТ IEC/TR 61000-1-6—2014, ГОСТ IEC/TR 61000-3-6—2020, ГОСТ IEC/TR 61000-3-7—2020, ГОСТ IEC/TR 61000-3-14—2019, ГОСТ IEC/TS 61000-1-2—2015 и ГОСТ IEC/TS 61000-3-5—2013.

Окончание таблицы ДА.1

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Официальный перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

** Соответствующий национальный стандарт отсутствует. Текст документа на русском языке доступен на http://www.ipc.org/.

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты;
- NEQ — неэквивалентный стандарт.

Библиография

IEC 60671:2007, Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing

IEC 61226, Nuclear power plants — Instrumentation, control and electrical power systems important to safety — Categorization of functions and classification of systems

IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 62340:2007, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF)

IEC 62645, Nuclear power plants — Instrumentation, control and electrical power systems — Cybersecurity requirements

IEC 63046:2020, Nuclear power plants — Electrical power systems — General requirements

ISO 9001, Quality management systems — Requirements

IAEA Safety Glossary:2018

IAEA SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants

IAEA SSR-2/1, Safety of Nuclear Power Plants: Design

AFCEN, RCC-E Ed. 2016, Design and construction rules for Electrical and I&C systems and equipment

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; аппаратные средства; аппаратные средства систем контроля и управления; требования к аппаратным средствам; жизненный цикл безопасности аппаратных средств; верификация аппаратных средств; аспекты аппаратных средств

Редактор *Н.А. Аргунова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 25.07.2024. Подписано в печать 30.07.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,12. Уч.-изд. л. 4,35.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru