ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ

ПНСТ 119—2016/ МЭК 62671: 2013

АТОМНЫЕ СТАНЦИИ

Контроль и управление, важные для безопасности. Выбор и использование промышленных цифровых устройств ограниченной функциональности

(IEC 62671:2013, IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 ПОДГОТОВЛЕН Негосударственным образовательным частным учреждением «Новая Инженерная Школа» (НОЧУ «НИШ») на основе официального перевода на русский язык англоязычной версии указанного в пункте 4 стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 45

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 8 июня 2016 г. № 41-пнст

4 Настоящий стандарт идентичен международному стандарту МЭК 62671:2013 «Атомные станции. Контроль и управление, важные для безопасности. Выбор и использование промышленных цифровых устройств ограниченной функциональности» (IEC 62671:2013 «Nuclear power plants — Instrumentation and control important to safety — Selection and use of industrial digital devices of limited functionality», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 9 мес до истечения срока его действия разработчику настоящего стандарта по адресу: vniinmash@gost.ru и в Федеральное агентство по техническому регулированию и метрологии по адресу: Ленинский просп., д. 9, Москва В-49, ГСП-1, 119991.

В случае отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «Национальные стандарты» и журнале «Вестник технического регулирования». Уведомление будет размещено также на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

a) Технические положения, основные вопросы и организация настоящего стандарта

Настоящий стандарт заостряет внимание на выборе и оценке предварительно разработанных специализированных устройств ограниченной, специфичной функциональности и ограниченной конфигурируемости для применения на атомной станции, где в эти устройства входит либо программное обеспечение, либо проекты цифровых схем, определенные с помощью языков описания аппаратуры, и где эти устройства были изготовлены согласно признанному неядерному стандарту, но не стандартам серии ПК 45А.

Настоящий стандарт предназначен для проектировщиков атомных станций, операторов АС (энергетических компаний), экспертов-системотехников и лицензиаров.

Настоящий стандарт направлен на два аспекта, которые не рассмотрены в других стандартах серии МЭК ПК 45А:

- в прочих стандартах рассматриваются аппаратные аспекты устройств, содержащих программное обеспечение, или рассматриваются сложные устройства типа PLC, содержащих программное обеспечение, где это программное обеспечение обладает потенциалом большей сложности[1)], чем в устройствах, охваченных настоящим стандартом; и
- прочие стандарты направлены на устройства, проектируемые специально для ядерных приложений, тогда как настоящий стандарт сосредоточен на факторах, необходимых для применения на атомных станциях устройств, которые не предназначены для ядерного использования.

Проектировщики систем контроля и управления для атомных станций вынуждены все чаще обращаться к подобным устройствам по таким причинам, как устаревание оборудования, малый объем ядерного рынка по сравнению с промышленным рынком и растущее число поставщиков, которые намерены проектировать по общим стандартам безопасности, таким как МЭК 61508.

Следовательно, для проектировщиков этих систем стало жизненно важным получить рекомендации настоящего стандарта, чтобы иметь возможность выбрать и оценить ранее разработанные образцы на пригодность к приложениям на атомных станциях. В настоящем стандарте предоставлено такое методическое руководство, без которого проектировщики систем контроля и управления были бы обязаны рассмотреть, каким образом интерпретировать МЭК 60880, МЭК 62138 или МЭК 62566 с этой целью.

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

МЭК 61513 является документом МЭК ПК 45А первого уровня и приводит рекомендации, применимые к контролю и управлению на системном уровне. Он дополнен рекомендациями на уровне устройств МЭК 60987 для проектирования аппаратных средств, МЭК 60880 и МЭК 62138 для программного обеспечения и МЭК 62566 для потенциально сложных устройств. Все эти стандарты направлены на специализированные ядерные проекты и применяют концепцию жизненного цикла.

МЭК 62671 является документом МЭК ПК 45А второго уровня, касающимся конкретной проблемы отбора и оценки устройств для применения на атомных станциях в случае, если ранее разработанные образцы спроектированы для неядерного использования (и, возможно, аттестованы как соответствующие общепринятым стандартам безопасности, например МЭК 61508). Кроме того, в МЭК 62671 рассмотрены только устройства, обладающие узкоспециализированной ограниченной и специфичной функциональностью и ограниченной конфигурируемостью.

МЭК 62671 рассматривают последовательно с МЭК 60880 (справочный), МЭК 62138 (справочный), МЭК 60987 (справочный) и МЭК 62566 (справочный), которые являются иными надлежащими документами ПК 45А МЭК, приводящими рекомендации о компьютеризированных системах, выполняющих функции, важные для безопасности на атомных станциях.

Более подробное описание структуры серии стандартов МЭК ПК 45А см. в перечислении d) настоящего введения.

[1)] Согласованное определение «сложности» отсутствует, но чем больший объем функциональности поддерживают устройства, тем больше сопутствующее увеличение объема кода, конфликтов за ресурсы системы и связанных с синхронизацией процессов, которые могут привести к неожиданным отказам устройства. В настоящем стандарте данные проблемы рассмотрены с охватом только устройств очень ограниченной функциональности.

c) Рекомендации и ограничения относительно применения стандарта

Важно отметить, что настоящий стандарт не устанавливает дополнительных функциональных требований к системам класса 1, 2 или 3.

Аспекты, в отношении которых в настоящем стандарте приведены требования и рекомендации:

- Использование запланированного процесса для выбора и последующей оценки ранее разработанных образцов, а также для включения аспектов интеграции устройства в системы станции.
- Критерии оценки функциональной пригодности устройства, которое содержит встроенное программное обеспечение или использует цифровые схемы, разработанные с помощью программных инструментов, таких как HDL (язык описания аппаратуры).
- Критерии рассмотрения и баланса в общей оценке для получения адекватного уровня гарантии того, что характеристики устройства будут такими, как было указано при возникшей необходимости обращения к нему.
- Аспекты безопасного применения выбранного устройства в системах станции.

Для гарантии того, что настоящий стандарт останется актуальным в будущем, особое внимание уделено принципиальным вопросам, а не конкретным технологиям.

По всему тексту настоящего стандарта сделан акцент на обзор свидетельств о наличии процессов у проектировщика и изготовителя (которые могут быть различными организациями), так как они являются организациями, которые влияют на приемлемость ранее разработанного образца для его намеченного применения. Возможно, такое свидетельство придется получить через поставщика, с которым у конечного пользователя установлен прямой контакт.

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

Стандартом высшего уровня в серии стандартов МЭК ПК 45А является МЭК 61513. Он содержит общие требования к системам и оборудованию контроля и управления, выполняющим функции, важные для безопасности на атомных станциях. МЭК 61513 формирует структуру серии стандартов МЭК ПК 45А.

МЭК 61513 содержит прямые ссылки на другие стандарты МЭК ПК 45А, рассматривающие общие темы, связанные с классификацией функций и классификацией систем, аттестацией, разделением систем, защитой от отказа по общей причине, аспектами программного обеспечения ЭВМ, аспектами аппаратных средств ЭВМ и проектированием пунктов управления. Стандарты второго уровня, на которые имеются ссылки, последовательно рассматривают вместе с МЭК 61513.

На третьем уровне стандарты МЭК ПК 45А, на которые нет прямых ссылок в МЭК 61513, — это стандарты, связанные с определенным оборудованием, техническими методами или определенной деятельностью. Как правило, документы, ссылающиеся на документы второго уровня (по общим темам), могут использоваться самостоятельно.

Четвертый уровень серии стандартов МЭК ПК 45А представляет собой Технические отчеты, которые не являются нормативными документами.

МЭК 61513 выполнен в том же формате изложения, что и основной документ по безопасности, МЭК 61508, и содержит полную схему жизненного цикла безопасности и структуру жизненного цикла системы. Касательно ядерной безопасности документ приводит интерпретацию основных требований, изложенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4, применительно к ядерной отрасли. С этой точки зрения МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 в части использования для ядерной отрасли. МЭК 61513 ссылается на стандарты ИСО, а также на документы МАГАТЭ GS-R-3, МАГАТЭ GS-G-3.1 и МАГАТЭ GS-G-3.5 по вопросам, связанным с обеспечением качества (ОК).

Серия стандартов МЭК ПК45А последовательно внедряет и детализирует принципы и основные аспекты безопасности, предусмотренные в Руководствах МАГАТЭ по безопасности атомных станций и в других документах по безопасности МАГАТЭ, в частности, в Требованиях NS-R-1, устанавливающих требования к безопасности при проектировании атомных электростанций, и в Руководстве по безопасности NS-G-1.3, рассматривающем системы контроля и управления, важные для безопасности на атомных электростанциях. Терминология и определения, используемые в стандартах ПК45А, соответствуют терминам и определениям, используемым в документах МАГАТЭ.

Примечание — Предполагается, что для проектирования систем контроля и управления на атомных станциях, которые реализуют традиционные функции безопасности (например, для решения проблем безопасности работников, защиты имущества или ресурсов, химических опасных факторов, опасных факторов процессов получения, переработки и использования энергии) будут применены международные или национальные стандарты, основанные на требованиях стандартов, например МЭК 61508.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ

АТОМНЫЕ СТАНЦИИ

Контроль и управление, важные для безопасности. Выбор и использование промышленных цифровых устройств ограниченной функциональности

Nuclear power plants. Instrumentation and control important to safety.
Selection and use of industrial digital devices of limited functionality

**Срок действия — с 2017—04—01
по 2018—03—31**

1 Область применения

1.1 Общие положения

Настоящий стандарт рассматривает определенные устройства, содержащие встроенное программное обеспечение или электронно-конфигурируемые цифровые схемы, которые не были произведены согласно другим стандартам МЭК, применяемым к системам и оборудованию, важному для безопасности на атомных станциях (далее — АС), но которые претендуют на использование на АС. Приведены требования к выбору и оценке таких устройств, в случае если они обладают узкоспециализированной[1)], ограниченной и специфичной функциональностью и ограниченной конфигурируемостью.

В соответствии с МЭК 61513 системы контроля и управления, важные для безопасности классов 1, 2 и 3, могут быть реализованы с помощью традиционного оборудования с жестким монтажом, оборудования на основе цифровой технологии (компьютеризированные или программируемые аппаратные средства) или с помощью сочетания обоих типов оборудования. Настоящий стандарт устанавливает критерии обоснования применения для выбора, оценки и использования определенных цифровых устройств, которые не были разработаны специально для использования в ядерных системах контроля и управления. Как правило, такие устройства разрабатывают с учетом соответствия МЭК 61508, и данный стандарт подтверждает, что соответствие МЭК 61508 может быть ключевым положительным фактором при аттестации неядерных элементов для использования в ядерной отрасли.

Рассматриваемые в настоящем стандарте устройства являются узкоспециальными устройствами ограниченной, специфичной функциональности, которые содержат или могут содержать элементы, активируемые программным обеспечением, или цифровые схемы, разработанные с помощью программных инструментов. Примерами служат интеллектуальные датчики, позиционеры клапанов, электрические защитные устройства или инверторы, которые содержат или могут содержать элементы, активируемые программным обеспечением, или цифровые схемы, разработанные с помощью программных инструментов. Настоящий стандарт не рассматривает аспекты программного обеспече-

[1)] Слово «специализированный» в том смысле, в котором оно используется в настоящем стандарте, относится к проектированию для одной конкретной функции, которую нельзя изменить в производственных условиях. См. 3.7.

Издание официальное

ния комплексных универсальных устройств, которые рассматриваются в других стандартах, таких как МЭК 60880 и МЭК 62138 для программного обеспечения. Настоящий стандарт обращается к вопросам, которые следует рассмотреть при оценке пригодности этих специализированных устройств ограниченной, специфичной функциональности к использованию на АС. Замысел состоит в применении дифференцированного подхода к данным проблемам, при этом к более высоким классам применяют повышенные требования.

Указанные проблемы включают в себя:

- функциональную пригодность (выполняет ли устройство требуемые функции и защищены ли соответственно данные функции от помех, исходящих от любых других функций);
- подтверждающие сведения, необходимые для демонстрации этой пригодности (например, процесс разработки, эксплуатационный опыт и зрелость устройства);
- аспекты, влияющие на интеграцию устройства в существующие системы (например, функциональная совместимость и влияние на техническое обслуживание и эксплуатацию);
- требования, связанные с обеспечением сохранения пригодности устройства на протяжении его требуемого срока службы (такого, как срок службы станции).

Настоящий стандарт опирается на другие стандарты, особенно на МЭК 60780, при рассмотрении вопросов аттестации аппаратуры, не связанных со сложностями программного обеспечения, а именно аспектов надежности, связанных с аттестацией для работы в условиях окружающей среды и отказами, обусловленными старением или физической деградацией. В качестве дополнительного руководства для анализа и оценки элементов можно использовать другие стандарты, такие как МЭК 61508, но признано, что аттестации только по одним неядерным стандартам недостаточно.

1.2 Справочная информация

Необходимость настоящего стандарта вытекает из современных тенденций в индустрии контроля и управления, включая прогрессирующее устаревание существующих устройств, используемых ныне на атомных станциях. Все более затрудняется и становится почти невозможной идентификация аналоговых устройств или замена многих существующих устройств идентичными, потому что поставщики все чаще используют микроконтроллеры, специализированные интегральные схемы (ASIC) и т. д., встроенные в рассматриваемые в качестве замены устройства, а аналоговые устройства становятся все менее доступными.

Существуют различные технические риски относительно обоснования применения данных устройств на ядерных установках, потому что:

- многие из данных устройств не дублируют точную функциональность заменяемого устаревшего устройства, обладая в некоторых случаях меньшей, а в других случаях большей функциональностью, или даже слегка иной функциональностью, которая может не соответствовать замыслу оригинального проекта;
- эти различия в функциональности не всегда очевидны. Существуют примеры проблем, которые возникли из-за отсутствия методических рекомендаций в этой области; проблемы обычно возникают из-за различия в целях проектирования между ядерными установками и промышленными приложениями, для которых проектируют оборудование;
- устройства могут обладать специфическими уязвимостями или видами отказа, которые не существовали при первоначальном оборудовании и которые нужно рассмотреть.

1.3 Назначение настоящего стандарта

Настоящий стандарт устанавливает требования к определению того, являются ли цифровые устройства промышленного качества, обладающие узкоспециализированной, ограниченной и специфичной функциональностью и ограниченной конфигурируемостью, пригодными для использования в ядерном приложении. Это потребует применения критериев, подобных применяемым к нецифровым устройствам, но в настоящем стандарте приведены дополнительные критерии, которые применимы к цифровым устройствам. Также будут учтены пределы выполнимости при условии, что в оцениваемом промышленном устройстве будут выполнены незначительные или не будет никаких изменений.

Настоящий стандарт предназначен для использования в контексте определенного приложения, для которого разработчики приложений ищут пригодные устройства для его реализации. Однако зачастую разработчик приложений вынужден рассматривать применение устройств, не предназначенных специально для ядерного применения. Цель настоящего стандарта состоит в том, чтобы помочь раз-

работчику приложений в выборе и использовании таких устройств и таким способом, который отвечает классу безопасности и требованиям намеченного приложения.

Таким образом, настоящий стандарт можно применять на различных этапах жизненного цикла проектирования системы согласно определению МЭК 61513. Настоящий стандарт можно применять на раннем этапе жизненного цикла проектирования станции, когда проектируется архитектура конкретной системы контроля и управления и наличие пригодных устройств может повлиять на проектирование системы. В случае более позднего применения, когда завершено проектирование системы, настоящий стандарт можно использовать для оценки ранее разработанного образца. Наконец, настоящий стандарт можно также применять для ситуаций реконструкции, когда система уже находится в эксплуатации и некоторые устройства необходимо заменить.

Классы 1, 2 и 3 характеризуют классифицированными наборами требований. Настоящий стандарт предназначен для интерпретации в контексте категории выполняемой функции безопасности и класса системы. Это означает, что классифицированная интерпретация требований адекватна и ожидаема. Также признано, что приемлемые режимы отказа могут весьма отличаться в каждом прикладном контексте станции, и это может определить приемлемость данного устройства или его форму использования. Предполагается, что интерпретация и строгость применения требований данного стандарта в каждом случае рассмотрены надлежащим образом.

Часто приходится сталкиваться с такой проблемой, как сопротивление поставщика предоставить доказательства правильности, например подробные сведения о внутренних функциях устройства или как оно было спроектировано. Данный вопрос следует рассматривать как можно раньше, возможно, посредством предварительной квалификации поставщиков, что может потребовать выбора других компаний-поставщиков в целях соблюдения данного стандарта.

План оценки и применения (EAP)[1)] устанавливает цели оценки и содержит руководство по интерпретации данного стандарта для конкретного устройства и приложения. В данном плане определены и обоснованы подходы, которые будут использоваться в проблематичных случаях, включая вид компенсационных мер, которые будут предприняты для решения таких вопросов, как расхождения между заданной и доступной функциональностью или отсутствие традиционного доказательства правильности.

Конечным этапом в процессе оценки является подготовка Отчета об оценке и применении (EAR). Данный отчет идентифицирует аттестуемое устройство, приложения, для которых его аттестуют, и все ограничения, которые применимы к его использованию.

1.4 Структура

Настоящий стандарт организован следующим образом:

- в разделе 5 рассматривается применимость данного стандарта и процесс оценки и определены:
- колебания функциональности устройства, охваченные данным стандартом, и
- степень гибкости и конфигурируемость устройства, охваченные данным стандартом, а также
- входные и выходные данные процесса оценки и EAP, который документально зафиксирует, как эксперт(ы) применит положения настоящего стандарта;
- содержание документа ООП, рассмотренное свидетельство и результаты анализа этого свидетельства, и сделанные выводы о пригодности устройства;
- в разделе 6 рассматриваются элементы функциональности и другие требования, которые необходимо оценить, например:
- минимальный уровень документации по разработке ранее разработанного образца;
- способность ранее разработанного образца выполнять заданную функцию(и);
- невосприимчивость основной функции ранее разработанного образца к нежелательным влияниям от излишних функций;
- способность ранее разработанного образца к функционированию при всех ожидаемых условиях окружающей среды согласно МЭК 60780 и другим указанным стандартам;
- надежность и ремонтопригодность ранее разработанного образца;
- адекватность мер по безопасности киберпространства;
- приведенная пользовательская документация;
- в разделе 7 рассматриваются критерии обеспечения уверенности в правильности проектирования и изготовления устройства, определяющие:

[1)] Требованию к плану аттестации, определенному в МЭК 61513, отвечает План оценки и применения.

- пригодность предыдущих неядерных аттестаций;
- методы, позволяющие избегать систематических отказов;
- применение жизненного цикла безопасности при проектировании устройства;
- обеспечение качества на производстве и
- разрешенные средства компенсации некоторых недостатков в подтверждение некоторых из этих проблем путем завершения дела в пользу принятия ранее разработанного образца на основе устойчивости продукта, сосредоточенного опыта эксплуатации, усовершенствований в документации или дополнительных испытаний и/или анализа;
- в разделе 8 рассматриваются критерии интеграции устройства в систему контроля и управления станции, включая:
- ограничения на способы использования устройства (например, самый высокий класс приложения, для которого он аттестован);
- модификации, которые могут понадобиться либо для устройства, либо для системы назначения, чтобы интегрировать устройство в систему назначения, и
- интеграция и ввод в эксплуатацию устройства в системах безопасности станции;
- в разделе 9 рассматриваются аспекты сохранения приемлемости устройства, а именно:
- уведомления, выдаваемые пользователям устройства проектировщиком устройства или изготовителем;
- срок поддержки устройства;
- сохранение средств обслуживания и документации;
- рекомендации для конечного пользователя.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие документы. Для датированных ссылок применяют только указанное издание ссылочного документа. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения).

МЭК 60671 Атомные электростанции. Системы контроля и управления, важные для безопасности. Испытания для проверки работоспособности (IEC 60671, Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing)

IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification (МЭК 60780:1998 Атомные электростанции. Электрическое оборудование системы безопасности. Квалификация)

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

IEC 60980:1989, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations (МЭК 60980:1989 Рекомендуемый порядок проведения сейсмической аттестации электрического оборудования систем безопасности для атомных электростанций)

IEC 60987:2007, Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems (МЭК 60987:2007 Программируемые цифровые компьютеры, используемые в системах, важных для безопасности АЭС)

IEC 61000 (all parts), Electromagnetic compatibility (EMC) (МЭК 61000 (все части) Электромагнитная совместимость)

IEC 61226:2005, Nuclear power plants — Instrumentation and control systems important to safety — Classification of instrumentation and control functions (МЭК 61226 Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления)

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

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

IEC 62138:2004, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (МЭК 62138:2004 Атомные станции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий B и C)

ISO 9001:2008, Quality management systems — Requirements (ИСО 9001:2008 Системы менеджмента качества. Требования)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **вспомогательная функция** (ancillary function): Любая функция, выполняемая ранее разработанным образцом, которая поддерживает его основную функцию.

Примечание 1 — Примерами служат функции ранее разработанного образца, используемого для поддержки функции, важной для безопасности, такой как обеспечение адекватного средства контроля его рабочих параметров или его непрерывного правильного функционирования, как того требует приложение безопасности.

Примечание 2 — См. также термины «Основная функция» и «Излишняя функция».

3.2 **подконтрольный** (auditable): Свойство документально зафиксированных подтверждающих данных, которые легко доступны для просмотра независимым персоналом.

3.3

категория функции контроля и управления (category of an I & C function): Одно из трех возможных обозначений (A, B, C) функций контроля и управления, устанавливаемое по результату рассмотрения влияния выполняемой функции на безопасность. Если функция не связана с безопасностью, то она не классифицируется.

Примечание 1 — См. также термины «класс системы контроля и управления», «функция контроля и управления».

Примечание 2 — Категории функций контроля и управления определены в МЭК 61226. Каждой категории соответствует ряд требований не только к функции контроля и управления (связанной с ее спецификацией, разработкой, внедрением, верификацией и валидацией), но и ко всей цепочке элементов, необходимых для реализации этой функции (связанной с характеристиками и соответствующей аттестацией) независимо от того, как они распределены между взаимосвязанными системами контроля и управления. Для большей ясности настоящий стандарт определяет категории функций контроля и управления и классы систем контроля и управления и устанавливает соотношение между категорией функции и минимальным требуемым классом соответствующих систем и оборудования.

[IEC 61513:2011, статья 3.4]

3.4

класс системы контроля и управления (class of an I&C system): Одно из трех возможных обозначений (1; 2; 3) систем контроля и управления, важных для безопасности, установленное в результате рассмотрения требований, предъявляемых к выполнению функций контроля и управления, имеющих разное отношение к безопасности. Если система контроля и управления не выполняет функции, связанные с безопасностью, то ее не классифицируют.

Примечание 1 — См. также термины «категория функции контроля и управления», «элементы, важные для безопасности».

[IEC 61513:2011, статья 3.6]

3.5

отказ по общей причине; ООП[1)] (Common Cause Failure; CCF): Отказ двух или более систем или элементов, обусловленный одиночным событием или причиной.

[IEC 61513:2011, статья 3.8]

[1)] Принятое в ОПБ-88/97 определение термина «отказ по общей причине» — отказы систем (элементов), возникающие вследствие одного отказа, или ошибки персонала, или внешнего или внутреннего воздействия, или иной внутренней причины.

3.6

компьютерная система (computer-based system): Система контроля и управления, функции которой в большой степени зависят от или полностью выполняются с использованием микропроцессоров, программируемого электронного оборудования или компьютеров.

Примечание 1 — Эквивалентно: программная система, программированная система.

[IEC 61513:2011, статья 3.11]

3.7 **специализированная функциональность** (dedicated functionality): Свойство устройств, предназначенных для выполнения только одной ясно определенной функции либо лишь очень узкого диапазона функций, включая, например, снятие и оповещение о значении технологического параметра или переключение источника электропитания переменного тока на постоянный ток. Данная функция (или узкий диапазон функций) является внутренне присущей устройству, а не полученной в результате программирования пользователем.

Примечание 1 — Вспомогательные функции (например, самоконтроль, самокалибровка, передача данных) могут также быть реализованы внутри устройства, но они не изменяют фундаментальную узкую область применимости устройства.

Примечание 2 — Настоящий стандарт применяется к устройствам специализированной функциональности, которые соответствуют всем заданным критериям в 5.2.2.

Примечание 3 — Слово «специализированный» в том смысле, в котором оно используется в данном стандарте, относится к проектированию для одной конкретной функции, которую нельзя изменить в производственных условиях.

3.8 **цифровое устройство** (digital device): Устройство, реализация которого основана на операциях, выполняемых с помощью сигналов с определенными, дискретными уровнями, или в котором присутствуют определенные, дискретные внутренние состояния и происходят переключения между этими состояниями.

Примечание 1 — Функции таких устройств обычно определяются процессами, которые включают в себя разработку и испытание с применением языков описания программного обеспечения или аппаратуры; такие устройства могут внутренне управляться программным обеспечением или могут состоять из специализированных интегральных схем или FPGA и т. д., сконфигурированных с помощью программного обеспечения.

Примечание 2 — Устройства, оборудование или системы, которые управляются программным обеспечением, описывают как «компьютерные», тогда как «цифровой» является более широким термином, который охватывает любое устройство, использующее цифровые схемы для реализации логики.

Примечание 3 — Цифровые устройства, разработанные для неядерной промышленности, называют промышленными цифровыми устройствами.

3.9

оборудование (equipment): Одна или более частей системы. Элемент оборудования — отдельный определяемый (обычно заменяемый) элемент или часть системы.

Примечание 1 — См. также термины «компонент», «система контроля и управления».

Примечание 2 — Оборудование может включать в себя программное обеспечение.

Примечание 3 — Термины «оборудование», «элемент» и «модуль» часто применяют как синонимы. Взаимоотношение между ними пока не стандартизовано.

Примечание 4 — Настоящее определение отклоняется от приведенного в МЭК 60780. Отклонение оправдано тем фактом, что в МЭК 61513 оборудование рассматривается как часть системы, тогда как в МЭК 60780 оборудование рассматривается как предмет аттестации.

[IEC 61513:2011, статья 3.16]

3.10

язык описания аппаратуры; HDL (Hardware Description Language; HDL): Язык, используемый для формального описания функций и/или структуры электронного элемента для документации, моделирования или синтеза.

Наиболее широко используемые языки описания аппаратуры — это VHDL (IEEE 1076) и Verilog (IEEE 1364).

[IEC 62566:2012, статья 3.6]

3.11

HDL-программируемое устройство; HPD (HDL-Programmed Device; HPD): Интегральная схема, конфигурируемая (для систем контроля и управления атомной станции) с помощью языков описания аппаратуры и сопутствующих программных инструментов.

Примечание 1 — Языки HDL и сопутствующие инструменты (например, симулятор, синтезатор) используют для реализации требований в надлежащей сборке предварительно разработанных микроэлектронных ресурсов.

Примечание 2 — При разработке HDL-программируемых устройств можно использовать предварительно разработанные блоки.

Примечание 3 — HDL-программируемые устройства, как правило, основаны на заготовках FPGA, ПЛИС или подобных микроэлектронных технологиях.

[IEC 62566:2012, статья 3.7]

3.12

функция контроля и управления (I & C function): Функция контроля, управления и/или наблюдения за определенной частью процесса.

Примечание 1 — Термин «функция контроля и управления» применяется инженерами-технологами при определении требований к функционированию контроля и управления. Функция контроля и управления определена таким образом, что она:

- дает полное представление о цели выполнения функции,
- может быть классифицирована по степени важности для безопасности,
- охватывает все составляющие от датчика до исполнительного устройства для достижения цели.

Примечание 2 — Функция контроля и управления может быть разделена на ряд подфункций (например, измерительная функция, функция управления, функция воздействия) с целью распределения по системам контроля и управления.

[IEC 61513:2011, статья 3.28]

3.13

система контроля и управления (СКУ)[1)] (I & C system): Система, основанная на применении электрической и/или электронной и/или программируемой электронной техники, выполняющая функции контроля и управления, а также функции обслуживания и наблюдения, связанные с эксплуатацией самой системы.

Термин используется как обобщающий, охватывающий все элементы системы, включая питание, датчики и другие входные устройства, линии передачи данных и другие связи, интерфейсы исполнительных устройств и других выходных устройств (см. примечание 2). Различные функции системы могут использовать как выделенные, так и разделенные ресурсы.

Примечание 1 — См. также термин «функция контроля и управления».

Примечание 2 — Элементы, входящие в состав конкретной системы контроля и управления, определяют в спецификации границ этой системы.

Примечание 3 — В соответствии с их функциональностью МАГАТЭ делает различие между системами автоматического и ручного управления, системами взаимодействия человек — машина, системами защиты и блокировки.

[IEC 61513:2011, статья 3.29]

[1)] В ОПБ-88/97 используются следующие термины: «управляющие системы нормальной эксплуатации», «управляющие системы безопасности» и «управляющие системы, важные для безопасности».

3.14

прерывание (interrupt): Приостановление процесса, например, выполнения компьютерной программы, вызванное внешним по отношению к данному процессу событием.

[IEC 61513:2011, статья 3.32]

3.15

элемент, важный для безопасности (item important to safety): Элемент, который является частью группы безопасности и/или неисправность или отказ которого может привести к радиационному облучению персонала на площадке или лиц из населения.

Элементы, важные для безопасности, включают в себя:

a) конструкции, системы и компонент системы, неисправность или отказ которых могут приводить к чрезмерному радиационному облучению персонала на площадке или лиц из населения;

b) конструкции, системы и компонент системы, которые препятствуют тому, чтобы ожидаемые при эксплуатации события приводили к аварийным условиям;

c) средства, которые предусматриваются для смягчения последствий неисправности или отказа конструкций, систем и компонентов системы.

Примечание 1 — Настоящее определение предназначено для всех аспектов ядерной безопасности.

Примечание 2 — В настоящем стандарте основные рассматриваемые элементы — системы контроля и управления или функции контроля и управления.

Примечание 3 — См. также термин «функция контроля и управления».

[IAEA Safety Glossary, 2007]

3.16 **ограниченная функциональность** (limited functionality): Синоним специализированной функциональности (см. 3.7)

3.17

полный жизненный цикл безопасности контроля и управления (overall I&C safety life cycle): Необходимый объем действий, включающий в себя оснащение всей архитектуры контроля и управления системами и оборудованием, важными для безопасности, и выполняемый в течение периода времени начиная с установления требований на основе проекта безопасности АС и заканчивая периодом, когда ни одна система контроля и управления непригодна к эксплуатации.

[IEC 61513:2011, статья 3.34]

3.18 **основная функция** (primary function): Исключительная функция (или минимальный набор связанных функций) ранее разработанного образца, которая требуется для системы, важной для безопасности, для выполнения ее функции, заявленной в анализе безопасности, и на которую опираются с целью автономного функционирования для достижения этой функции.

Примечание 1 — Согласно определению в 5.2.2 многофункциональное устройство может предложить возможность использования нескольких своих главных функций в качестве «основной функции», но такое устройство может не входить в область применения настоящего стандарта, или в любом случае будет менее предпочтительным, чем монофункциональное устройство.

Примечание 2 — См. также термины «вспомогательная функция» и «излишняя функция».

Примечание 3 — Например, можно использовать интеллектуальный усилитель для генерации и выдачи и логарифмического электрического сигнала, и линейного сигнала, каждый из которых используется для сигнала аварийного останова реактора. Эти две функции сформировали бы набор основных функций (и в целях настоящего стандарта к этому набору будет применяться термин «основная функция»), тогда как функциональность в поддержку изменения выходного масштаба или фильтрования выходных сигналов была бы вспомогательной функцией. Прочие функции, не являющиеся необходимыми для выбора устройства, такие как локальная индикация или дистанционная сигнализация посредством сетевого соединения, были бы излишними функциями.

Примечание 4 — Например, интеллектуальный датчик может быть способен к выводу сигнала, представляющего поток или уровень через аналоговый выход в диапазоне от 4 мА до 20 мА или по протоколу HART. Если проектировщик ядерного приложения решает использовать сигнал от 4 мА до 20 мА в целях безопасности, то это будет основной функцией, а остальные выходные сигналы будут излишними.

3.19

аттестация (qualification): Процесс определения соответствия системы или элементов эксплуатационным условиям. Аттестация осуществляется для установления соответствия определенного класса системы контроля и управления определенному набору аттестационных требований.

Примечание 1 — Требования аттестации вытекают из контекста конкретного класса системы контроля и управления и конкретного приложения.

Примечание 2 — Системы контроля и управления, как правило, реализуют на основе взаимодействующих комплектов оборудования. Такое оборудование может быть разработано как часть выполнения проекта, или оно может уже существовать (т. е. разработано в рамках предыдущего проекта или является серийным готовым продуктом). Как правило, аттестация «системы контроля и управления» выполняется этапами: сначала аттестацией отдельного, ранее существовавшего оборудования (обычно в начале процесса реализации системы); на втором этапе — аттестацией комплексной системы контроля и управления (т. е. окончательный полученный проект).

[IEC 61513:2011, статья 3.38]

3.20

качество (quality): Степень соответствия совокупности присущих характеристик требованиям.
[ISO 9000:2005]

3.21

обеспечение качества (quality assurance; QA): Функция системы управления, которая обеспечивает уверенность в том, что установленные требования будут выполнены.
[IAEA Safety Glossary, 2007]

3.22

требование (requirement): Выражение в содержании документа, передающее критерии, которые необходимо выполнить в случае заявления о соответствии данному документу и отклонение от которых недопустимо.
[ISO/IEC Directives, Part 2, 2011, статья 3.3.1]

Примечание 1 — В документах МЭК ПК 45А проведено различие между следующими типами требований:

Требования безопасности — требования, наложенные органами власти (законодательными, распорядительными или органами стандартизации) и проектными организациями на безопасность атомной станции с точки зрения воздействия на человека, общество и окружающую среду в течение жизненного цикла атомной станции.

Функциональные требования и требования к рабочим характеристикам — в функциональных требованиях сформулировано, какие действия должна предпринять система в ответ на конкретные сигналы или условия, а требования к рабочим характеристикам определяют свойства, например, время реакции и точность.

Эксплуатационные требования — требования к работоспособности и характеристикам станции, наложенные владельцем.

Требования к проектированию станции — технические требования к общему проекту станции для выполнения требований безопасности и эксплуатационных требований к станции.

Требования к проектированию системы — требования к проектированию индивидуальных систем для получения полного проекта станции, выполняющего требования к проекту станции.

Требования к оборудованию — требования к индивидуальному оборудованию в отношении выполнения им требований проектирования системы.

Примечание 2 — Глоссарий МАГАТЭ по вопросам безопасности издания 2007 г. содержит следующие определения:

Требуемый (требующийся), требование — требуемый (национальными или международными) законами или регулирующими положениями, либо Основами безопасности или Требованиями безопасности МАГАТЭ.

Настоящее определение МАГАТЭ удобно в рамках публикаций МАГАТЭ, но слишком узко для применения в техническом стандарте. Оно соответствует определению «требование безопасности» МЭК/ПК 45А, приведенному в примечании 1.

Примечание 3 — Подразумевается, что любые отклонения от требований будут обоснованы.

Примечание 4 — Если возникнут отклонения от требований, то эти отклонения и их обоснования будут также четко документально зафиксированы в ООП, чтобы позволить потенциальному пользователю устройства обосновать свое применение устройства или выбрать альтернативное устройство.

[IEC 61513:2011, статья 3.44]

3.23 **ограниченная конфигурируемость** (restricted configurability): Применяется к устройствам, которые можно весьма ограниченно конфигурировать, выбирая из числа относительно немногих опций способ, которым устройство будет функционировать при своем намеченном применении.

