ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62671— 2024

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ СТАНЦИЙ

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)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 июля 2024 г. № 919-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62671:2013 «Атомные электростанции. Системы контроля и управления, 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).

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

Отличия в подходах к категоризации функций контроля и управления и классификации систем контроля и управления приведены в дополнительном приложении ДА.

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

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

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

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

© IEC, 2013
© Оформление. ФГБУ «Институт стандартизации», 2024

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
1.1 Общие положения 1
1.2 Вводная информация 2
1.3 Область применения настоящего стандарта 2
1.4 Структура стандарта 3
2 Нормативные ссылки 4
3 Термины и определения 5
4 Сокращения 11
5 Общие требования 11
5.1 Общие положения 11
5.2 Применение настоящего стандарта 12
5.3 Общие требования к процессу оценки 13
6 Критерии функциональной и эксплуатационной пригодности 16
6.1 Общие положения 16
6.2 Функциональная состоятельность основной функции 17
6.3 Вспомогательные функции 17
6.4 Возможность изменения конфигурации 18
6.5 Избыточные функции 19
6.6 Эксплуатационная надежность аппаратных средств 19
6.7 Надежность, ремонтопригодность и тестируемость 20
6.8 Информационная безопасность 21
6.9 Пользовательская документация по безопасности 21
7 Критерии функциональной надежности и доказательства корректности 22
7.1 Общие положения 22
7.2 Предварительная аттестация 24
7.3 Предотвращение систематических отказов 26
7.4 Свидетельства, подтверждающие качество устройства в процессе проектирования 28
7.5 Свидетельства обеспечения качества при изготовлении 34
7.6 Стабильность изделия 36
7.7 Опыт эксплуатации 36
7.8 Дополнительные испытания и/или анализ (верификация) 37
7.9 Доработка документации 39
8 Критерии интеграции устройства с целью применения. Пределы и условия использования 39
8.1 Общие положения 39
8.2 Ограничения применения 39
8.3 Модификации устройства, необходимые для его целевого применения 40
8.4 Модификации системы для размещения устройства 40
8.5 Интеграция и ввод устройства в эксплуатацию в системах безопасности АС 41
9 Вопросы, связанные с сохранением приемлемости устройства 41
9.1 Общие положения 41
9.2 Уведомления от проектировщика и изготовителя устройства 42
9.3 Процесс изготовления и срок поддержки текущей версии 42
9.4 Сохранение инструментов и документации, относящихся к техническому обслуживанию 42
9.5 Рекомендации для конечного пользователя 43
Приложение А (справочное) Возможные конструктивные особенности системы программного обеспечения, которые могут влиять на общую надежность устройства 44
Приложение ДА (справочное) Отличия в подходах к категоризации функций контроля и управления и классификации систем контроля и управления в зависимости от их важности для безопасности атомных станций, применяемых в МЭК и Российской Федерации 46
Приложение ДБ (справочное) Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам 47
Библиография 49

Введение

a) Техническая справка, основные вопросы и организация настоящего стандарта

В настоящем стандарте основное внимание уделено выбору и оценке предварительно разработанных специализированных устройств ограниченной, особой функциональности и ограниченной возможности изменения конфигурации для применения на атомных станциях (АС), где эти устройства объединяют с программным обеспечением или цифровыми схемами, определенными с использованием языков описания аппаратных средств. При этом данные устройства произведены в соответствии со стандартом, признанным в неядерной области, а не в соответствии с серией стандартов ПК 45А.

Настоящий стандарт предназначен для использования проектировщиками АС, операторами АС (эксплуатирующими организациями), экспертами-системотехниками и лицензиарами.

Предметом обсуждения настоящего стандарта являются два аспекта, которые не рассматриваются в других стандартах серии стандартов ПК 45А МЭК:

- другие стандарты рассматривают аспекты аппаратных средств устройств, содержащих программное обеспечение, или рассматривают сложные устройства, такие как программируемые логические контроллеры (ПЛК), содержащие программное обеспечение, потенциально обладающее большей сложностью[1)], чем в устройствах, рассматриваемых в настоящем стандарте;

- другие стандарты рассматривают устройства, проектируемые специально для применения в ядерной энергетике, тогда как в настоящем стандарте основное внимание уделено вопросам применения на АС тех устройств, которые первоначально не были предназначены для использования в ядерной энергетике.