3.24

защищенность (security): Способность компьютерной системы защитить информацию и данные так, чтобы не допустить их несанкционированного прочтения или изменения другими системами и отдельными лицами, и для того, чтобы допущенные к ним системы и лица не получали отказов.

Примечание 1 — В настоящем стандарте термин «защищенность» следует интерпретировать, заменяя выражение «компьютерная система» на выражение «цифровое устройство, содержащее программное обеспечение или проекты с цифровыми схемами, определенные с помощью языков описания аппаратуры».

[IEC 61513:2011, статья 3.48]

3.25

самоконтроль (self-supervision): Автоматическое испытание рабочих характеристик аппаратной части системы и корректности программного обеспечения компьютерной системы контроля и управления.

Примечание 1 — Употребляемое в настоящем стандарте определение расширено и выходит за рамки простого испытания, включая автоматические функции, выполняемые программируемым устройством, разработанным для обнаружения (прежде всего) аппаратных отказов, которые могут быть по существу безопасными или опасными (т. е. отказы, которые препятствуют выполнению устройством своей функции безопасности), в целях преобразования их в безопасные события, либо оповещая об отказе, либо заставляя устройство перейти в безопасное состояние.

Примечание 2 — См. также термин «контрольное испытание», которое не инициализируется автоматически.

Примечание 3 — Выражение «испытания с самоконтролем» эквивалентно.

[IEC 60671:2007, статья 3.8]

3.26

программное обеспечение (software): Программы (т. е. наборы упорядоченных инструкций), данные, правила и сопутствующая документация, относящаяся к эксплуатации компьютерной системы контроля и управления.

[IEC 61513:2011, статья 3.51]

3.27 **анализ критичности программного обеспечения** (software criticality analysis): Анализ программного обеспечения с целью классификации каждой функции в программном обеспечении относительно ее потенциала вызвать опасные отказы.

3.28

дефект программного обеспечения (software fault): Ошибка программирования, содержащаяся в одном из компонентов программного обеспечения.

[IEC 61513:2011, статья 3.53]

3.29 **излишняя функция** (superfluous function): Все функции, выполняемые ранее разработанным образцом, которые не являются требуемыми функциями.

Примечание 1 — Например, основной функцией может быть считывание передаваемого давлением сигнала от 4 до 20 мА на другое устройство, а вспомогательной функцией может быть функция, поддерживающая настройку параметров фильтрования этого выходного сигнала для достижения желательной функции безопасности, тогда как излишней функцией может быть второй выходной сигнал, например сигнал напряжения, необязательный для функции безопасности.

Примечание 2 — См. также «основная функция» и «вспомогательная функция».

3.30 **контрольное испытание** (surveillance test): Инициализированное вручную сквозное испытание функции безопасности. Его можно проводить как однократное сквозное испытание или как серию перекрывающихся испытаний. Испытание инициализируется вручную, но может включать в себя автоматическое или полуавтоматическое испытательное оборудование для реализации испытания и/или регистрации результатов испытаний. Контрольные испытания выполняют в отношении основной функции(ий) безопасности устройства.

Примечание 1 — МЭК 60671 определяет «контрольные испытания» как «полный комплекс мероприятий для демонстрации того, что сохраняются функциональные возможности оборудования и систем контроля и управления, важных для безопасности, и подтверждения соответствия техническим условиям проекта». Настоящий стандарт признает, что автоматические испытания с самоконтролем являются требованием МЭК 61508 на более высоких уровнях целостности безопасности и которые отличаются от инициализированных вручную испытаний из-за большой разницы в частоте инициирования и тестовом покрытии.

Примечание 2 — Синонимом служит «проверочное испытание».

Примечание 3 — См. также «самоконтроль» («испытания с самоконтролем»), которые инициализируются автоматически.

3.31

систематический отказ (systematic fault): Отказ, обусловленный определенной причиной, который может быть исключен за счет внесения изменений в проект или в технологический процесс, эксплуатационную операцию, документацию и т. п.

[IEC 61513:2011, статья 3.60]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ASIC — специализированная интегральная схема;
CB — компьютерный;
CM — компенсирующая мера;
COTS — серийно выпускаемое изделие;
CPU — центральный процессор;
EAP — план оценки и применения;
EAR — отчет об оценке и применении;
EMI — электромагнитная помеха;
FMEA — анализ видов и последствий;
FMECA — анализ видов, последствий и критичности отказов;
FMEDA — анализ видов, последствий и диагностики отказов;
FPGA — программируемая пользователем вентильная матрица;
FTA — анализ дерева отказов;
HART — HART-протокол;
HAZOP — опасность и работоспособность;
HDL — язык описания аппаратуры;
HMI — человеко-машинный интерфейс;
HPD — программируемое устройство;
I&C — контроль и управление;
I/O — ввод/вывод;
PLC — программируемый логический контроллер;
PROM — постоянное запоминающее устройство;
QA — обеспечение качества;
VHDL — интегральных схем;
AC — атомная станция.

5 Общие требования

5.1 Общие положения

Основное затруднение с цифровыми устройствами состоит в том, что они зачастую сложные, и эта сложность создает потенциал для систематических отказов в их конструкции, в частности в их программном обеспечении или конструкции HDL-программируемого устройства; и отказы могут не обнаружиться до возникновения события, обладающего таким функциональным разрезом, который не входил в тестовый сценарий. Следовательно, главная цель настоящего стандарта состоит в указании критериев для оценки конструкции цифрового устройства, чтобы обеспечить уровень гарантии, соразмерный с классом намеченного применения так, чтобы при вызове в условиях применения устройство не оказалось неспособным к выполнению своей функции из-за систематических отказов.

С этой целью в 5.2.2 определены конкретные требования, которые необходимо соблюдать в устройстве, чтобы данный стандарт можно было применять. Затем в настоящем стандарте определен процесс и требования к оценке рассматриваемого для применения устройства на основе пригодности его функций и уровня достоверности, которые можно получить в его конструкции и эксплуатации, и во вторую очередь — уверенность, что технические требования устройства устойчивы. Также рекомендуется рассмотреть вероятность долгосрочной поддержки.

5.2 Применение настоящего стандарта

5.2.1 Общие положения

Предметом данного подраздела является оказание помощи в применении настоящего стандарта тем, кто ответственен за оценку пригодности промышленного устройства к использованию в приложении, важном для безопасности на атомной электростанции.

В настоящем подразделе приведены:

- критерии для принятия решения о применимости данного стандарта и
- принципы, связанные с определением применимости данного стандарта.

5.2.2 Критерии применимости настоящего стандарта

Необходимо, чтобы цифровое устройство, к которому может быть применен настоящий стандарт, соответствовало следующим критериям:

a) устройство представляет собой существующее цифровое устройство, которое содержит ранее разработанное программное обеспечение или программируемую логику (например, HDL-программируемое устройство) и претендует на использование в приложении, важном для безопасности;

b) основная выполняемая функция четко определена и применима только к одному типу приложения в системе контроля и управления, такому как измерение температуры или давления, позиционирование клапана, или управление скоростью механического устройства, или выполнение функции сигнализации;

c) основная выполняемая функция концептуально проста и имеет ограниченную область действия (хотя способ ее выполнения внутренне может быть сложным);

d) устройство не предназначено ни для перепрограммирования после производства, ни для изменения функций устройства в общих чертах, чтобы оно выполняло концептуально иную функцию: пользователи могут конфигурировать только предопределенные параметры;

e) если основную функцию устройства можно настроить или сконфигурировать, то эта возможность ограничена параметрами, связанными с технологическим процессом (например, диапазон процесса), эксплуатационными характеристиками (быстродействие или синхронизация), настройкой интерфейса сигналов (например, выбор диапазона напряжения или тока) или коэффициентами усиления (например, настройка области пропорционального регулирования).

Примечание 1 — Предпочтение отдают устройствам без вспомогательных функций и, в частности, без излишних функций. В случае если такие функции будут существовать в устройстве, то их идентифицируют и оценивают с точки зрения их потенциала создавать помехи для основной функции устройства согласно 6.3 и 6.5 соответственно.

Примечание 2 — Намеренно исключают устройства, обладающие способностью определять функциональность с помощью либо универсального языка, например языка С, либо с помощью специализированного языка, например многоступенчатой логики или функциональных блоков.

Примечание 3 — Невозможно определить все устройства, подпадающие под действие настоящего стандарта, но перечисленные ниже функции служат примерами, при допущении, что они обеспечивают степень конфигурируемости, сопоставимую с предполагаемой областью действия настоящего стандарта:

- датчики давления и температуры;
- интеллектуальный датчик (например, передатчик давления);
- позиционер клапана;
- электрозащитные устройства, например реле максимального напряжения/тока;
- пусковое устройство электродвигателя;
- специализированное устройство индикации (например, многосегментный полосный индикатор) или
- специализированные простые коммуникационные интерфейсы.

Примечание 4 — Невозможно определить все устройства, не подпадающие под действие настоящего стандарта, но перечисленные ниже оборудование и устройства служат примерами:

- PLC;
- устройства, снабженные программируемым языком, независимо от его ограниченной природы (исходя из числа функциональных блоков (или эквивалентов) или входов и выходов), в случае если такие устройства по своему назначению позволяют конфигурирование более чем для одного приложения (пример: одноконтурный цифровой контроллер с языком функциональных блоков).

5.3 Общие требования к процессу оценки

5.3.1 Процесс оценки

Предмет настоящего подраздела состоит в определении основных шагов, необходимых для выбора и оценки ранее разработанного образца, рассматриваемого для целевого приложения. Данные шаги показаны на рисунке 1 и уточнены в тексте ниже.

Процесс оценки и применения должен состоять из следующих шагов:

a) необходимой предпосылкой процесса оценки и применения является документирование всех функциональных и эксплуатационных требований, применимых к устройству в целевом приложении. Это может повлечь за собой перестройку проектных основ приложения[1)]. При определении требований к ранее разработанному образцу необходимо рассмотреть все нижеуказанные аспекты:

- определение назначения целевой системы или приложения в аспекте безопасности, достаточно подробное, для поддержки категоризации функции целевого приложения согласно МЭК 61226 или процесса, эквивалентного МЭК 61226 и принятого государственными органами власти;
- категории безопасности функции целевого приложения и класса системы, занятой в этом целевом приложении;
- основная функциональность, требуемая от устройства, включая функциональные и эксплуатационные требования, например, время реакции, соответствующее критериям, определенным в 5.2.2;
- все остальные конкретные свойства и характеристики безопасности, требуемые от продукта, — подобно рассматриваемым в разделе 6;

b) необходимо подготовить EAP, в котором учтены документированные функциональные и эксплуатационные требования согласно 5.3.2 и 5.3.4 и в необходимых случаях определена стратегия учета многократного использования ранее разработанного образца (выполнять ли однократную оценку для охвата всех намеченных видов использования или выполнять индивидуальные оценки).

По мере следования EAP может потребоваться пересмотр Плана исходя из полученных результатов или наличия доказательства правильности;

c) ранее разработанный образец необходимо выбирать и оценивать согласно настоящему стандарту, только если он отвечает требованиям пункта 5.2.2.

В случае если заменяется устройство для уже разработанной системы, то функциональные и эксплуатационные требования относительно фиксированы, тогда как для новой системы требования могут быть более подвижны, поскольку присутствует больше свободы в определении интерфейсов между

[1)] Несмотря на то что настоящий стандарт применяется к замене любого устройства цифровым, стоит рассмотреть некоторые конкретные соображения при замене аналоговых устройств цифровыми, например: частота дискретизации и теорема дискретизации, аналого-цифровое преобразование и помехи, обусловленные младшим разрядом, вследствие которых могут подниматься вопросы о цифровом устройстве, не воспринимающем событие, а с другой стороны, возможна усовершенствованная фильтрация при помощи цифровых методик, позволяющая цифровому устройству обнаружить событие, к которому аналоговое устройство будет невосприимчиво. Такие вопросы необходимо рассмотреть при обновлении проектных основ и требований к цифровому устройству.

устройствами. Для новых систем разработчики, скорее всего, заранее рассмотрят вероятность успеха в оценке каждого ранее разработанного образца и возможные последствия его применения в целевой системе, таким образом сужая выбор ранее разработанных образцов. При этом стираются различия между выбором и оценкой ранее разработанных образцов, но это не является причиной для того, чтобы избегать соблюдения предписанного процесса;

d) каждый ранее разработанный образец необходимо оценить согласно EAP (описание которого приведено в 5.3.2 и 5.3.4) с целью демонстрации того, что оно соответствует требованиям настоящего стандарта;

e) оценки необходимо документально зафиксировать в EAR. В данном отчете необходимо документально зафиксировать:

1) оценку ранее разработанного образца относительно каждого требования для целевого приложения согласно EAP и

2) привести ясное заключение о его приемлемости, а именно: устройство приемлемо как есть, приемлемо при некоторых конкретных условиях и/или ограничениях или неприемлемо.

В данных целях в EAR необходимо привести ссылки на конкретные полные требования в существующих и доступных документах либо необходимо включить в него документацию о перераспределенных требованиях.

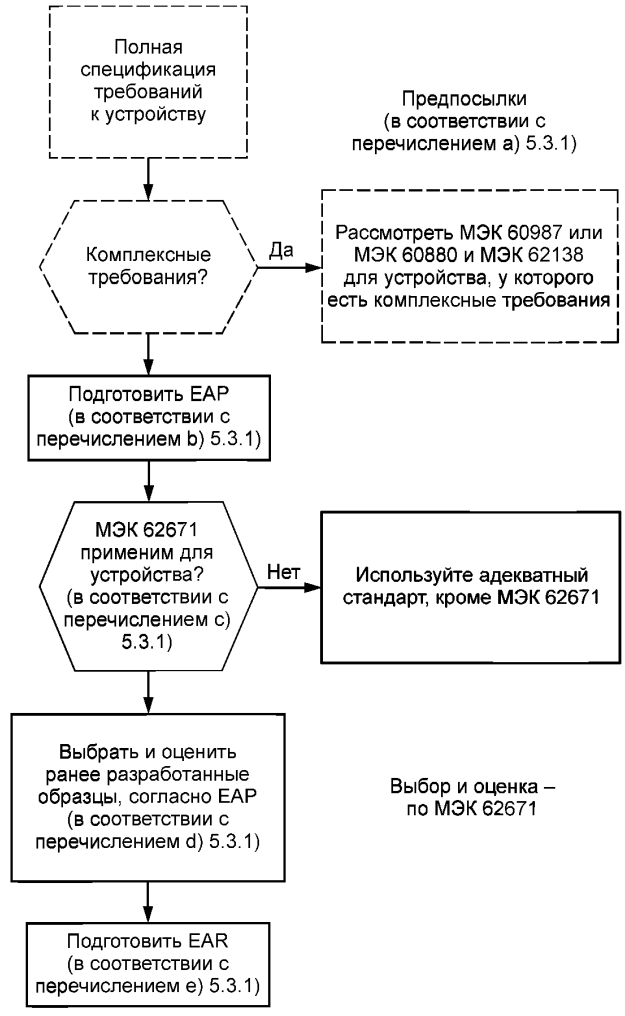

Рисунок 1 — Процесс выбора и оценки

5.3.2 План оценки и применения (EAP)

Предметом настоящего пункта служит определение цели и области действия EAP.

В EAP:

a) необходимо обосновать применимость настоящего стандарта исходя из критериев, приведенных в 5.2;

b) необходимо идентифицировать область действия и применимость работы по оценке исходя из:

- приложения (функции безопасности) или приложений и соответствующего класса или классов системы;
- в случае если рассматривается более одного приложения, аттестовать только одно приложение наивысшего класса или каждое;
- ранее разработанных образцов, подлежащих охвату в EAR;

c) следует идентифицировать технические ресурсы и их аттестацию, необходимую для выполнения работы по оценке, например:

- специалисты по приложениям безопасности для обеспечения полной спецификации требований, в частности, в ситуациях модернизации;
- специалисты по программному обеспечению для исследования восприимчивости программного обеспечения к систематическим отказам;
- специалисты по специальному аппаратному обеспечению для оценки аттестации на электромагнитную совместимость и влияние электромагнитных помех и т. д.;

d) необходимо идентифицировать критерии, определенные в подразделах раздела 6, относящиеся к целевому приложению;

e) необходимо идентифицировать рекомендуемые (там, где применяется слово «следует») критерии, определенные в подразделах раздела 7, который необходимо применять, и обосновать упущение этих критериев и расчет на компенсирующие меры, дозволяемые в разделе 7;

f) следует идентифицировать критерии выбора и их относительную важность, которая может повлиять на выбор ранее разработанных образцов, например:

- необходимый срок службы устройства в целевом приложении;
- объем поддержки от поставщика, который может потребоваться, и на какой период;
- до какой степени может понадобиться модификация целевой системы, в которую может быть интегрирован ранее разработанный образец, чтобы позволить использовать устройство с учетом его функций и типов отказа, и т. д.;

g) необходимо идентифицировать требования к обзору для EAR.

5.3.3 Отчет об оценке и применении (EAR)

Предметом настоящего подпункта служит определение области действия и содержания EAR.