Проектировщики систем контроля и управления (СКУ) для АС вынуждены все чаще использовать подобные устройства в связи с устареванием оборудования, малым объемом рынка ядерной энергетики по сравнению с промышленным рынком и растущим числом поставщиков, которые предпочитают проектировать системы, соответствующие общим стандартам безопасности, например МЭК 61508.

Поэтому для проектировщиков этих систем рекомендации настоящего стандарта крайне необходимы при выборе и оценке устройств с точки зрения их пригодности для применения на АС. В настоящем стандарте представлены рекомендации, без которых проектировщики СКУ должны были бы самостоятельно интерпретировать положения МЭК 60880, МЭК 62138 или МЭК 62566.

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

МЭК 61513 является стандартом первого уровня ПК 45А МЭК и содержит рекомендации, применимые к контролю и управлению на системном уровне. Он дополнен рекомендациями МЭК 60987 по проектированию аппаратных средств на уровне устройств, рекомендациями МЭК 60880 и МЭК 62138 по программному обеспечению и рекомендациями МЭК 62566 по проектированию потенциально сложных устройств. Все эти стандарты рассматривают проектные решения в области ядерной энергетики и применяют концепцию жизненного цикла.

МЭК 62671 является стандартом второго уровня ПК 45А МЭК, рассматривающим конкретную задачу выбора и оценки устройств для применения на АС при том, что эти устройства были изначально спроектированы для использования в неядерной области (и возможно, сертифицированы как соответствующие общепринятым стандартам по общей безопасности, например МЭК 61508). Кроме того, МЭК 62671 рассматривает только устройства, имеющие узкоспециализированную ограниченную функциональность и ограниченную возможность изменения конфигурации.

МЭК 62671 следует рассматривать совместно с МЭК 60880, МЭК 62138, МЭК 60987 и МЭК 62566, которые, являясь также стандартами ПК 45А МЭК, содержат полезную информацию в данной области и рекомендации по компьютерным системам, выполняющим функции, важные для безопасности АС.

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

c) Рекомендации и ограничения, касающиеся применения настоящего стандарта

Настоящий стандарт не устанавливает дополнительных функциональных требований к системам класса 1, 2 или 3[2)].

[1)] Общепринятое определение понятия «сложность» отсутствует, но бóльшая функциональность устройств связана с увеличением объема кода, конкуренцией системных ресурсов и процессами синхронизации, которые могут привести к неожиданным отказам устройств. В настоящем стандарте данные проблемы рассматриваются применительно только к устройствам с очень ограниченной функциональностью.

[2)] *Сравнение подходов к категоризации функций контроля и управления по влиянию на безопасность, а также к классификации СКУ, важных для безопасности атомных станций, применяемых в МЭК и Российской Федерации, представлено в приложении ДА.*

Аспектами, по которым настоящий стандарт устанавливает соответствующие требования, являются:

- использование планируемых процедур выбора и последующей оценки устройств-кандидатов для применения, включая вопросы интеграции рассматриваемых устройств в системы АС;
- критерии оценки функциональной пригодности устройства, содержащего встроенное программное обеспечение или использующего цифровые схемы, разработанные с помощью программных инструментов, таких как язык описания аппаратных средств;
- критерии, которые необходимо учитывать и сопоставлять при проведении общей оценки для достижения надлежащего уровня гарантии того, что рабочие характеристики устройства будут соответствовать заявленным;
- вопросы, связанные с безопасным применением выбранного устройства в системах АС.

Для гарантии сохранения актуальности в будущем настоящий стандарт акцентирует внимание на принципиальных вопросах, а не на конкретных технологиях.

В настоящем стандарте особое внимание уделено проверке сведений о процессах, выполняемых проектировщиком и изготовителем (которые могут быть разными организациями), так как именно они влияют на пригодность выбираемого устройства для его целевого применения. Такие данные могут быть получены от поставщика, с которым напрямую взаимодействует конечный пользователь.