В EAR:

a) необходимо документировать результаты оценки;

b) необходимо документировать причины, которые обоснуют применение настоящего стандарта, исходя из критериев применимости, приведенных в 5.2.2;

c) необходимо определить область действия и применимость работы по оценке и приведенной в EAR оценки, исходя из:

- конкретного целевого приложения (функции безопасности) и класса системы;
- при необходимости — более высокий класс, по которому оценивалось устройство;
- охватываемые EAR ранее разработанные образцы, включая точную идентификацию ранее разработанного образца, включая название продукта, номер версии программного обеспечения и элементов аппаратуры, конфигурацию и любые прочие элементы или опции, которые могут относиться к оценке;

d) необходимо подытожить или сослаться на ключевые функциональные и эксплуатационные требования (включая те, которые, возможно, придется обновить), которые влияют на приемлемость устройства, целевой класс, безопасные виды отказа и критерии экологических условий эксплуатации;

Примечание 1 — В случае если присутствуют отклонения от требований, то эти отклонения и их обоснование так же четко документируют в EAR, чтобы позволить потенциальному пользователю устройства обосновать свое применение устройства или выбрать альтернативное устройство.

e) необходимо документировать пределы надежности, достижимые устройством самостоятельно или в избыточной конфигурации;

f) необходимо документировать критерии отбора, идентифицированные в EAP;

g) необходимо в него включить (или привести ссылки, если они доступны для просмотра) все документы, используемые для проверки каждого этапа разработки устройства, включая стратегию верификации и проведенные испытания; либо, в ином случае, включить ссылки на эти документы при условии, что ссылочные документы доступны стороннему эксперту;

h) необходимо документировать способ применения критериев, определенных в пунктах разделов 6—9, согласно 5.3.4 и привести обоснование относительного ранжирования важности или упущения этих критериев;

i) необходимо документировать необходимые компенсирующие меры для рассматриваемого целевого приложения(й), чтобы охватить тот случай, в котором ранее разработанный образец либо не отвечает всем требованиям о соответствии, либо оригинальное доказательство соответствия считается недостаточным.

Потенциальные компенсирующие меры могут включать в себя дополнительные испытания, усовершенствования в документации, добавочные контрольные испытания при эксплуатации, строгие ограничения на использование устройства (например, использовать только в системах с определенными функциональными свойствами), запрет определенных опций или модификации целевой системы либо весьма ограниченные модификации самого устройства, как указано в разделе 8;

j) необходимо идентифицировать все модификации, подпадающие под действие 8.3 и 8.4. которые могут понадобиться устройству или целевой системе в целях интеграции ранее разработанного образца в целевую систему(ы) и сохранения приемлемости согласно предыдущим пунктам. Любые такие модификации устройства необходимо ограничить по области применения и не затрагивать разработку программного обеспечения или HDL-программируемых устройств, чтобы устройство сохраняло свою оригинальную функцию, иначе это устройство перестанет быть стандартным промышленным устройством, подпадающим под действие настоящего стандарта;

Примечание 2 — Примерами такой модификации служат замена резистора согласования по импедансу, изменения крепежного кронштейна или замена коммутируемого элемента переключателем или потенциометром.

k) необходимо идентифицировать все ограничения, накладываемые на применение устройства в каждом приложении, и класс, для которого оно приемлемо;

l) необходимо идентифицировать меры (и их адекватность), рекомендуемые в целях гарантии того, что при применении ранее разработанного образца соблюдаются все ограничения и рекомендации, приведенные в EAR;

m) необходимо изложить окончательное заключение о приемлемости ранее разработанного(ых) образца(ов) для применения в каждом из своих целевых приложений, выражаемое в следующих терминах:

- ранее разработанный образец приемлем как есть,

или

- ранее разработанный образец приемлем при перечисленных условиях,

или

- ранее разработанный образец не приемлем.

5.3.4 Применение положений настоящего стандарта

Предметом данного подпункта является указание о том, как применять требования, представленные в разделах 6—9 при оценке цифровых устройств специализированной функциональности согласно определению в 3.7 для применения в заданном приложении:

a) необходимо обосновать применимость настоящего стандарта исходя из критериев применимости в 5.2.2;

b) необходимо выполнять оценку ранее разработанного образца на основе намеченной функции и ее категории или намеченного приложения и его класса;

c) необходимо документально фиксировать доказательства для демонстрации функциональной и эксплуатационной пригодности ранее разработанного образца согласно определению в разделе 6 на основе всех применимых критериев в этом разделе;

d) необходимо документально фиксировать доказательства для демонстрации правильности, на основе комбинированной качественной оценки всех применимых критериев в разделе 7 согласно EAP;

e) в ходе оценки необходимо идентифицировать все ограничения, которые необходимо применять, чтобы его использование ограничивалось рамками доказательств, документально зафиксированных согласно разделу 7;

f) в ходе оценки необходимо идентифицировать все ограничения, которые необходимо применять для безопасного использования ранее разработанного образца в целевом приложении (см. раздел 8);

g) в доказательстве необходимо продемонстрировать, что результаты оценки можно сохранять на протяжении адекватного периода времени, с учетом срока службы станции и соответствующих планов по замене оборудования, на основе всех применимых критериев в разделе 9.

6 Критерии функциональной и эксплуатационной пригодности

6.1 Общие положения

Критерии функциональной и эксплуатационной пригодности рассматривают следующие вопросы:

- выполняет ли ранее разработанный образец требуемые функции[1)];
- выполняет ли оно только эти функции (или, как вариант, показано ли, что не требуемая функциональность не вмешивается в выполнение требуемых функций);
- выполняет ли оно свои функции с приемлемой надежностью и определенными приемлемыми видами отказа и
- зафиксирована ли эта функциональность документально надлежащим образом.

Необходимо, чтобы в ходе анализа и/или испытаний и обзора спецификаций сопрягаемых устройств каждый применимый критерий был продемонстрирован как надлежащий. Данную демонстрацию необходимо документировать.

6.2 Функциональная компетенция основной функции

Основная функция или функции ранее разработанного образца должны отвечать функциональным требованиям, вытекающим из требований станции и системы. В случае если ранее разработанный образец будет установлен в намеченном приложении:

a) необходимо, чтобы ранее разработанный образец был способен работать в полном диапазоне технологических сигналов станции и во всей эксплуатационной области деятельности, указанной для намеченного приложения;

b) необходимо, чтобы ранее разработанный образец продемонстрировал требуемую точность и воспроизводимость во всем данном диапазоне;

c) необходимо, чтобы ранее разработанный образец продемонстрировал требуемую скорость отклика и приемлемую обработку цифровых сигналов (определенную исходя из соответствующих критериев, например частоты дискретизации, временной задержки, времени нарастания фронта импульса, полосы пропускания, характеристик фильтра, таких как частота излома, шумоподавление и т. д.);

d) в случаях, когда важна функция преобразования в диапазоне частот (например, в приложении замкнутого цикла), необходимо, чтобы ранее разработанный образец продемонстрировал адекватное усиление и сдвиг фазы во всем рассматриваемом диапазоне частот;

e) необходимо четко определить виды отказа, и в этих видах отказа необходимо установить значения выходных сигналов в заранее определенные выходные состояния (например, обрыв цепи, либо увеличение или уменьшение выходных сигналов, либо равновесное состояние «как есть» на выходе), которые либо изначально безопасны в целевом приложении, либо их можно обнаружить и преобразовать в состояние, безопасное в приложении, либо в случае, если их нельзя ни обнаружить, ни преобразовать в состояние, безопасное в приложении, они должны обладать приемлемо низким уровнем вероятности;

f) в целях приведенного выше перечисления e) необходимо проанализировать виды отказа с точки зрения влияния ранее разработанного образца на систему, в которой оно будет установлено, с учетом всех факторов, которые могут повлиять на виды отказа (см. также 6.7). Особое внимание следует уделить отказам по общей причине, особенно тем, что касаются других устройств (возможно, в других классах), роль которых отражается в отчете по анализу безопасности как защита от одинаковых инициирующих событий.

[1)] Как правило, ранее разработанные образцы оценивают для приложения на основе предполагаемого соответствия функциональным требованиям к приложению. Данное положение содержит указания по рассмотрению критериев, чтобы убедиться в том, что при оценке ранее разработанного образца учтены все надлежащие критерии.

6.3 Вспомогательные функции

К вспомогательным функциям ранее разработанного образца относятся функции, не являющиеся частью основной функции устройства, но которые способны настроить параметры основной функции таким образом, чтобы оно могло выполнять свою обязательную функцию безопасности или чтобы повысить общую надежность устройства, например, посредством самоконтроля.

a) Для приложений классов 1 и 2 необходимо показать посредством анализа (и/или испытания, если это можно сделать достаточно убедительно), что ни работа, ни режим отказа вспомогательных функций не могут помешать выполнению основных функций, за исключением указанных случаев (например, путем выполнения вручную изменений уставок), или перевести устройство в состояние, которое является безопасным в контексте приложения.

Примечание 1 — Тип отказа, который считается «безопасным», зависит от приложения и не всегда является нормально закрытым или нормально открытым контактом. Некоторые примеры приведены в 7.2.

b) Необходимо, чтобы вспомогательные функции, связанные с настройкой параметров основных функций, отвечали требованиям 6.4.

c) Для приложений класса 3, в которых два или более устройств определены как эквивалентные во всех прочих отношениях, необходимо выбрать устройство, на котором с наименьшей вероятностью негативно отразятся отказы вспомогательной функции. Число, вероятность и тяжесть постулированных отказов вспомогательной функции необходимо использовать как факторы при сравнении.

d) В случае если для связи с ранее разработанным образцом используется внешнее устройство более низкого класса, то ни работа, ни отказ внешнего устройства не должны непредвиденным образом помешать основной функции ранее разработанного образца.

Примечание 2 — Данное требование основано на требовании к обеспечению связи в МЭК 61513, где не допускается, чтобы система более высокого класса была непреднамеренно затронута системой более низкого класса. В связи с этим связь между устройствами разных классов, как правило, односторонняя (например, связь с системой мониторинга, которая не может повлиять на систему классом выше), либо соединение включают лишь временно. Кроме того, системы более высокого уровня, как правило, тестируют после короткого периода двусторонней связи, а двустороннюю связь контролируют таким образом, что одновременно подключен только один канал системы более высокого уровня.

6.4 Конфигурируемость

Необходимо, чтобы функции ранее разработанного образца, которые можно настраивать, и вспомогательные функции, обеспечивающие эту конфигурируемость, вместе отвечали следующим требованиям:

a) конфигурационные параметры основных функций необходимо ограничить в отношении возможности включить/отключить (активировать/деактивировать) масштабирующие настройки или регулировки (например, калибровка технологического диапазона и объемов, настройки усиления или затухания и т. д.);

b) для системных приложений классов 1 и 2 в защиту конфигурации необходимо включить умышленные конструктивные особенности, чтобы понадобилось более одной ошибки человека, прежде чем зафиксируется ошибка в задании параметра конфигурации;

Примечание 1 — Обычной практикой является проверка влияния на основную функцию устройства после любого изменения параметров ее конфигурации.

c) параметры конфигурации основных функций необходимо защищать от случайного, вредоносного или несанкционированного изменения в соответствии с общим планом по обеспечению безопасности ядерной установки (см. МЭК 61513, пункт 5.4.2). В такие средства защиты необходимо включать защиту паролем, если ее поддерживает ранее разработанный образец.

Допускается незащищенный доступ только на чтение параметров конфигурации, при условии что этот доступ только на чтение отвечает требованиям по невмешательству во вспомогательную функцию, как в нижеприведенном перечислении d).

Для систем класса 1 ограничения физического доступа включают в себя ограничения доступности, такие как запирающиеся шкафы или аппаратные. (Данное требование распространяется на установку, а не на сам ранее разработанный образец, и, следовательно, ответственность возлагается на конечного пользователя.);

d) в случае если необходимо сконфигурировать дополнительные или излишние функции так, чтобы они не мешали основной функции, эти параметры конфигурации необходимо защитить, как в перечислениях b) и c);

e) необходимо обеспечить возможность проверки устройства после того, как были изменены его параметры конфигурации, чтобы убедиться в правильности выполненных изменений;

f) если устройство предоставляет операторам визуальный доступ к параметрам конфигурации или доступ с поддержкой изменений, то устройство должно обеспечивать возможность доступа только к тем параметрам конфигурации, которые необходимы им для выполнения своих служебных обязанностей;

g) в случае если устройство предоставляет операторам доступ к параметрам конфигурации с поддержкой изменений, все входные данные оператора должны укладываться в применимый диапазон данных и проходить проверки их достоверности и/или пределы, соответствующие приложению;

h) в случае если требуется, чтобы параметры конфигурации и любые необходимые сопутствующие логические состояния автоматически восстанавливались после сбоя питания, частично или полностью, и чтобы это свойство можно было конфигурировать, эти параметры конфигурации необходимо защищать, как в перечислениях b) и c).

Неотъемлемые части фильтров или ПИД-контроллеров являются типичными источниками всплеска в выходном сигнале при возобновлении работы после мощностного переходного процесса;

i) в случае, если устройство работает в системе с каналами, необходимо предусмотреть, чтобы одновременно только один канал избыточной системы мог подвергнуться изменениям конфигурации.

Примечание 2 — Указанное характерно для систем классов 1 и 2.

6.5 Излишние функции

К излишним функциям ранее разработанного образца относятся функции, не являющиеся ни частью обязательной функции безопасности устройства, ни его необходимыми вспомогательными функциями. Несмотря на то, что излишние функции часто являются неотъемлемыми частями устройства, их присутствие означает возможную излишнюю сложность и дополнительные потенциальные виды отказа, которые нежелательны в приложениях более высоких классов.

a) Для приложений классов 1 и 2 необходимо показать в ходе анализа (и/или испытания, если его можно провести достаточно убедительно), что ни один вид отказа излишних функций не может помешать основной функции.

b) Для приложений классов 1 и 2 необходимо показать в ходе анализа (и/или испытания, если его можно провести достаточно убедительно), что при всех эксплуатационных условиях излишние функции могут быть сконфигурированы (или изначально функционировать) так, что не смогут вмешиваться в основную функцию.

c) Для приложений класса 3, где два или более устройств определены как эквивалентные во всех прочих отношениях, необходимо выбрать устройство, с наименьшей вероятностью затрагиваемое излишними функциями или их отказами. Число, вероятность и тяжесть постулированных отказов излишней функции необходимо использовать как факторы при сравнении.

d) Для приложений классов 1 и 2 если нельзя показать невмешательство излишней функции в основную функцию согласно перечислениям b) и c), то она должна отвечать всем требованиям к проектированию с учетом требований безопасности, как это необходимо для основной функции(й).

e) Для приложений классов 1 и 2 необходимо показать в ходе анализа (и/или испытания, если его можно провести достаточно убедительно), что при всех эксплуатационных условиях ни работа, ни отказ внешнего устройства, находящегося в состоянии связи с ранее разработанным образцом, не должны быть способны вмешаться непредвиденным образом в основную функцию ранее разработанного образца. Если это невозможно показать, то необходимо обеспечить возможность испытания основной функции ранее разработанного образца после такого использования каналов связи с внешним устройством.

Примечание 1 — См. примечание 2 в подразделе 6.3.

f) Необходимо устранить излишние функции, отдав предпочтение минимизации числа вспомогательных функций.

Примечание 2 — Подраздел 8.3 применяют к модификациям устройства.

6.6 Ошибкоустойчивость аппаратуры

Ошибкоустойчивость аппаратуры оценивается посредством функциональной аттестации и аттестации по условиям окружающей среды (также называемых аттестацией аппаратуры) и необходима для гарантии того, что ранее разработанный образец будет выполнять свои функции в любых условиях окружающей среды (как при нормальной эксплуатации АС, так и во время аварии и после нее), в которых оно должно функционировать.

МЭК 61513 рассматривает устойчивость аппаратуры в 6.4.2.1 и приводит ссылки на МЭК 60780 и МЭК 60980, которые в свою очередь ссылаются на прочие стандарты по мере необходимости. МЭК 61513 разрешает аттестацию на промышленные условия для устройств, которые используют в приложении 3-го класса, но требует документального подтверждения для запроса на эксплуатацию в нештатных условиях окружающей среды. Один из способов достичь этого состоит в применении МЭК 60780.

Примечание 1 — В МЭК 61513 также приведены ссылки на МЭК 60987 для заказных компьютерных систем в приложениях классов 1 и 2.

a) Ошибкоустойчивость ранее разработанного образца необходимо оценить с точки зрения всех условий окружающей среды (температура, давление, влажность, излучения, электромагнитные помехи) и длительности этих условий, которым он может подвергнуться и в которых ему предназначено выполнять свою функцию. (Сюда могут входить аварийные условия внутри защитной оболочки реактора.).

b) Для аттестации ранее разработанного образца необходимо оценить ошибкоустойчивость устройства исходя из ссылочных стандартов, указанных ниже; и в случаях, где соответствие стандарту документально не зафиксировано, этот недочет необходимо проанализировать и обосновать, либо необходимо предусмотреть компенсационные меры для решения следующих вопросов:

- температура и влажность в соответствии с МЭК 60780 для 1-го и 2-го классов и в соответствии с МЭК 61513 для 3-го класса;
- излучения;
- вибрации и сейсмические условия в соответствии с МЭК 60980;
- невосприимчивость к электромагнитным помехам в соответствии со стандартами серии МЭК 61000;

Примечание 2 — МЭК 62003 охватывает электромагнитные помехи и применяется для систем, важных для безопасности атомных станций, и ссылается на большое число частей МЭК 61000-4. МЭК 61000-6-2 представляет собой нормальный промышленный стандарт.

- пыль и аэрозольные частицы.

c) Для аттестации ранее разработанного образца необходимо также рассмотреть влияние ранее разработанного образца на остальные устройства в системе, где он будет установлен. Это может потребовать изменения устройства или оценки других устройств в соответствии с пунктом a) выше, учитывая присутствие ранее разработанного образца в своей рабочей среде. Принимается во внимание следующее:

- вибрации, вызываемые ранее разработанным образцом;
- тепло, выделяемое ранее разработанным образцом;
- электромагнитные помехи, производимые ранее разработанным образцом, и
- влияние на сейсмическую аттестацию конструкции, в которой эти устройства будут установлены.

6.7 Надежность, ремонтопригодность и контролепригодность

Надежность, ремонтопригодность и контролепригодность — это связанные между собой свойства устройства, так как частота испытаний определяется в значительной мере частотой случайных отказов, присущих рассматриваемому устройству или системе, и требуемой вероятностью отказа по запросу. Ремонтопригодность играет важную роль в сокращении времени ремонта и возможности избежать недостатков обслуживания, которые могут привести к отказам.