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

Стандартом самого высокого уровня серии стандартов ПК 45А МЭК является МЭК 61513. В нем изложены общие требования к СКУ и оборудованию, используемым для выполнения важных для безопасности АС функций. МЭК 61513 является структурной основой серии стандартов ПК 45А МЭК.

МЭК 61513 содержит прямые ссылки на другие стандарты ПК 45А МЭК в отношении общих вопросов, касающихся категоризации функций и классификации систем, квалификации, разделения систем, защиты от отказов по общей причине, программного обеспечения компьютерных систем, аппаратного обеспечения компьютерных систем и проектирования пунктов управления. Стандарты второго уровня, на которые есть прямые ссылки, следует рассматривать вместе с МЭК 61513 как единый комплект документов.

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

Четвертый уровень серии стандартов ПК 45А МЭК представляют технические отчеты, которые не являются нормативными документами.

МЭК 61513 представлен в том же формате, что и основной стандарт по безопасности МЭК 61508, с той же схемой жизненного цикла безопасности в целом и схемой жизненного цикла системы. В отношении ядерной безопасности МЭК 61513 содержит толкование основных требований, действующих в атомной энергетике и приведенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4. В такой структуре МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 применительно к атомной энергетике. МЭК 61513 содержит ссылки на стандарты ИСО, а также на документы МАГАТЭ GS-R-3, GS-G-3.1 и GS-G-3.5 по вопросам, связанным с обеспечением качества (ОК).

Серия стандартов ПК 45А МЭК последовательно реализует и подробно описывает принципы и основные аспекты обеспечения безопасности, предусмотренные в нормах МАГАТЭ по безопасности АС и в серии документов МАГАТЭ по безопасности, в частности в Требованиях NS-R-1, устанавливающих требования к безопасности при проектировании АС, и в Руководстве по безопасности NS-G-1.3, рассматривающем СКУ, важные для безопасности АС. Терминология и определения, используемые в стандартах ПК 45А, соответствуют терминам и определениям, используемым в документах МАГАТЭ.

Примечание — Предполагается, что при проектировании систем контроля и управления АС, реализующих стандартные функции безопасности (например, обеспечение безопасности работников, защита объекта, химическая безопасность, энергетическая безопасность технологических процессов), будут применяться международные или национальные стандарты, основанные на требованиях таких стандартов, как МЭК 61508.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ СТАНЦИЙ

Выбор и использование промышленных цифровых устройств ограниченной функциональности

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

Дата введения — 2024—11—01

1 Область применения

1.1 Общие положения

Настоящий стандарт распространяется на устройства, содержащие встроенное программное обеспечение или электронно-конфигурированные цифровые схемы, произведенные не в соответствии со стандартами МЭК, применимыми к системам и оборудованию, важным для безопасности АС, но которые являются устройствами, потенциально применимыми на АС. Настоящий стандарт устанавливает требования к выбору и оценке таких устройств в случаях, когда они имеют узкоспециализированную[1)], ограниченную и специфическую функциональность, а также ограниченную возможность изменения конфигурации.

В соответствии с МЭК 61513 важные для безопасности СКУ классов 1, 2 и 3 могут быть реализованы с использованием обычного аппаратного оборудования, оборудования на основе цифровых технологий (компьютеры или программируемые аппаратные средства) или с использованием комбинации обоих типов оборудования. Настоящий стандарт устанавливает критерии приемлемости для выбора, оценки и использования определенных цифровых устройств, которые не были разработаны специально для применения в СКУ АС. Очень часто такие устройства разрабатывают в соответствии с МЭК 61508, а настоящий стандарт указывает, что соответствие МЭК 61508 может быть ключевым положительным фактором при квалификации компонентов, не созданных для ядерной энергетики, как пригодных для использования в ядерной отрасли.