Требования к разработке периодических испытаний и самодиагностики (самоконтроля) рассматриваются в МЭК 60671. В данном разделе освещаются вопросы, касающиеся испытаний и ремонтопригодности в целях выбора, оценки и применения ранее разработанного образца.

FMEA и его расширения, такие как FMEDA и FMECA, являются широко используемыми методами систематического анализа устройства с целью определения видов его аппаратных отказов, их частоты и влияния. Прочие методы включают в себя FTA.

Необходимо оценить ранее разработанный образец, а результаты оценки — документально зафиксировать с учетом критериев, перечисленных ниже:

a) необходимо выполнить анализ для определения (или подтверждения) видов отказа устройства и определить, насколько они безопасны или опасны в контексте предполагаемого применения.

Виды отказа интерпретируют исходя из назначения устройства и влияния на безопасность станции. Может потребоваться провести различие между необходимостью отказа под напряжением и при отключении питания, отказа при нарастании и снижении значений или как есть, или немедленно оповестить об отказе, так чтобы оперативный персонал мог оценить влияние на безопасность станции;

b) для намеченных приложений классов 1 и 2 в ходе анализа следует показать, что приемлемо большая доля аппаратных видов отказа четко определена, их обнаруживают и о них оповещают;

c) для намеченных приложений классов 1 и 2 в ходе анализа следует показать, что подмножество отказов, которые могут быть опасны в приложении, имеет приемлемо низкую вероятность для этого приложения;

d) в случае приложений, где требования включают в себя количественные частоты отказов, необходимо использовать количественный анализ для определения частот отказов и в ходе анализа необходимо показать, что приемлемая доля аппаратных видов отказа, которые могут быть опасны в приложении, обнаруживается, и о них оповещают или своевременно преобразуют их в безопасные отказы с приемлемо низкой вероятностью, так чтобы соблюдались требования приложения;

Примечание 1 — Примерами количественных методов служат FTA и FMEDA. См. также 5.3 в МЭК 60987.

Примечание 2 — В стандартах, включая МЭК 61508, дается представление об этих методиках.

Примечание 3 — Важность обнаружения отказа при заданных временных ограничениях должна позволять корректирующее ручное действие и замену устройства бездефектным в пределах достаточно короткой задержки, соответствующей цели готовности для функций безопасности.

e) условия в проекте по самоконтролю и периодическим контрольным испытаниям устройства не должны представлять угрозу непреднамеренного вмешательства в защиту основной функции устройства от помех, исходящих от вспомогательных или излишних функций, или представлять угрозу ненадлежащего изменения конфигурационных параметров;

f) если устройство обладает возможностью самоконтроля, то об обнаружении отказа необходимо сигнализировать, оповещать или реагировать посредством перевода выходных сигналов в состояние, которое безопасно в контексте приложения;

g) периодические испытания, которые по определению должны демонстрировать длительную готовность устройства, необходимо разработать так, чтобы максимизировать возможности обнаружения отказов, которые не обнаружены с помощью самоконтроля;

h) при оценке следует рассмотреть условия для испытаний ранее разработанного образца, в частности, требуется ли от этих испытаний сложность, включая следующие критерии:

- процедуры и интервалы технического обслуживания и контрольных испытаний;
- сложность и частота требуемых испытаний;
- практичность осуществления испытаний на мощности;
- оценка программных инструментов, необходимых для испытаний;

i) необходимо идентифицировать специфичные элементы, ограничивающие срок службы (например, алюминиевые или электролитические конденсаторы), чтобы обеспечить основу для замены элемента или устройства прежде, чем ожидаемая частота отказов устройства приведет доказательство окончания срока службы.

Примечание 4 — Элементы затронуты в большей или меньшей степени различными условиями (например, температура, излучение, вибрация и т. д.), и это может привести к другому набору элементов, ограничивающих срок службы, в зависимости от приложения.

6.8 Безопасность киберпространства

Ранее разработанный образец и его сопутствующую конфигурацию, техническое обслуживание или испытательные инструменты необходимо включить в оценку безопасности киберпространства его главной системы.

Примечание 1 — В МЭК 62645 приведены требования к программам безопасности киберпространства.

Примечание 2 — В МЭК 61513 приведены требования к защищенности на уровне архитектуры контроля и управления и индивидуальной системы контроля и управления.

Примечание 3 — В МЭК 60880 приведены требования к защищенности программного обеспечения для приложений класса 1, а в МЭК 62138 приведены требования к защищенности программного обеспечения для приложений классов 2 и 3.

6.9 Пользовательская документация по безопасности

Для ранее разработанного образца необходима поддержка в виде проектной и верификационной документации (см. 7.4.6) и инструкций по его безопасному применению. Безопасное применение устройства означает соблюдение целей безопасности, заложенных в приложении, учитывая способ установки, конфигурацию и техническое обслуживание устройства в надлежащем соответствии с документацией, предоставляемой поставщиком устройства.

a) Документацию пользователя по безопасности можно разделить на следующие документы:

- Руководство по технике безопасности — документ или указатель на документы, в которых зафиксированы все требования к безопасному использованию и применению устройства, в том числе точная идентификация, включая идентификатор версии устройства;
- Инструкция по установке — документ, который определяет, как необходимо установить устройство и подключить к другим устройствам, чтобы обеспечить его работоспособность в соответствии с функциональной спецификацией;
- Руководство пользователя или руководство по эксплуатации — документ, который определяет, как штатный пользователь будет взаимодействовать с устройством (например, как оператор станции будет читать некое отображение данных и изменять некие параметры, которые ему разрешено изменять);
- Руководство по техническому обслуживанию — документ, который охватывает все аспекты обслуживания устройства на предприятии: меры безопасности для персонала, меры безопасности для системы, испытания устройства по месту установки, вывод устройства из эксплуатации и возврат в рабочее состояние.

Примечание — Точные требования к документации, например, конкретное название или область действия каждого документа, будут зависеть от конкретной эксплуатирующей.

Настоящий стандарт не требует конкретного названия или определения области действия каждого документа; скорее он требует, чтобы предмет был документально зафиксирован в комплекте документов:

b) с целью правильного и безопасного использования ранее разработанного образца в документах, указанных в вышеприведенном пункте a), необходимо в совокупности привести следующую информацию:

- полные сведения о версии;
- документация об основной функции в плане общей функциональности как «черного ящика», в том числе специфические эффекты параметров конфигурации, интерфейсы устройства, поведение при включении питания, поведение во время прерывания подачи питания, влияние отказов, отклик во временном и частотном диапазоне (если возможно), скорость нарастания выходного напряжения, входные и выходные сопротивления и диапазоны и др.;
- документация об основной функции в части видов отказа и индикации отказов;
- документация о вспомогательных и излишних функциях в плане функциональности, включая в соответствующих случаях средства конфигурации для предотвращения вмешательств в основную функцию;
- требования о функциональной целостности, такие как самонаблюдение для выявления сбоев аппаратуры, и действия, предпринимаемые при обнаружении отказа (в отличие от функциональных требований);
- ограничения по условиям окружающей среды и ограничения по ошибкоустойчивости устройства, а также элементы, ограничивающие срок службы;
- все процедуры технического обслуживания и соответствующие меры предосторожности;
- все рабочие процедуры и соответствующие меры предосторожности;
- все требования и процедуры периодических контрольных испытаний и соответствующие меры предосторожности;
- любая иная информация, важная для безопасного использования прибора, и соответствующие меры предосторожности.

7 Критерии общей надежности — сведения, подтверждающие правильность

7.1 Общие положения

Предметом данного раздела является предоставление рекомендаций в отношении:

- сбора и оценки сведений, подтверждающих, что ранее разработанный образец пригоден к использованию в приложении, важном для безопасности АС, на основании процессов при его проектировании и производстве; и
- средств, которые можно использовать для компенсации любых недостатков в таких доказательствах правильности.

Примечание 1 — Оценка сведений, подтверждающих правильность устройства, как правило, качественная, поскольку отсутствуют общепризнанные средства ее количественной оценки, и потому, что может оказаться невозможным получение всех видов сведений, установленных в настоящем пункте. Она основана на сбалансированной оценке элементов процессов и изделий в отношении как проектирования, так и изготовления, которые документально фиксируют, принимая во внимание возможность того, что некоторые элементы доказательства правильности могут по отдельности или в сочетании компенсировать ограниченные недостатки в других, как описано в соответствующих подпунктах.

Доказательства правильности необходимо устанавливать посредством:

- оценки процессов, согласно которым продукт был спроектирован, и теперь его конструкция поддерживается (в том числе его верификация и валидация как для текущей конструкции, так и для ее изменений);
- оценки документации по доработке устройства;
- оценки процессов, согласно которым продукт изготовлен; и
- оценки качественных характеристик самого продукта.

Сведения, подтверждающие правильность, касаются раздельно проектирования и изготовления, поскольку для проектирования и производства подходят различные средства компенсации недостатков в доказательстве правильности.

Кроме того, определенные компенсационные меры нельзя применить обобщенно: определенные компенсационные меры применяются только к конкретным недостаткам в основных элементах доказательства правильности.

Главные элементы доказательства правильности проектирования включают в себя:

- доказательство упорядоченного жизненного цикла разработки и сопровождения для проектирования;
- доказательство наличия средств, используемых для поддержки упорядоченного жизненного цикла (например, контроль изменений, управление конфигурацией);
- доказательство надлежащей независимости от возможных систематических отказов;
- обзор документации по доработке, в том числе по верификации и валидации;
- обзор документации по проектированию и эксплуатации устройства.

Примечание 2 — Если выполнена общая предварительная оценка или аттестация ранее разработанного образца, то она может служить удобным источником ссылок на сведения, подтверждающие правильность, или может содержать полезные результаты анализа.

В число средств, которые можно использовать для компенсации некоторых недостатков в основных элементах доказательства правильности проектирования, входят:

- применимый и заслуживающий доверия эксплуатационный опыт, который можно использовать там, где это оправдано, для компенсации недостатков в других элементах;
- доказательство устойчивости (т. е. низкая норма изменений) изделия на протяжении значимого объема производства и использования изделия;
- зависящие от конкретного устройства дополнительные испытания, выполняемые для восполнения пробелов в существующей документации по испытаниям или расширения тестового покрытия по мере необходимости согласно назначению, и другие элементы доказательства правильности;
- компенсация на системном уровне в целях смягчения отказов устройства или преобразования их в безопасные отказы;
- усовершенствования в документации, изначально предоставленной проектировщиком.

Главные элементы доказательства правильности изготовления включают в себя:

- подтверждение упорядоченного жизненного цикла разработки и сопровождения для изготовления, включая контроль изменений и управление конфигурацией;
- документации по изготовлению и эксплуатации устройства.

В число средств, которые можно использовать для компенсации некоторых недостатков в элементах доказательства правильности изготовления, входят:

- доказательство устойчивости (т. е. низкая норма изменений) изделия на протяжении значимого объема производства и использования изделия;
- зависящие от конкретного устройства проверки, функциональные испытания и испытания на старение, соответствующие недостаткам в элементах доказательства правильности изготовления;
- закупка достаточного числа устройств из одной производственной партии, чтобы обеспечить достаточный объем запчастей на срок службы АС.

В EAP (см. 5.3) определен и обоснован способ ранжирования требований нижеприведенных подпунктов по значимости, и какие из допустимых компенсационных мер будут рассмотрены.

В некоторых нижеприведенных подпунктах использованы таблицы, чтобы наиболее четко определить требования к этим трем классам и допустимые компенсационные меры. В этих таблицах необходимо применять следующие интерпретации:

a) «M» должна указывать на обязательную природу описанного критерия, соответствующую использованию слова «должен/необходимо» в изложении требования;

b) «R» должна указывать на рекомендуемую природу изложения требования, соответствующую использованию слова «следует/желательно» в изложении требования;

c) столбцы, обозначенные «СМ», должны указывать компенсационные меры, которые могут быть доступны, и:

- «PS» указывает, что можно использовать применение устойчивости продукта в соответствии с 7.6, чтобы в некоторой степени компенсировать недостатки в основных доказательствах;
- «OE» указывает, что можно использовать применение опыта эксплуатации в соответствии с 7.7, чтобы в некоторой степени компенсировать недостатки в основных доказательствах;
- «CT» указывает, что можно использовать применение дополнительного испытания и/или анализа в соответствии с 7.8, чтобы в некоторой степени компенсировать недостатки в основных доказательствах;
- «DI» указывает, что можно использовать применение усовершенствования документации в соответствии с 7.9, чтобы в некоторой степени компенсировать недостатки в основных доказательствах.

Указанный потенциал компенсационных мер нельзя истолковывать как позволение широкого уклонения от необходимости основных форм доказательств; указания в таблицах о возможности применения компенсационных мер необходимо использовать умеренно.

Примечание 3 — Широкая необходимость компенсационных мер является указанием на отсутствие четкого процесса разработки или строгого соблюдения заявленного процесса, а это может исключить обоснование применения ранее разработанного образца.

Примечание 4 — Как пример: присутствие «M» в столбце «класс 3» и присутствие «CT» в столбце компенсационных мер «СМ» для класса 3 интерпретировалось бы как то, что критерий обязателен для класса 3, но что некоторые недостатки в выполнении проектировщиком и изготовителем этого подпункта можно компенсировать при помощи документации, выработанной при дополнительных испытаниях и/или анализе в соответствии с 7.8.

7.2 Предыдущая аттестация

В большинстве случаев имеются существенные преимущества для отбора устройства, которое было ранее аттестовано по соответствующим нормам безопасности. Такие устройства склонны к четко определенным видам отказа и разработаны в рамках упорядоченного процесса разработки программного обеспечения и/или HDL-программируемого устройства, и потому, скорее всего, существует сопроводительная документация, хотя она может быть защищена правом собственности.

Примечание 1 — МЭК 61508 является соответствующим стандартом безопасности.

Зачастую ситуация совсем иная для неаттестованных изделий, потому что их, как правило, разрабатывают с целью быстрой поставки на рынок и частых изменений для добавления расширенных новых функций. Таким образом, неаттестованные изделия могут обладать функциональными возможностями, которые не требуются для намеченного ядерного приложения. Кроме того, возможно, что изделия могут

обладать функциональными возможностями, которые не только не требуются, но и не определены явно (то есть функциональность скрыта) в спецификации изделия. Напротив, устройства, которые были разработаны по нормам безопасности, вероятно, будут обладать конкретной, четкой функциональностью.

Второе преимущество аттестации по нормам безопасности по сравнению с неаттестованными изделиями состоит в том, что процесс выбора может идти с большей уверенностью, что будут доступны необходимые доказательства правильности, потому что процессы разработки, выполняемые по таким стандартам, могут потребовать наличия документации, подобной документации, необходимой согласно ядерным стандартам.

Примечание 2 — МЭК 62138 и МЭК 60880 являются ядерными стандартами, в которых присутствует этот вид требования к документации.

Тем не менее необходимо проявлять осторожность при оценке как ранее аттестованных, так и неаттестованных устройств в отношении видов отказа. Даже при том, что могут быть четко определены виды отказа устройств, аттестованных по неядерному стандарту безопасности, их обычно задумывают в рамках методологии отключения процесса, такой как аварийный останов реактора, тогда как другие ядерные приложения могут потребовать состояния отказ — работа в противоположность состоянию отказ — отключение. Примерами этому служат контроллеры дизельного генератора и компрессоры, от которых требуется функционирование после возникновения аварии: в таких случаях контроллер устройства просто сигнализирует об условиях, например, о высокой вибрации, которая потребует отключения в неядерном приложении.

Таким образом, в общем, оценка промышленного устройства облегчается и, возможно, упрощается, если оно аттестовано по неядерному стандарту безопасности, но этого самого по себе не достаточно, и, полагаясь на аттестацию, необходимо рассмотреть определенные условия.

Аттестация по неядерному стандарту безопасности может использоваться как доказательство для критериев в разделе 7; в этом случае аттестация должна отвечать следующим критериям:

a) в тех случаях, когда аттестация, используемая для поддержки соответствия подпункту настоящего стандарта, выполнена по стандарту, который не признан широко, то это использование необходимо обосновать;

b) в случае, когда аттестация используется для поддержки соответствия подпункту настоящего стандарта, в ходе аттестации необходимо предоставить доказательства правильности, которые непосредственно рассматриваются в этом подпункте;

c) подтверждающий материал доказательства для аттестации должен быть доступным для просмотра. Данное доказательство должно включать в себя все элементы, необходимые для независимой оценки области действия и границ аттестации, в частности:

- оцениваемая документация;
- гипотезы о предполагаемом использовании устройства и его ожидаемом поведении для всех случаев использования;
- методы и инструменты аттестации;
- оцениваемые свойства устройства (успешен ли результат оценки) и результаты;

d) необходимо, чтобы аттестация была актуальной и применялась к ранее разработанному образцу следующим образом:

- для намеченных приложений классов 1 и 2, где отказ ранее разработанного образца вызвал бы отказ целевой системы (например, если бы оно было установлено во всех каналах системы с резервированием), аттестация должна относиться к конкретной версии, которая была аттестована;
- для намеченных приложений классов 1 и 2, где отказ ранее разработанного образца не вызвал бы отказ целевой системы, аттестация должна относиться к версии, которая отличается от предназначенной для использования версии лишь незначительно, что четко документально зафиксировано и утверждено, и это не влияет на основную функцию;
- для намеченных приложений класса 3 аттестация должна относиться к версии, которая отличается от предназначенной для использования версии таким образом, который четко документально зафиксирован и утвержден;
- в случае, когда предназначенная для использования версия не идентична аттестованной версии(ям), вывод о том, что различия незначительны, необходимо поддержать посредством удобного и подконтрольного анализа. Различия, которые влияют на фундаментальные концепции проектирования, используемые устройством, такие как применяемый физический принцип, используемая технология и средства предотвращения систематических отказов, не являются незначительными. Различия в

настройках параметров, которые относятся к диапазонам сигналов, вероятно, будут незначительны;

e) условия использования, предполагаемые при аттестации, должны соответствовать условиям использования в намеченном ядерном приложении (см. также 7.7);

f) необходимо идентифицировать аттестующий орган, и он должен быть независим от проектировщика и изготовителя устройства;

g) аттестующий орган должен быть компетентен для аттестуемых свойств и/или измерений, и его компетентность необходимо оценивать на основе всей доступной информации о его опыте и аттестациях.