Рассматриваемые в настоящем стандарте устройства являются узкоспециализированными устройствами ограниченной, специфической функциональности, содержащими или могущими содержать компоненты, находящиеся под управлением программного обеспечения или цифровых схем, разработанных с применением программных инструментов. Примерами таких устройств могут служить интеллектуальные датчики, механизмы установки положения клапанов, электрические защитные устройства или инверторы, которые содержат или могут содержать элементы под управлением программного обеспечения или цифровых схем, разработанных с применением программных инструментов. Настоящий стандарт не рассматривает аспекты программного обеспечения сложных универсальных устройств, которые рассмотрены в других стандартах, посвященных программному обеспечению, таких как МЭК 60880 и МЭК 62138. В настоящем стандарте рассмотрены факторы, которые следует учитывать при оценке пригодности этих узкоспециализированных устройств ограниченной, специфи-

[1)] В настоящем стандарте определение «узкоспециализированный» означает, что проект устройства предусматривает выполнение им одной конкретной функции и проектное решение нельзя изменить в производственных условиях. См. 3.7.

Издание официальное

ческой функциональности для использования на АС. Предложен дифференцированный подход к указанным факторам, при этом к системам более высокого класса применяют более строгие требования.

Указанные факторы включают в себя следующее:

- функциональную пригодность (выполняет ли устройство требуемые функции и достаточно ли защищены данные функции от помех, исходящих от любых других функций);
- данные, необходимые для подтверждения такой пригодности (такие, как соблюдение требований к процессу разработки, эксплуатационный опыт и уровень развития устройства);
- аспекты, связанные с интеграцией устройства в существующие системы (например, функциональная совместимость и влияние на техническое обслуживание и эксплуатацию);
- требования, связанные с гарантированием сохранения пригодности устройства на протяжении предусмотренного срока службы (например, срока службы АС).

В настоящем стандарте учтены положения других стандартов, особенно МЭК 60780, при рассмотрении вопросов квалификации аппаратных средств, не связанных со сложностями программного обеспечения, а именно при рассмотрении аспектов надежности, имеющих отношение к экологической аттестации и отказам, обусловленным старением или снижением физических характеристик. В качестве дополнительного руководства для анализа и оценки компонентов можно использовать другие стандарты, например МЭК 61508, однако следует иметь в виду, что сертификация только по стандартам, не имеющим отношения к ядерной энергетике, является недостаточной.

1.2 Вводная информация

Необходимость разработки настоящего стандарта обусловлена современными тенденциями на рынке СКУ, в том числе все большим устареванием существующих устройств, используемых в настоящее время на АС. Становится все труднее, а иногда и невозможно, идентифицировать аналоговые устройства или заменять многие существующие устройства идентичными, потому что поставщики все чаще используют микроконтроллеры, специализированные интегральные схемы (ASIC) и т. д., встроенные в устройства, рассматриваемые в качестве замены, и аналоговые устройства становятся все менее доступными.

Существуют различные риски технического характера, связанные с принятием этих устройств в эксплуатацию на АС, так как:

- многие из этих устройств не дублируют в точности функционал заменяемого устаревшего устройства, обладая в некоторых случаях меньшим, а в других случаях большим функционалом или даже несколько иным функционалом, который может не соответствовать первоначальному назначению конструкции;
- эти различия функционала не всегда очевидны. Существуют примеры проблем, возникающих из-за отсутствия рекомендаций в этой области, вызванных обычно разницей в целях проектирования оборудования для применения на АС и в других отраслях промышленности;
- устройства могут иметь специфические уязвимости или формы отказа, которые не существовали у первоначального оборудования и которые необходимо учитывать.

1.3 Область применения настоящего стандарта

Настоящий стандарт устанавливает требования к процедуре определения того, являются ли пригодными для применения в ядерной энергетике цифровые устройства промышленного качества, имеющие узкоспециализированную, ограниченную и специфическую функциональность и ограниченную возможность изменения конфигурации. Такая процедура требует применения критериев, подобных применяемым к нецифровым устройствам, но настоящий стандарт устанавливает дополнительные критерии, применимые к цифровым устройствам. Также учтены пределы реализуемости, позволяющие установить возможность внесения в оцениваемое промышленное устройство незначительных изменений или отсутствие такой возможности.

Настоящий стандарт предназначен для использования в контексте определенного приложения, по которому разработчики приложения ищут подходящие устройства для их реализации. Однако часто разработчик приложения вынужден рассматривать возможность применения устройств, не предназначенных специально для ядерной энергетики. Цель настоящего стандарта заключается в оказании помощи разработчику приложений в выборе и использовании таких устройств в соответствии с классом безопасности и требованиями к целевому назначению.

Настоящий стандарт может быть применен на различных этапах жизненного цикла проектирования системы, как указано в МЭК 61513. Он может быть применен на раннем этапе жизненного цикла проектирования АС, когда архитектура конкретной СКУ существует только в виде чернового эскиза и доступность подходящих устройств может повлиять на проект системы. При более позднем применении, когда проектирование системы завершено, настоящий стандарт можно использовать для оценки планируемых к применению устройств. И наконец, настоящий стандарт может быть также применен при доработке оборудования, когда система уже находится в эксплуатации, а некоторые устройства необходимо заменить.

Классы оборудования (систем) 1, 2 и 3 характеризуют разными наборами требований, которые устанавливают в зависимости от важности оборудования (системы) для обеспечения безопасности. Настоящий стандарт следует интерпретировать в контексте категории выполняемой функции безопасности и класса системы. Это означает, что целесообразным и ожидаемым является дифференцированное толкование требований. Также считается, что допустимые виды отказов могут значительно отличаться для разных АС в зависимости от их применения, и это может определять приемлемость данного устройства или форму его использования. Интерпретацию и строгость соблюдения требований настоящего стандарта следует определять для каждого отдельного случая.

Другая довольно часто встречающаяся проблема заключается в нежелании поставщика предоставить доказательства корректности работы устройства, например подробные данные о внутренних функциях устройства или о том, как оно было разработано. Эту проблему следует решать как можно раньше, например на этапе предварительного отбора поставщиков, и, возможно, выбрать других поставщиков в целях соблюдения требований настоящего стандарта.

В плане оценки и применения (EAP)[1)] устанавливают задачи оценки и приводят рекомендации по интерпретации настоящего стандарта для конкретного устройства и его применения. В указанном плане определяют и обосновывают подходы, которые следует применять в проблематичных случаях, включая виды компенсирующих мер, которые следует принять для решения таких проблем, как несоответствие необходимого и доступного функционала или отсутствие обычных доказательств корректности работы устройств.

Конечным шагом процесса оценки является подготовка отчета об оценке и применении (EAR). В этом отчете определяют квалифицируемое устройство, его применение, для которого устройство квалифицируют, и все ограничения его использования.

1.4 Структура стандарта

Настоящий стандарт организован следующим образом:

- раздел 5 посвящен применимости настоящего стандарта и процессу оценки, при этом рассмотрены:

1) изменение функциональности устройства, входящего в область распространения настоящего стандарта;

2) степень гибкости и возможность изменения конфигурации устройства, входящего в область распространения настоящего стандарта;

3) входные и выходные данные процесса оценки и EAP, в котором документально должно быть зафиксировано, как эксперт(ы) применяет(ют) положения настоящего стандарта;

4) содержание EAP, рассмотренные доказательства и результаты анализа этих доказательств, а также заключения о пригодности устройства;

- в разделе 6 рассмотрены составляющие функциональности и другие требования, которые необходимо оценить, такие как:

1) минимальный уровень документации по разработке планируемого к использованию устройства;

2) способность устройства выполнять заданную(ые) функцию(и);

3) невосприимчивость основной функции устройства к нежелательному воздействию избыточных функций;

4) способность устройства функционировать во всех ожидаемых условиях окружающей среды согласно МЭК 60780 и другим указанным стандартам;

5) надежность и ремонтопригодность устройства;

[1)] Требование о наличии Плана квалификации, указанное в стандарте МЭК 61513, выполняется в Плане оценки и применения.