7.3 Предотвращение систематических отказов

Представленные в данном подразделе критерии применяются, в частности, к намеченным приложениям классов 1 и 2, но также рекомендуются для класса 3. Следует отметить, что в случае программного обеспечения и HDL-программируемых устройств уверенность в предотвращении систематических отказов получают, прежде всего, посредством проведения анализа. В то же время условия окружающей среды также могут привести к систематическим отказам, но при аттестации можно использовать анализ или испытания согласно МЭК 60780, в соответствии с 6.6.

Необходимо документальное подтверждение тому, что устройство свободно от потенциальных причин систематических отказов. В целях определения для каждого класса, в данном подпункте используются таблицы, где «M» указывает на «обязательный» («mandatory»), что соответствует слову «должен/необходимо» в изложении требования, а «R» указывает на «рекомендуется» («recommended»), что соответствует слову «следует».

Это необходимо подтвердить с помощью оценки общей архитектуры устройства для гарантии того, что:

a) необходимо оценить конструкцию цифрового контроллера устройства (т. е. цифровую часть устройства). Для оценки необходимо предоставить следующие сведения согласно определению для каждого класса в нижеприведенной таблице 1:

Таблица 1

Предоставляемые сведения	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
1 Общее функционирование цифрового контроллера устройства в нормальных и аномальных условиях (в том числе в условиях отказов)	M	DI	M	DI	M	DI
2 Общая архитектура цифрового контроллера устройства, определяющая и излагающая роли главных элементов цифрового оборудования (в том числе программируемых интегральных схем) и программного обеспечения	M	DI	M	DI	M	DI
3 Все документы, необходимые для проверки соблюдения требований раздела 6, в том числе стратегия верификации и проведенные испытания или анализ	M	CT	M	CT	M	CT
4 Все документы, необходимые для того, чтобы показать, что выполнена верификация каждой фазы разработки устройства, в том числе стратегия верификации и проведенные испытания или анализ	M	CT	M	CT	R	CT

Примечание 1 — Спецификация интерпретации обозначений «M», «R», «DI» и «CT» приведена в 7.1.

Примечание 2 — В случае если указано «DI», это означает, что изменения документации, внесенные в соответствии с 7.9, представляют собой потенциальные компенсационные меры для уточнения конструкции системы.

Примечание 3 — В случае если указано «CT», это означает, что документально зафиксированные дополнительные испытания или анализ в соответствии с 7.8 представляют собой потенциальные компенсационные меры для восполнения существующих пробелов в документации по верификации.

b) сведения, касающиеся общего функционирования цифрового устройства, в частности, должны охватывать сведения, описанные в таблице 2 согласно определению для каждого класса:

Таблица 2

Предоставляемые сведения	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
1 Общий подход к проектированию (напр., контролируемое по времени проектирование или проектирование на основе контроля событий, статическое и динамическое управление ресурсами, синхронное и асинхронное проектирование с помощью электронных средств)	M	DI	M	DI	R	DI
2 Входные (включая прерывания) и выходные сигналы контроллера устройства	M		M		M	
3 Как обрабатываются входные сигналы для получения выходных сигналов	M	CT	M	CT	M	CT
4 Четкое определение и характеристика всех факторов, которые могут повлиять на поведение устройства во время работы	M	CT	M	CT	R	CT
5 Различные задачи (в том числе обработка прерываний), выполняемые в устройстве	M		M			
6 Последовательность и синхронизация задач	M		M			
7 Защита/отделение задач, выполняющих основную функцию устройства, от выполняющих вспомогательные функции	M		M		R	
8 Факторы, влияющие на время реакции и изменчивость времени реакции основной функции	M		M		R	
9 Оперативные и автономные испытательные и диагностические возможности, предоставляемые устройством	M		M		R	
10 Условия пуска, останова и сброса, в том числе мощностные переходные процессы, включая потерю электропитания и перезапуск, и отклик устройства	M		M	CT	R	CT

Примечание 4 — Спецификация интерпретации обозначений «M», «R», «DI» и «CT» приведена в 7.1;

c) в соответствии с таблицей 3 необходимо предоставить указанные подтверждения для каждого класса с целью демонстрации того, что:

Таблица 3

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
1 На основную функцию не будет оказано неблагоприятное воздействие любыми состояниями прерываний	M		M		R	CT
2 При поддержке с помощью документации проектирование любых мер самоконтроля таково, что при обнаружении отказа мерами самоконтроля устройство просигнализирует или самостоятельно отключится	M		M	CT	M	CT
3 Отказы, которые влияют на основную функцию, обнаруживают мерами самоконтроля или другими средствами, такими как периодические контрольные испытания	M	CT	M	CT	R	CT
4 Документально зафиксирован анализ, который определяет возможные остаточные механизмы отказа и виды отказа (например, с помощью FTA, FMEA или анализа критичности) и демонстрирует, что приняты меры для снижения вероятности механизмов отказа и видов отказа, открытых таким образом)	M		M			

Примечание 5 — Для элемента 2 ссылка на «безопасное самостоятельное отключение» основана на требованиях 6.2, перечисление e).

Примечание 6 — Для пункта 4 возможные меры могут включать в себя сосредоточенное дополнительное испытание, ограничение в использовании устройства или внешний мониторинг.

Примечание 7 — Для элемента 4 в приложении А приведено руководство по некоторым проектным особенностям программного обеспечения, которые могут оказаться проблематичными в смысле соблюдения требований данного подпункта.

7.4 Доказательство качества в процессе проектирования

7.4.1 Общие положения

Критерии, представленные в данном подпункте, обеспечивают уверенность в том, что процесс проектирования был систематическим и следует общим принципам, иллюстрируемым жизненными циклами, определенными в соответствующих ядерных стандартах.

Для всех тем необходим следующий общий подход:

- получить от проектировщика устройства доказательство использования цикла разработки на основе качества;
- сравнить доступное доказательство с соответствующими требованиями МЭК 61513, настоящим стандартом и другими адекватными стандартами МЭК, предназначенными для АС; и
- определить, приемлемы ли какие-либо недостатки, упущения или расхождения, и могут ли компенсационные меры (при их наличии), указанные для каждого требования, дополнить доказательство, необходимое для заключения о том, что ранее разработанный образец приемлем.

Подпункты, приведенные ниже, представляют критерии, которые необходимо изучить согласно предыдущему пункту.

7.4.2 Программа обеспечения качества проектировщика изделия

В нижеприведенной таблице определены требования к программе QA проектирования с точки зрения предоставляемой информации или соблюдаемого критерия. Требования необходимо применять, заменяя «___» на «должен/необходимо» там, где указано «М», и «следует/желательно», где указано «R», в соответствии с таблицей 4:

Таблица 4

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
a Проектировщику ___ поддерживать и соблюдать, и продолжать соблюдать документально зафиксированную программу QA, которую ___ оценить с точки зрения требований QA МЭК 61513. В данной оценке ___ идентифицировать любые пробелы и рассмотреть их или привести обоснование их приемлемости	M		M		R	
b Если части процессов разработки программного обеспечения или аппаратных средств (включая HDL-программируемые устройства) определены в документах о качестве, отличных от программы QA, то ___ , чтобы эти документы о качестве разработки (например, план QA программного обеспечения) согласовались с общей программой QA	M		M		R	
c Если части процессов разработки программного обеспечения или аппаратных средств (включая HDL-программируемые устройства) определены в документах о качестве помимо программы QA, то требования данного подпункта ___ применять одинаково к этим вспомогательным документам о качестве	M		M		R	
d Необходимо, чтобы в программе QA на протяжении всего процесса проектирования и доработки требовалось следующее до уровня, обозначенного «М» или «R»	—		—		—	
1) ___ , чтобы лица, выполняющие мероприятия по проектированию и доработке, были компетентны в назначаемой им работе	M		M	OE CT	R	OE CT
2) ___ , чтобы окончательный проект проходил независимую валидацию с уровнем независимости, соответствующим классу намеченного приложения	M		M		M	

Окончание таблицы 4

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
3) В каждый этап проектирования и доработки ___ включать проверку того, что требования этого этапа соблюдены	M		M		R	
4) Управление конфигурацией ___ выполнять в соответствии с 7.4.4	M		M		M	
5) Контроль изменений ___ выполнять в соответствии с 7.4.5	M		M		M	
6) Практику ведения документации ___ проводить в соответствии с 7.4.6	M		M		M	
e В случае если при проектировании и доработке использовались инструменты, то необходимо, чтобы в программе проектировщика по обеспечению качества требовалось обоснование их назначения по уровню, указанному «M» или «R». В случае если квалификатор или разработчик приложения считают обоснование инструментов недостаточным, то он должен рассмотреть, какие компенсационные меры могут и будут применены	—		—		—	
1) история использования инструментов, их устойчивость, пользовательская документация, уведомления о неисправностях и др.	M	CT OE	R	CT OE		
2) вероятность внесения ими ошибки или отказа при обнаружении ошибок в конструкции устройства, а также вероятность таких отказов инструмента, раскрываемых с помощью других средств	M	CT	M	CT		
f В случае если проектировщик и/или производитель допускает использование субподрядчиков, все требования данного стандарта, применимые к производителю или проектировщику устройства, ___ применять в равной степени к субподрядчикам	M		M		M	

Примечание — В отношении перечисления e): инструмент, который может внести неисправность, которую нельзя обнаружить с помощью других средств (например, осмотр человеком), потребует обоснования, сравнимого с классом предполагаемого применения устройства, конструкция которого зависит от инструмента. Инструмент, который может не обнаружить неисправность, но не может внести неисправность, будет считаться классом ниже.

7.4.3 Процесс проектирования и доработки

В таблице 5 определены требования к процессу проектирования и доработки с точки зрения предоставляемой информации или соблюдаемого критерия. Требования необходимо применять, заменяя «___» на «должен/необходимо» там, где указано «M», и на «следует/желательно», где указано «R», в соответствии с таблицей 5:

Таблица 5

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
a В планах доработки программного и аппаратного обеспечения (в том числе HDL-программируемых устройств) ___ требовать, чтобы процесс проектирования и доработки следовал жизненному циклу, который разделяет проектирование и доработку на этапы	M		M		R	
b На каждом этапе жизненного цикла проектирования и доработки в Плане QA ___ документировать следующее: - цели, - входные и выходные данные, - используемые инструменты	M		M		R	
c ___ наличие доказательств, что все вышеуказанные требования соблюдены при проектировании конкретного устройства. Это доказательство ___ документировать в доступной и прозрачной форме	M	CT	M	CT	R	CT OE

Примечание — В число стандартов, требующих надлежащих жизненных циклов, входят: МЭК 61513 (для проектирования на системном уровне), МЭК 62138 и МЭК 60880 (для программного обеспечения), МЭК 60987 (для заказного компьютерного оборудования), МЭК 61508 (для программного и аппаратного обеспечения), или МЭК 62566 для HDL-программируемых устройств.

7.4.4 Управление конфигурацией проекта

В нижеприведенной таблице определены требования к управлению конфигурацией проекта с точки зрения предоставляемой информации или соблюдаемого критерия. Требования необходимо применять, заменяя «___» на «должен/необходимо» там, где указано «M», и «следует/желательно», где указано «R», в соответствии с таблицей 6:

Таблица 6

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
a ___ документировать доказательства использования системы управления конфигурацией в отношении доработки ранее разработанного образца, его программного обеспечения и аппаратных средств (в том числе HDL-программируемых устройств). В эту систему управления конфигурацией ___ включить всю проектную документацию, и методики валидационных испытаний, и отчеты об испытаниях, и их ___ связать с версиями аппаратного, программного обеспечения и HDL-программируемых устройств	M	CT	M	CT	R	CT
b Система управления конфигурацией ___ быть в наличии для всех артефактов (документов, экспертиз проекта, проектов программного обеспечения и HDL-программируемых устройств, чертежей оборудования, результатов испытаний и др.) с начала разработки устройства	R		R			
c Система управления конфигурацией ___ была быть в наличии для всех артефактов (документов, экспертиз проекта, проектов программного обеспечения и HDL-программируемых устройств, чертежей оборудования, результатов испытаний и др.) с начала валидационных испытаний устройства	M		M		M	

7.4.5 Контроль изменений проекта

Необходимо документально подтвердить доказательства того, что проектировщик устройства поддерживает систему контроля изменений, включая процедуры и программные средства, в степени, указанной как «M» или «R», в соответствии с таблицей 7:

Таблица 7

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
a Поддерживает и требует созыва ревизионной комиссии, действующей в рамках управляемого процесса рассмотрения и утверждения изменений, которая должна утвердить все изменения и зарегистрировать свои решения	M		M		M	
b Поддерживает и требует, чтобы все изменения проекта и документации оборудования, программного обеспечения и HDL-программируемых устройств содержали ссылку на разрешение изменений	M		M		R	

Окончание таблицы 7

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
c Систематически собирает и отслеживает отчеты о проблемах в производственных условиях, проблемы изготовления, которые оказывают влияние на конструкцию, и аномалии испытаний в качестве входных данных для процесса управления изменениями. Примечание — Настоящий стандарт не предписывает цепи обратной связи для отчетов о проблемах в производственных условиях, где конечный пользователь сообщает о проблеме дистрибьютору, производителю или проектировщику. Существенным элементом является то, чтобы конечному пользователю была предоставлена точка контакта, обеспечивающая соответствующую информационную связь со стороной, которая наилучшим образом способна решить указанные проблемы	M		M		R	
d Отслеживает все версии и релизы программного обеспечения и конструкции HDL-программируемых устройств или конфигурации оборудования и может сообщать об изменениях, которые были выявлены и устранены в каждой версии или релизе	M		M		R	
e Поддерживает и требует проведения анализа влияния каждого предлагаемого изменения и использования этого анализа влияния в процессе утверждения изменений. Необходимо, чтобы в этот анализ влияния входили анализ степени изменения, его влияние на основные функции ранее разработанного образца, его потенциал негативного влияния на надежность основных функций, часть жизненного цикла реализации, где необходимо начать работу, и масштаб и тщательность необходимых валидационных испытаний	M		R			
f Поддерживает и требует второго рассмотрения утвержденного изменения комиссией по обзору изменений, чтобы разрешить его выпуск в производство, во время которого комиссия по обзору изменений должна основать свое разрешение на обзоре полноты и точности: - документации об изменениях; - документации о повторной валидации; - документации пользователя	M		R			
g Наличествует с начала разработки конкретной модели устройства	R		R			
h Наличествует с начала валидационных испытаний конкретной модели устройства	M		M		M	

Вполне возможно разработать процесс контроля изменений, который включает в себя два уровня комиссии по обзору изменений, при условии, что существуют четкие процедуры и правила, чтобы комиссия нижнего уровня могла распознать, что изменение идет для рассмотрения под эгидой комиссии более высокого уровня. Эти правила могут учитывать класс системы, затрагиваемой изменением, величину изменения или иные соответствующие критерии.

7.4.6 Проектная документация

Проектная документация является частью «документации по безопасности», которая рассматривается как часть оценки. Другая часть «документации по безопасности», поставляемая для пользователей, которые будут проектировать системы с помощью устройства или которые будут эксплуатировать и обслуживать эти системы, рассматривается в 6.9.

Таблица ниже определяет требования к проектной документации исходя из предоставляемых сведений или соблюдаемого критерия. Требования необходимо применять, заменяя «___» на «должен/необходимо» там, где указано «M», и на «следует/желательно», где указано «R», в соответствии с таблицей 8:

Таблица 8

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
a Все документы ___ проверяться и утверждаться уполномоченными на то лицами	M		M		R	
b Все документы ___ быть полными, правильными и однозначными	M	DI	M	DI	R	DI
c Документация по функциональным требованиям:						
Документ по функциональным требованиям определяет функции устройства, реализованного в аппаратных, программных средствах или HDL-программируемом устройстве. В данном документе указаны явно определенным языком основные функции, вспомогательные и излишние функции (если таковые имеются) и любые ограничения на использование устройства	—		—		—	
Проектировщик устройства должен подготовить документацию, охватывающую функциональные требования, которая предоставляет следующие сведения в степени, обозначенной «M» или «R»:						
1) основные, вспомогательные и излишние функции, предоставляемые устройством	M		M		M	
2) в случае уместности средства для обеспечения защиты основных функций от всех преднамеренных и непреднамеренных действий вспомогательных и излишних функций	M		M		R	
3) предоставляемые функции самоконтроля и их действия при обнаружении отказов	M		M		R	
4) внутренние интерфейсы между модулями устройства	M		R		—	
5) внешние интерфейсы устройства	M		M		M	
6) роли, типы, форматы, диапазоны и ограничения входных, выходных сигналов, сигналов исключения, параметров и данных конфигурации, в надлежащих случаях	M		M		M	
7) различные режимы поведения и соответствующие условия перехода	M		M		M	
8) любые ограничения, соблюдаемые при использовании устройства	M		M		M	
9) время отклика, пропускная способность и другие динамические параметры, необходимые для полного понимания функций и ограничений устройства	M	CT	M	CT	M	CT
10) ограничения по условиям окружающей среды (см. 6.6)	M	CT	M	CT	M	CT
d Принцип эксплуатационной документации						
В документации приведена теория, лежащая в основе принципов эксплуатации устройства, конструкции устройства и общего функционирования технических средств и программного обеспечения и HDL-программируемых устройств, достаточно подробно, чтобы можно было оценить эффективность верификации и валидации устройства	M	DI	M	DI	R	DI
e Документация на аппаратные средства						
В документации на аппаратные средства приводится общая структура аппаратных средств, функций и свойств элементов аппаратуры (в том числе свойства ошибкоустойчивости — см. 6.6), которые используются при проектировании и взаимодействии с программным обеспечением или HDL-программируемым устройством, в той степени подробности, которая необходима для грамотной модификации оборудования с целью размещения элемента замены, который не идентичен оригиналу	M	DI	M	DI	R	DI

Окончание таблицы 8

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
f Описание программного обеспечения и HDL-программируемого устройства В настоящей документации приведена общая структура функциональной логики, реализованной в программном обеспечении или HDL-программируемом устройстве, ее декомпозиция на модульном уровне, при котором обслуживание или изменение потребует знаний, и подробности взаимодействия между традиционными аппаратными средствами и программным обеспечением или HDL-программируемым устройством	M	DI	M	DI	R	DI
g Регистрационные записи о верификации и испытаниях на каждом этапе проектирования. Для программного обеспечения и HDL-программируемого устройства сюда войдут испытания элементов (для класса 1), комплексные испытания и валидационные испытания	M	CT	M	CT	R	CT
h Идентификационная информация о версии, подлинность которой может быть заверена во время установки на площадке	M		M		M	
i Пользовательская документация по безопасности согласно описанию в 6.9	M	DI	M	DI	M	DI
j История модификации — отчет или извлекаемый отчет из системы управления конфигурацией, который идентифицирует историю редакций изделия согласно требованиям 7.4.4	M		M		R	

7.5 Доказательство качества при изготовлении

Обеспечение качества при изготовлении важно в том, что это может обеспечить основу обоснования применения устройств одинаковых или подобных моделей, которые могут быть изготовлены позже, даже при том, что на устройство могут влиять такие факторы, как доступность идентичных элементов.

Таблица ниже определяет требования к доказательству качества при изготовлении исходя из предоставляемых сведений или соблюдаемого критерия. Требования необходимо применять, заменяя «___» на «должен/необходимо» там, где указано «M», и «следует/желательно», где указано «R», в соответствии с таблицей 9:

Таблица 9

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
a ___ документально зафиксировать доказательство того, что поставщик поддерживает программу QA при производстве, сопоставимую с ИСО 9001	M		M		M	OE PS
b ___ документально зафиксировать доказательство соответствия с программой QA при производстве	M		M		R	
c ___ документально зафиксировать доказательство того, что изготовитель поддерживает программу квалификации поставщика, которая: - выполняет входную проверку; - выполняет проверку и/или испытание первого выпуска; - контролирует изменения и замену составных частей; и - сообщает об изменениях и заменах проектной организации	M		M		R	OE
d ___ документально зафиксировать доказательство того, что изготовитель выполняет адекватные эксплуатационные испытания и приработку устройства Примечание — «CT» в данном случае относится к конечному пользователю, выполняющему приработку	R	CT	R	CT	R	CT

Окончание таблицы 9

Предоставляемые сведения или соблюдаемый критерий	Класс 1		Класс 2		Класс 3	
		СМ		СМ		СМ
e ___ документально зафиксировать сведения, подтверждающие версию и серийные номера испытательного оборудования, используемого для функциональных испытаний, и что калибровка этого испытательного оборудования отвечает надлежащим стандартам для калибровки	M	CT	M	CT	R	CT
f ___ документально зафиксировать доказательство того, что присутствуют механизмы, гарантирующие, что при производстве в устройстве устанавливают только известное и проверенное программное обеспечение и конфигурации HDL-программируемых устройств	M		M		M	
g ___ документально зафиксировать доказательство того, что изготовитель поддерживает регистрационные записи о дате изготовления, полной информации о версии и серийном номере устройств по мере их производства	M		M		R	
h ___ документально зафиксировать доказательство того, что изготовитель прикрепляет к каждому поставляемому элементу полную идентификационную информацию о версии или релизе, относящуюся к этому элементу (это может быть ярлык для прочтения человеком или электронно-считываемый внутренний параметр)	M		M		M	
i ___ документально зафиксировать доказательство того, что изготовитель облегчает отчетность о производственных проблемах, связанных с устройством, и систематически собирает и отслеживает отчеты о проблемах в производственных условиях, связанных с конструкцией устройства, и сообщает о них проектировщику устройства Примечание — Настоящий стандарт не может предписать цепочку обратной связи для отчетов о проблемах в производственных условиях, где конечный пользователь сообщает о проблеме дистрибьютору, изготовителю или проектировщику. Существенным элементом является то, чтобы конечному пользователю была предоставлена точка контакта, обеспечивающая соответствующую информационную связь со стороной, которая наилучшим образом способна решить указанные проблемы	M		M		R	
j ___ учитывать влияние устойчивости производственного процесса	M	OE PS CT	M	OE PS CT	M	OE PS CT

7.6 Устойчивость изделия

Критерии, представленные в данном подразделе, позволяют исследовать доказательство зрелости изделия и вероятность того, что изделие останется неизменным, и поставщик сможет осуществлять его поддержку на протяжении всего срока его установки на атомной станции. Это также мера тщательности, с которой используется анализ влияния при контроле изменений и применении полной строгости процесса проектирования к изменениям, включая адекватное регрессионное тестирование. Устойчивость изделия тесно связана с его эксплуатационным опытом, и в случае, если на эксплуатационный опыт полагаются как на фактор оценки, устойчивость изделия существенно важна.

а) Устойчивость изделия необходимо оценивать с точки зрения объема изменений основной функции, объема изменений, имеющих потенциал влияния на основную функцию, объема изменений, влияющих на другие функции, влияние любого из изменений на основную функцию и причины этих изменений (включая поправку ошибки, замену устаревших частей, изменения нормативной базы и т. д.).

Примечание — Низкая частота исправительных изменений за существенный период использования изделия может указывать в известной степени на устойчивость и правильность и/или разумность конструкции изделия.

b) Оценку согласно перечислению a) необходимо выполнять на основе записей о техническом обслуживании, поддерживаемых при контроле изменений и с помощью инструментов управления конфигурацией, и процедур, которые должны отвечать требованиям 7.4.4, 7.4.5 и 7.5.

c) Устойчивость изделия необходимо оценивать, принимая во внимание объем установок и приложений, и необходимо засчитывать, только если изделие показало значимый объем производства и применения изделия.

d) В случае если применяется устойчивость изделия, ее необходимо применять в поддержку слабых или отсутствующих доказательств специфичных критериев в пунктах 7.3, 7.4 или 7.5, где соответствующий подпункт позволяет применять устойчивость изделия или где она поддерживает применение эксплуатационного опыта.

7.7 Опыт эксплуатации

Критерии, представленные в данном подпункте, позволяют исследовать доказательство ошибкоустойчивости изделия перед лицом эксплуатационных сред и функциональных разрезов, подобных намеченному приложению и не менее сложных. Такое доказательство важно, потому что оно представляет собой проверку устройства с помощью функциональных разрезов, которые могут дополнить испытание ранее разработанного образца вне ограниченного числа тестовых сценариев, которые можно выполнять при доработке.

a) Необходимо, чтобы все засчитанные доказательства опыта эксплуатации были контролируемы.

b) Необходимо документально зафиксировать идентификационные сведения о дающей отчет организации или организациях.

c) Доказательство опыта эксплуатации необходимо увязать с точно известными версиями программного обеспечения и HDL-программируемого устройства.

d) Доказательство опыта эксплуатации необходимо увязать с известными конфигурационными настройками аппаратных средств и программного обеспечения и HDL-программируемого устройства.

e) В случае, когда опыт эксплуатации должен быть засчитан для версий программного обеспечения, HDL-программируемого устройства или аппаратных средств, отличных от версии, которая будет использоваться, необходимо предоставить обоснование, в котором проанализированы различия между этими версиями, и эти результаты анализа необходимо использовать, чтобы определить, насколько можно засчитать опыт эксплуатации каждой версии устройства.

Дополнительное испытание может послужить для зачета более ранних версий программного обеспечения и HDL-программируемого устройства в опыте эксплуатации.

f) При анализе доказательства опыта эксплуатации необходимо принять во внимание, функционируют ли специфичные функции ранее разработанного образца на непрерывной основе или периодически по требованию. В первом случае в основу доказательства необходимо положить часы фактической эксплуатации; в последнем случае в основу доказательства необходимо положить число циклов исполнения (включая контрольные испытания) без отказа функций, вызываемых по требованию.

g) Необходимо, чтобы все аспекты функций ранее разработанного образца в намеченном приложении были охвачены опытом эксплуатации.

h) Необходимо, чтобы покрытие и объем опыта эксплуатации были достаточны для обеспечения уверенности в ранее разработанном образце, соразмерной с классом намеченного приложения.

i) Необходимо, чтобы покрытие и объем опыта эксплуатации были достаточны для обеспечения уверенности в ранее разработанном образце, соразмерной со сложностью устройства, принимая во внимание и программное обеспечение, и HDL-программируемые устройства, и другие аппаратные средства.

j) В случае, когда опыт эксплуатации является главным или весомым критерием для доказательства правильности, объем и широта опыта эксплуатации крайне важны, поэтому объем и источник требуемых данных из опыта эксплуатации необходимо обосновать.

Достаточное время работы следует определить в зависимости от конкретного случая с помощью инженерной оценки. В этой оценке следует особенно принять во внимание ожидаемый уровень надежности, требуемый на системном уровне для функций, в которых используется устройство.

Для намеченных приложений класса 1 опыт эксплуатации следует основать на нескольких приложениях от нескольких дающих отчет организаций.

Отсутствуют требования о том, чтобы опыт эксплуатации был реализован на ядерной установке. Намерение данного требования состоит в том, чтобы покрытие и объем эксплуатационного опыта были тщательно задокументированы (что может не соответствовать состоянию дел в промышленных средах)

и отвечали функциональному разрезу, тестируемому ранее разработанным образцом в намеченном приложении [см. перечисление k) ниже].

Примечание — В МЭК 61508-7, приложение D, приведены сведения, связывающие объем опыта эксплуатации с критериями надежности.

k) Необходимо, чтобы в зачтенный опыт эксплуатации вошли условия эксплуатации не менее сложные, чем в намеченном приложении. Эти условия должны включать в себя следующее, в зависимости от обстоятельств:

- технологический режим (например, температура, давление, вязкость, содержание частиц и т. д.) для смачиваемых устройств, таких как клапаны или датчики (см. 6.6);
- режим эксплуатации аппаратуры (например, температура, влажность, вибрация, электромагнитные помехи, излучение) (см. 6.6);
- функциональный разрез или метод использования (например, скорость переходных процессов, таких как пуск компрессора или гармоники, видимые инвертором при питании от генератора вместо электросети), если он может каким-либо образом повлиять на эксплуатацию ранее разработанного образца с точки зрения загрузки программного обеспечения;
- интерфейсы с другими устройствами.

l) Необходимо документально зафиксировать доказательство того, что настроена и используется надежная система сообщения об отказах, чтобы эксплуатационный опыт можно было оценить с высокой степенью достоверности. В случае, если не обо всех отказах или нарушениях нормальной эксплуатации можно было сообщить, расчетный эксплуатационный опыт необходимо исключать из рассмотрения, чтобы отразить неопределенность в точности системы сообщения об отказах.

Например, в случае если не существует убедительных доказательств того, что обо всех отказах сообщается, расчетные эксплуатационные часы можно обесценить на 30 % в пределах гарантийного срока и на 50 % или более вне его.

m) В случае, когда эксплуатационный опыт указывает на эпизоды очевидных случайных аппаратных отказов, превышающих прогнозируемую интенсивность, то необходимо рассмотреть возможность того, что в устройстве могут существовать систематические отказы, например, отказ в программном обеспечении или конструкции HDL-программируемого устройства, климатическая слабость элемента изделия и т. д.

n) В случае, когда применяется эксплуатационный опыт, его необходимо применять в поддержку слабых или отсутствующих доказательств для конкретных критериев в 7.3, 7.4 или 7.5, где соответствующий подпункт позволяет применение эксплуатационного опыта.

7.8 Дополнительные испытания и/или анализ (верификация)

Дополнительные испытания могут использоваться по многим причинам. Они могут включать в себя подтверждение применимости более ранних версий устройства в эксплуатационном опыте, подтверждение изменений устройства, закрытие пробелов в валидационных испытаниях, компенсации некоторой нехватки опыта эксплуатации или подтверждение правильности или надежности в применимых условиях эксплуатации.

Можно также использовать дополнительные испытания, чтобы компенсировать пробелы в процессе проектирования (или его знании), проектной документации (особенно упущения в функциональных требованиях и валидационных испытаниях), документации, охватывающей отклики на конкретные входные состояния (например, аномальные входные сигналы), и отсутствие специфичного эксплуатационного опыта посредством подробной идентификации отклика на конкретные входные сигналы, или проверить ошибкоустойчивость устройства к специфичным воздействиям.

Примеры применимых видов испытаний включают в себя:

- испытания с имитацией отказа для подтверждения того, что функции самоконтроля обнаруживают каждый отказ и дают в результате выходные сигналы отказоустойчивого устройства;
- специфические испытания для подтверждения характеристик малопроизводительных или уравновешенных функций (то есть тех, которые ждут обнаружения конкретного события, в противоположность функциям, которые работают непрерывно), для которых эксплуатационный опыт по определению трудно накопить;
- специфические испытания для подтверждения тех областей функционального поведения устройства, которые задокументированы не полностью или неоднозначно;
- специфические испытания, связанные с модификацией, для подтверждения приемлемости включения предшествующих версий в зачтенный объем эксплуатационного опыта;

- специфические испытания для определения отклика устройства на недопустимые или неисправные входные сигналы (например, входной сигнал от 4 до 20 мА на входе 4 мА или монотонное понижение напряжения в источнике питания, подаваемого на аналоговый вход и контур измерительного прибора) и определения приемлемости этого отклика в целевом приложении;

- статистически действительное случайное испытание, подобное приведенному в МЭК 61508-7, приложение D. Необходимо отметить, что выполнить предпосылки для такого испытания может быть весьма трудно;

- дополнительные испытания для подтверждения того, что в конфигурации(ях) и предназначенных условиях использования устройство отвечает своим функциональным и эксплуатационным требованиям;

- специфические испытания для подтверждения отсутствия возмущения основной функции излишними или вспомогательными функциями;

- специфические испытания для подтверждения эффективности механизмов, ориентированных на сохранность и безопасность.

Примечание — Ссылка на термин «отказоустойчивый» основана на требованиях, приведенных в 6.2, перечисление e).

В случае, когда при оценке ранее разработанного образца используется дополнительное испытание, необходимо применять, документировать и держать доступным для просмотра следующее:

a) в документацию по испытаниям необходимо включить идентификационные сведения о точной версии проверяемого изделия;

b) проверяемые функции необходимо документально фиксировать (сюда необходимо включить порядок проведения испытаний, экспериментальные данные, ожидаемые результаты испытаний и наблюдаемые результаты);

c) испытания необходимо разработать с учетом намеченного приложения, чтобы показать соответствие поведения устройства требованиям приложения, включая критические и исключительные условия;

d) необходимо выполнить обзор результатов испытаний с учетом намеченного приложения, чтобы показать соответствие поведения устройства требованиям приложения;

e) необходимо, чтобы внешние условия при испытаниях были репрезентативными по отношению к намеченному приложению, или необходимо документировать причины приемлемости отклонений;

f) в случае, если намеченное приложение относится к классу 1 или классу 2, необходимо документировать основание испытаний, чтобы объяснить, почему результаты испытаний покажут то, что требуется (сюда может, например, войти анализ или модель программного обеспечения, HDL-программируемого устройства или другие испытываемые конструктивные особенности аппаратных элементов);

g) необходимо регистрировать идентификационные сведения об организации, проводящей испытание;

h) в случае применения дополнительных испытаний или анализа их необходимо применять в поддержку отсутствующего доказательства для конкретных критериев в подразделах 7.3, 7.4 или 7.5, где соответствующий подпункт позволяет компенсационное испытание или анализ.

7.9 Усовершенствование документации

Во многих случаях можно компенсировать недочеты в документации, получаемой от проектировщика или изготовителя, путем усовершенствований в тексте документации в процессе оценки или в соответствии с EAR.

Один из видов усовершенствования документации часто называют «воссозданием документа». Обычно оно основано на использовании дополнительных испытаний для реализации формы обратного проектирования, нацеленного на разъяснение проектной спецификации и порядка проведения валидационных испытаний. При воссоздании документа конечный продукт никак не модифицируется, и проект спецификации типа «черного ящика» изделия подготавливают исходя из всей доступной информации, включая поддержку от проектировщиков. По этому проекту спецификации разрабатывают порядок проведения испытаний и выполняют их. Различия между ожидаемыми результатами испытаний и фактическими результатами испытаний используют для модификации проекта спецификации изделия и спецификации испытаний, и весь процесс повторяют многократно, пока точность спецификации не будет подтверждена успешными испытаниями.

Если усовершенствование документации используют как компенсационную меру, то необходимо применять следующее:

a) необходимо наличие прочной, уже существующей основы для усовершенствований в документации, состоящей либо из полного официального описания, либо из комбинации описаний программного и аппаратного обеспечения, а также описания принципа действия;

Примечание 1 — Намерение состоит в том, чтобы положиться на документацию, подготовленную проектировщиком, а не создавать документацию с чистого листа. Это обусловлено тем, что значимое отсутствие упорядоченной документации, которая действительно объясняет работу изделия, является показанием недочета в подходе проектировщика, что ставит под сомнение непосредственно проект.

b) необходимо, чтобы все усовершенствования в документации, приводящей описание функциональности конструкции, были рассмотрены проектировщиком ранее разработанного образца.