6) достаточность мер обеспечения информационной безопасности;

7) предоставляемая пользовательская документация;

- в разделе 7 приведены критерии, обеспечивающие уверенность в корректности проектирования и изготовления устройства, включающие:

1) возможность использования предыдущих аттестаций, не относящихся к области ядерной энергетики;

2) методы, позволяющие избегать систематических отказов;

3) применение жизненного цикла обеспечения безопасности при проектировании устройства;

4) обеспечение качества изготовления;

5) допустимые способы компенсации недостаточности доказательств в отношении некоторых вопросов путем завершения оценки в пользу принятия устройства на основе стабильности изделия, целенаправленного опыта эксплуатации, уточнений в документации или дополнительных испытаний и/или анализа;

- в разделе 8 рассмотрены критерии интеграции устройства в СКУ АС, включающие:

1) ограничения способов использования устройства (например, самый высокий класс системы, для применения в которой оно квалифицировано),

2) модификации устройства или целевой системы, необходимые для интеграции устройства в целевую систему;

3) интеграция и ввод в эксплуатацию устройства, интегрированного в системы безопасности АС;

- в разделе 9 рассмотрены аспекты сохранения приемлемости устройства, а именно:

1) уведомления проектировщиков или изготовителей устройства, предоставляемые пользователям устройства;

2) срок оказания технической поддержки устройства;

3) сохранение инструментов для технического обслуживания и документации;

4) рекомендации для конечного пользователя.

2 Нормативные ссылки

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

IEC 60671:2007, Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing (Атомные электростанции. Системы контроля и управления, важные для безопасности. Контрольные испытания)

IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification (Атомные электростанции. Электрооборудование системы безопасности. Квалификация)[1)]

IEC 60880:2006, Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer based systems performing category A functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А)

IEC 60980, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations (Рекомендуемая практика проведения сейсмической квалификации электрооборудования системы безопасности для атомных электростанций)[2)]

IEC 60987:2007, Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer based systems (Электростанции атомные. Контрольно-измерительные приборы и системы управления, важные для обеспечения безопасности. Требования к проектированию аппаратуры для компьютерных систем)[3)]

[1)] Заменен на IEC/IEEE 60780-323:2016. Однако для однозначного соблюдения требования настоящего стандарта рекомендуется использовать только указанное в этой ссылке издание.

[2)] Заменен на IEC/IEEE 60980-344:2020. Однако для однозначного соблюдения требования настоящего стандарта рекомендуется использовать только указанное в этой ссылке издание.

[3)] Действует IEC 60987:2021. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

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

IEC 61226, Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления)[1)]

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

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

IEC 62138:2004, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий B или C)[2)]

ISO 9001:2008, Quality management systems — Requirements (Системы менеджмента качества. Требования)[3)]

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **вспомогательная функция** (ancillary function): Любая функция, выполняемая потенциально применимым устройством, которая поддерживает его основную функцию.

Примечание 1 — Примерами служат функции потенциально применимого устройства, используемые для поддержки функции, важной для безопасности, такие как обеспечение надлежащих способов контроля рабочих параметров устройства или контроля его непрерывного корректного функционирования, необходимого для безопасного применения устройства.

Примечание 2 — См. также термины «основная функция» и «избыточная функция».

3.2 **поддающийся контролю** (auditable): Свойство задокументированного факта, заключающееся в легкой возможности его проверки независимыми лицами.

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 с учетом важности выполняемой функции для обеспечения безопасности. Если функция не значима для безопасности, то ей не присваивают обозначение категории[4)].

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

Примечание 2 — Категории функций контроля и управления определены в МЭК 61226. Каждой категории соответствует ряд требований, предъявляемых как к функции контроля и управления (касающихся их спецификации, проектирования, внедрения, верификации и валидации), так и ко всей цепочке элементов, необходимых для реализации этой функции (касающихся характеристик и соответствующей квалификации), независимо от того, как эти элементы распределены между взаимосвязанными СКУ. Для большей ясности настоящий стандарт определяет категории функций контроля и управления и классы СКУ и устанавливает соотношение между категорией функции и минимальным требуемым классом связанных с этой функцией систем и оборудования.

[МЭК 61513-2011, пункт 3.4]

3.4 **класс СКУ** (class of an I&C system): Одно из трех возможных обозначений (1, 2, 3) системы, важной для безопасности, присваиваемое в зависимости от того, какие функции контроля и управле-

---

[1)] Заменен на IEC 61226:2020 «Nuclear power plants — Instrumentation, control and electrical power systems important to safety — Categorization of functions and classification of systems».

[2)] Заменен на IEC 62138:2018. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[3)] Заменен на ISO 9001:2015. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[4)] *В Российской Федерации категории управляющим и информационным функциям назначают в соответствии с Федеральными нормами и правилами в области использования атомной энергии НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций».*

ния, имеющие разное значение для безопасности, должна реализовывать система. Если СКУ не выполняет функции, важные для безопасности, то ей не присваивают обозначение класса[1)].

Примечание — См. также термины «категория функции контроля и управления», «элемент, важный для безопасности».

[МЭК 61513:2011, пункт 3.6]

3.5 **отказ по общей причине;** ООП (common cause failure, CCF): Отказ двух или более конструкций, систем или компонентов, явившийся результатом единичного события или причины[2)].

[МЭК 61513:2011, пункт 3.8]

3.6 **компьютерная система** (computer-based system): СКУ, функции которой в большой степени зависят или полностью выполняются с использованием микропроцессоров, программируемого электронного оборудования или компьютеров.

Примечание — То же, что система с программным обеспечением, программируемая система.

[МЭК 61513-2011, пункт 3.11]

3.7 **узкоспециализированная функциональность** (dedicated functionality): Свойство устройств, разработанных для выполнения только одной четко определенной функции или только очень узкого диапазона функций, например таких, как сбор данных и оповещение о значении технологического параметра или переключение с источника электропитания переменного тока на источник постоянного тока. Эта функция (или узкий диапазон функций) присуща данному устройству и не является результатом программирования пользователем.

Примечание 1 — Вспомогательные функции (например, самоконтроль, самокалибровка, передача данных) также могут быть реализуемы устройством, но они не меняют основную узкую область применения устройства.

Примечание 2 — Настоящий стандарт применим к устройствам узкоспециализированной функциональности, которые соответствуют всем критериям, приведенным в 5.2.2.

Примечание 3 — Термин «узкоспециализированная» в том смысле, в котором он используется в настоящем стандарте, относится к конструкции, выполняющей одну конкретную функцию, которую нельзя изменить в производственных условиях.

3.8 **цифровое устройство** (digital device): Устройство, реализация которого основана на операциях, выполняемых с использованием сигналов определенных дискретных уровней, или которое находится в определенных дискретных внутренних состояниях и между этими состояниями происходят переключения.

Примечание 1 — Функции таких устройств обычно определяются процессами, которые включают в себя разработку и испытания с применением языков описания аппаратных средств или программного обеспечения. Такие устройства могут быть внутренне управляемыми программным обеспечением или состоять из специализированных интегральных схем (ASIC) или программируемых логических интегральных схем (ПЛИС) и др., конфигурированных с помощью программного обеспечения.

Примечание 2 — Устройства, оборудование или системы, управляемые программным обеспечением, описывают как «компьютерные», тогда как термин «цифровой» имеет более широкий смысл и включает 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. Единица оборудования представляет собой отдельно определяемый (и обычно заменяемый) элемент или часть системы.

Примечания

1 См. также термины «компонент»[3)], «СКУ».

[1)] *Федеральные нормы и правила не устанавливают классификацию систем по классам. В НП-001-15 «Общие положения обеспечения безопасности атомных станций» установлена классификация элементов по классам в зависимости от влияния отказа конкретного элемента на безопасность АС.*

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

[3)] *В соответствии с ГОСТ Р МЭК 61513—2020 «компонент: Одна из составных частей системы. Компонент может представлять собой аппаратное или программное обеспечение и может сам состоять из других компонентов».*

2 Оборудование может включать в себя программное обеспечение.

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

4 Данное определение отличается от приведенного в МЭК 60780. Отличие заключается в том, что в МЭК 61513 под термином «оборудование» понимают часть системы, тогда как в МЭК 60780 оборудование рассматривают как объект квалификации.

[МЭК 61513:2011, пункт 3.16]

3.10 **язык описания аппаратных средств** (hardware description language, HDL): Язык, используемый для формального описания функций и/или структуры электронного компонента для документирования, моделирования или синтеза.

Примечание — Наиболее широко используемыми языками описания аппаратных средств являются VHDL (см. IEEE 1076) и Verilog (см. IEEE 1364).

[МЭК 62566:2012, пункт 3.6]

3.11 **HDL-программируемое устройство;** HPD (HDL-programmed device, HPD): Интегральная микросхема, конфигурированная (для СКУ АС) с использованием языков описания аппаратных средств или соответствующих программных средств.

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

Примечание 2 — При разработке HPD могут быть использованы предварительно разработанные блоки.

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

[МЭК 62566:2012, пункт 3.7]

3.12 **функция контроля и управления** (I&C function): Функция управления, эксплуатации и/или контроля определенной части технологического процесса.

Примечание 1 — Термин «функция контроля и управления» используется инженерами-технологами для структурирования функциональных требований к контролю и управлению. Функцию контроля и управления определяют таким образом, чтобы:

- она давала полное представление о цели выполнения функции,
- ей могла быть присвоена категория по степени важности для безопасности,
- для достижения цели она охватывала все составляющие, от датчика до исполнительного устройства.

Примечание 2 — Функцию контроля и управления можно подразделить на несколько подфункций (например, функция измерения, функция управления, функция исполнения) с целью распределения по СКУ.

[МЭК 61513-2011, пункт 3.28]

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

Термин используется как обобщающий, охватывающий все элементы системы, включая внутренние источники питания, датчики и другие входные устройства, скоростные линии передачи данных и другие коммуникационные линии, интерфейсы исполнительных устройств и других выходных устройств (см. примечание 2). Различные функции системы могут использоваться как специально выделенные, так и общие распределенные ресурсы.

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

Примечание 2 — Элементы, входящие в состав конкретной СКУ, определяют границы этой системы.

Примечание 3 — В соответствии с типичными функциональными возможностями МАГАТЭ различает системы автоматического и ручного управления, системы ЧМИ, системы защиты и системы блокировки.

[МЭК 61513-2011, пункт 3.29]

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

[МЭК 61513-2011, пункт 3.32]

3.15 **элемент, важный для безопасности** (item important to safety): Элемент, который является частью группы безопасности[1)] и/или неисправность или отказ которого может привести к радиационному облучению персонала на площадке или населения.

Элементы[2)], важные для безопасности[3)], включают:

a) конструкции, системы и компоненты, неисправность или отказ которых могут привести к превышающему допустимые пределы облучению персонала АС или населения;

b) конструкции, системы и компоненты, которые предотвращают вероятные нарушения нормальной эксплуатации, могущие привести к созданию аварийной ситуации;

c) средства, обеспечивающие смягчение последствий неисправности или отказа конструкций, систем или компонентов.

Примечание 1 — Данное определение предполагает охватить все аспекты ядерной безопасности.

Примечание 2 — В настоящем стандарте из элементов рассмотрены преимущественно системы контроля и управления или функции контроля и управления.

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

[Глоссарий МАГАТЭ по вопросам безопасности, 2007]

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

3.17 **полный жизненный цикл безопасности контроля и управления** (overall I&C safety life cycle): Необходимый объем действий, осуществляемых для реализации систем и оборудования, важных для безопасности архитектуры контроля и управления, совершаемый в течение периода времени начиная с установления требований к контролю и управлению на основе проекта безопасности АС и заканчивая моментом, когда ни одна СКУ не пригодна для эксплуатации.

[МЭК 61513-2011, пункт 3.34]

3.18 **основная функция** (primary function): Отдельная функция (или минимальный набор связанных функций) потенциально применимого устройства, востребованная системой, важной для безопасности, для выполнения ее функции, необходимой при анализе безопасности, которая, как предполагается, будет осуществляться автономно и способствовать выполнению функции системы.

Примечание 1 — Согласно 5.2.2 многофункциональное устройство может обеспечить возможность использования нескольких своих главных функций в качестве основной функции, но такое устройство может не входить в область применения настоящего стандарта и в любом случае будет менее предпочтительным, чем устройство с одной функцией.