Примечание 2 — Намерение состоит в том, чтобы гарантировать техническую правильность в критических областях проектирования изделий, которые являются ключевыми в защите основной функции в сравнении со вспомогательными или излишними функциями при всех профилях электропотребления;

c) если дополнительное испытание используют как часть методологии воссоздания документации, то это испытание должно соответствовать 7.8;

d) если применяют усовершенствование документа, то его необходимо применять в поддержку слабых описаний для конкретных критериев в подразделах 7.3, 7.4 или 7.5, где соответствующий подпункт позволяет усовершенствование документа.

8 Критерии для интеграции в приложение — пределы и условия использования

8.1 Общие положения

В настоящем разделе рассмотрены возможные пределы и условия, которые могут ограничить использование ранее разработанного образца. Данные условия и ограничения могут возникнуть либо исходя из результатов оценки пригодности, либо могут быть наложены, чтобы частично аттестовать устройство для использования при наложенных ограничениях и условиях. Все ограничения необходимо документально зафиксировать в EAR (см. 5.3.3) и пользовательской документации по безопасности (см. 6.9), охватывающих ранее разработанный образец.

8.2 Ограничения использования

Ранее разработанный образец можно оценивать как аттестованный для использования в определенных приложениях при условии, что его использование подлежит определенным ограничениям и условиям.

В EAR необходимо идентифицировать следующее:

- самый высокий класс, для которого ранее разработанный образец пригоден для использования;
- в применимых случаях конкретные приложения, для которых ранее разработанный образец пригоден для использования;
- пределы надежности, которых устройство может достигнуть самостоятельно или в избыточной конфигурации;
- конкретные опции или вторичные функции, которые необходимо разрешить или блокировать, включая конкретные настройки параметров, требуемые для каждого класса;
- пределы эксплуатационной среды (согласно 6.6), для которой ранее разработанный образец аттестован для эксплуатации;
- ограничивающие факторы, влияющие на эксплуатационный срок службы (такие, как использование алюминиевых конденсаторов);
- любые особые меры, которые необходимо соблюдать во время эксплуатации или испытания, чтобы гарантировать безопасное использование устройства.

8.3 Модификации устройства, необходимые для приложения

Ранее разработанный образец можно оценивать как пригодный для использования в определенных приложениях, если определенные модификации аппаратных средств или чрезвычайно незначи-

тельные модификации программного обеспечения устройства выполнены до использования. Иногда это может быть необходимо, например, в приложениях реконструкции, где важно соответствие форме или где может потребоваться согласование импедансов, но при этом принципиально важно, чтобы такие изменения не имели эффекта создания нового устройства, ибо в таком случае настоящий стандарт больше не применим.

Например, некоторые потенциальные ранее разработанные образцы могут обладать вторичными функциями, такими как HART, который реализован наложением высокочастотных сигналов на технологический сигнал от 4 до 20 мА. Может потребоваться блокировка этой опции или применение фильтра низких частот, чтобы высокие частоты не влияли на другие устройства в целевой системе.

В случае, если необходимо каким-либо образом модифицировать устройство, применяют следующее:

a) в EAR необходимо:

- идентифицировать требуемые изменения и
- проверить уровень поддержки этих изменений от проектировщика устройства;

b) необходимо, чтобы все модификации в конструкции устройства были такими, которые не аннулируют опыт эксплуатации, зачтенный при оценке. Модификации не должны концептуально менять основную функцию ранее разработанного образца;

c) необходимо, чтобы все модификации были небольшими по своему масштабу, ограниченными по уровню и простыми для верификации и валидации;

d) необходимо, чтобы все модификации выполнялись согласно всем требованиям, приведенным в 7.4, и до известной степени соответствовали классу намеченного приложения;

e) EAR необходимо пересмотреть после изменений, и при этом необходимо учесть все факторы, которые могут повлиять на выводы отчета.

8.4 Модификации системы для размещения устройства

Ранее разработанный образец можно оценить как пригодный для использования в определенных приложениях, если в систему до использования внесены определенные модификации. Настоящий подпункт в частности применим к реконструкциям, при которых, к примеру, может понадобиться промежуточное реле для обеспечения необходимых интерфейсов между ранее разработанным образцом и другими элементами системы.

В таких случаях необходимо рассмотреть и документально зафиксировать следующие проблемы при оценке ранее разработанного образца:

a) в EAR необходимо рассмотреть возможные изменения в конструкции системы, которые могут потребоваться, включая следующее:

- дополнительное оборудование для контроля возникновения отказа;
- дополнительное необходимое резервирование или неодинаковость;
- потребность в межканальных сравнениях;
- переназначение функции другой подсистеме;
- изменения, вызванные защитой от условий окружающей среды, такие как дополнительное экранирование, вентиляция, охлаждение и т. д.;
- изменения в техническом обслуживании и/или практике эксплуатации;

b) в EAR необходимо рассмотреть требования к обучению на системном уровне, которые возникнут при использовании ранее разработанного образца;

c) после модификаций EAR необходимо пересмотреть и в этой пересмотренной редакции необходимо учесть все факторы, которые могут повлиять на выводы отчета.

8.5 Интеграция и ввод в эксплуатацию устройства в системах безопасности станции

Ранее разработанный образец, аттестованный для использования в данном приложении, будет в конечном счете введен в эксплуатацию и интегрирован в новое конструктивное исполнение или введен в реконструированную систему безопасности станции.

Здесь следует различать две ситуации:

- приложения, в которых вновь аттестованное устройство используется самостоятельно, таким способом, который не несет риска порождения полного отказа функции безопасности станции; и
- приложения, в которых вновь аттестованное устройство используется во всех каналах системы или в одиночной потенциальной точке отказа, в связи с чем присутствует риск порождения этим

устройством полного отказа функции безопасности станции, такой как защитное устройство источника питания системы безопасности.

На основе EAR необходимо подготовить План ввода в эксплуатацию/интеграции, и он должен:

a) содержать надлежащие требования раздела 6 МЭК 61513;

b) содержать рекомендации и ограничения, документально зафиксированные в EAR, и инструкции поставщика по вводу в эксплуатацию;

c) в случае если остались подлежащие валидации аспекты функциональности устройства, в Плане ввода в эксплуатацию/интеграции необходимо также:

1) рассмотреть поэтапное введение ранее разработанного образца в систему, рассматривая возможность начального периода валидации, где ранее разработанный образец вводят в эксплуатацию только в одном канале или тракте избыточной системы, чтобы разрешить оценку устройства при эксплуатации в настоящей целевой системе;

2) определить соответствующие средства для гарантии и верификации правильных настроек параметров во всех устройствах, реализованных в системе, включая указанные в EAR;

3) определить тестовые сценарии ввода в эксплуатацию на основе динамических аспектов систем безопасности (переходных процессов), где:

- выбор конкретных тестовых сценариев следует основать на моделировании и имитациях системы;
- в этих испытаниях необходимо рассмотреть время реакции устройства и правильную последовательность и приоритет защитных мероприятий; и
- для устройств, защищающих системы электропитания, в тестовые сценарии следует включать целые последовательности пуска системы, и нагрузочное тестирование выбранных систем безопасности;

4) требовать регистрации следующего при вводе в эксплуатацию:

- все отклонения функции устройства от данных EAR. Малыми отклонениями нельзя пренебречь, поскольку они могут указать на серьезные недостатки в программном обеспечении устройства или конструкциях HDL-программируемых устройств;
- значения всех настроек параметров устройства;
- все результаты испытаний, вплоть до конечной интеграции устройства в систему.

9 Аспекты сохранения приемлемости

9.1 Общие положения

При оценке ранее разработанного образца устройство может оказаться идеальным с точки зрения функциональной пригодности и доказательства правильности, но следует взвесить как фактор срок службы устройства и долгосрочную поддержку от поставщика из-за длительных сроков службы ядерных установок.

В данном пункте определены критерии для оценки ранее разработанного образца с этой перспективы, особенно с перспективы возможности сопровождения программного обеспечения и HDL-программируемых устройств.

9.2 Уведомления от проектировщика и изготовителя устройства

Необходимо предпринять надлежащие меры для гарантии того, что пользователь будет формально предупрежден о любых модификациях аттестованного устройства. В случае выполнения модификации аппаратного, программного обеспечения или HDL-программируемого устройства необходимо провести анализ влияния, а устройство повторно аттестовать в соответствии с настоящим стандартом.

Ранее разработанный образец следует оценивать с точки зрения уведомлений об отказах от изготовителя или проектировщика, которые возникают после периода оценки эксплуатационного опыта, когда устройство может находиться в процессе эксплуатации. Изучение отказа на другой установке можно использовать для инициирования профилактического обслуживания или замены устройства.

В ходе оценки следует рассмотреть следующие факторы и сообщить о результатах попытки получить согласие изготовителя (и проектировщика) на то, чтобы:

- обеспечить своевременное уведомление о каждом отказе на других установках;

- включить в уведомление анализ, который может помочь определить, может ли дефект повлиять на основную функцию или снизить ее невосприимчивость к отказам вспомогательных и излишних функций;
- сделать доступным актуальный список дефектов, который идентифицирует возможные влияния сообщаемых отказов, текущий статус их разрешения и точные затрагиваемые версии;
- обеспечить уведомление о каждом изменении, будь это замещение элемента аппаратуры, изменение в производственном процессе или изменение в программном обеспечении или HDL-программируемом устройстве.

9.3 Изготовление и срок поддержки текущей версии

Ранее разработанный образец следует оценивать с точки зрения ожидаемого срока поддержки изделия для ранее разработанного образца, а также долговечности непосредственно устройства. В первом случае более длинные периоды поддержки желательны и, возможно, обсуждаемы. Во втором случае это знание служит для планирования замены устройства до конца срока службы устройства.

В ходе оценки следует рассмотреть и документально зафиксировать в EAR следующие факторы:
- долговечность текущей версии и устройства в общем;
- срок обслуживания последней версии и устройства в общем;
- готовность изготовителя или проектировщика предупреждать о снятии с эксплуатации этой версии и устройства в общем;
- готовность поставщика придерживаться совместимости по соединителям будущих замен;
- готовность поставщика придерживаться функциональной совместимости будущих замен;
- влияние модификаций по требованию заказчика, необходимых для приложения.

9.4 Сохранение средств технического обслуживания и документации

Жизненный цикл атомных станций намного длиннее, чем у цифровых устройств, поэтому при оценке устройства следует рассмотреть устаревание. В ходе оценки следует рассмотреть, желает ли проектировщик устройства обеспечить договорное обязательство (например, в договоре под отлагательным условием) или дать гарантии того, что в случае решения проектировщика или изготовителя о прекращении поддержки ранее разработанного образца будет доступно следующее:
- установочные копии конфигурационных инструментов, таких как редакторы, компиляторы;
- копия операционной среды этих инструментов (например, конкретная версия Unix или Windows);
- копии всех исходных файлов, файлов построения, библиотек и т. д. из системы управления конфигурацией;
- специальные аппаратные инструменты (например, программаторы PROM, логические анализаторы);
- производственные чертежи;
- копии всей документации (спецификации, акты испытаний и т. д.); и
- подробное описание компьютерной аппаратуры и принадлежностей, необходимых для использования операционной системы, программное обеспечение инструмента и аппаратные средства инструмента или фактическое оборудование.

9.5 Рекомендации для конечного пользователя

С целью поддержки долгосрочного использования ранее разработанного образца рекомендуют следующее для реализации компанией, эксплуатирующей атомную станцию, за пределами области оценки устройства:
- поддерживать систему управления конфигурацией независимо от поставщика, чтобы учесть:
- все модификации конфигурационных параметров,
- все начальные модификации, как документально зафиксировано в ООП,
- все версии, полученные от поставщика, и состояние их установки и конфигурации;
- поддерживать систему контроля изменений с эффективным анализом влияния;
- выполнять валидационные испытания после всех конфигурационных изменений (даже изменений параметров);
- поддерживать копии конфигурационных инструментов, таких как редакторы, компиляторы;
- в случае если устройство используется в приложениях различных классов, обслуживать все мероприятия поддержки в установленном порядке для самого высокого класса.

Приложение А
(справочное)

Возможные конструктивные особенности системы программного обеспечения, которые могут повлиять на общую надежность устройства

Настоящее приложение приводит рекомендации по верификации выводов, сделанных при оценке проекта относительно свойств, которые имеют тенденцию избегать систематических отказов (см. 7.3).

Приведенная в настоящем приложении информация, в частности, предназначена для приложений класса 1 или класса 2, но может быть применена к классу 3. Следует отметить, что в случае программного обеспечения предотвращение систематических отказов гарантируют прежде всего посредством анализа. В то же время условия окружающей среды могут также привести к систематическим отказам, но при аттестации можно проводить анализ или испытание согласно МЭК 60780, как указано в 6.6.

Как указано в 7.3, оценка ошибкоустойчивости конструкции для предотвращения систематических отказов начинается с исследования полного проекта системы. В случае программного обеспечения это может привести к исследованию возможных механизмов в проектировании, которые, по широкому признанию, являются источниками потенциальных проблем. Нижеприведенный список не претендует на полноту, но может служить отправной точкой:

a) чувствительность к профилю электропотребления может влиять на загрузку центрального процессора, порядок обслуживания прерываний и т. д. Ниже приведены примеры возможных источников отказа устройства:

- взаимодействие между двумя или более входами;
- поведение сигнала (например, короткие выбросы за пределы диапазона) из-за электромагнитных помех;
- перегрузка из-за каскадных событий, обнаруженных на входах;
- нарушение аспектов синхронизации в наихудшем случае.

Примечание — МЭК 60880 (применяется к системам класса 1) налагает требование о том, что планирование программного обеспечения должно быть детерминировано, а МЭК 62138 (применяется к системам класса 2) — что программное обеспечение должно обеспечивать возможность предсказуемого поведения во время выполнения. Фактически настоящий стандарт стремится к тому, чтобы в ходе соответствующего анализа наихудшего случая было показано, что электронный блок (или блок, обеспечивающий основную функциональность) будет всегда срабатывать вовремя или реагировать в пределах требуемого времени;

b) в случае, если архитектура проекта допускает недостатки в фундаментальном подходе, которые могут снизить уверенность в том, что соблюдены требуемые свойства системы (учитывая уровень уверенности, адекватный классу приложения), может представлять ценность исследование проекта на присутствие конкретных конструктивных особенностей, которые могут быть уместны.

Для намеченных приложений класса 1 обеспокоенность могут вызвать:

- упреждающее планирование и
- все причины, перечисленные для классов 2 и 3.

Для намеченных приложений класса 2 обеспокоенность могут вызвать:

- динамические объекты, созданные в режиме реального времени;
- сборка «мусора»;
- любое, исключая самое простое, использование указателей (например, использование адресной арифметики с указателями);
- асинхронный доступ к ресурсам или их блокировка;
- зависимости от времени или даты, влияющие на основную функцию(и); и
- все причины, перечисленные для класса 3.

Для намеченных приложений класса 3 обеспокоенность могут вызвать:

- коммуникационные перегрузки, вызываемые другими устройствами (такими, как спорадически вибрирующий элемент);
- неконтролируемое или неограниченное использование стека или динамической области;
- планирование, зависящее от входных сигналов;
- рекурсия;
- динамические приоритеты заданий;
- высокая загрузка системы, измеренная с точки зрения времени центрального процессора или использования памяти;

c) для приложений класса 1 трудно гарантировать, что основная функция сработает вовремя, если проект опирается на любое, кроме самого простого, использование прерываний или если они используются в проекте вторичных функций, где могут влиять на загрузку системы и таким образом косвенно влиять на основные функции;

d) конкретно для приложений классов 1 и 2 систематические отказы считают менее вероятными в случае, где программное обеспечение разработано с помощью:

- соглашения о присвоении имен;
- предотвращения потенциально опасных языковых конструкций, интерпретация которых компилятором или интерпретатором может быть нестандартной;

e) для намеченных приложений классов 1 и 2 желательно использовать адекватный статический анализ исходного кода;

f) меры самоконтроля, такие как логический мониторинг выполнения программы, утверждения и т. д., могут быть полезными, особенно если эти функции используются для выдачи сигнала тревоги или безопасного отключения устройства.

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 60671	—	*
IEC 60780:1998	—	*
IEC 60880	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А»
IEC 60980:1989	—	*
IEC 60987:2007	IDT	ГОСТ Р МЭК 60987:2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризованных систем»
IEC 61000 (все части)	—	*
IEC 61226	IDT	ГОСТ Р МЭК 61226—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
IEC 61508-7:2010	IDT	ГОСТ Р МЭК 61508-7:2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства»
IEC 61513:2011	IDT	ГОСТ Р МЭК 61513—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
IEC 62138:2004	IDT	ГОСТ Р МЭК 62138—2010 «Атомные станции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С»
ISO 9001:2008	IDT	ГОСТ Р ИСО 9001—2008 «Системы менеджмента качества. Требования»

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

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

- IDT — идентичные стандарты.

Библиография

[1] IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements

[2] IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

[3] IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements

[4] IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

[5] IEC 62003:2009, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for electromagnetic compatibility testing

[6] IEC 62566:2012, Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions

[7] IEC 62645, Nuclear Power Plants — Instrumentation and control important to safety — Requirements for security programmes for computer-based systems (to be published)

[8] IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection 2007 Edition)

[9] Licensing of safety critical software for nuclear reactors — Common position of seven European nuclear regulators and authorised technical support organizations, 2010 edition

УДК 621.311.049.75:006.354 ОКС 27.120.20 IDT

Ключевые слова: атомные станции, контроль, управление, промышленные цифровые устройства, безопасность киберпространства

Редактор *В.А. Сиволапов*
Технический редактор *В.Ю. Фотиева*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 28.06.2016. Подписано в печать 20.07.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,50. Тираж 25 экз. Зак. 1699.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru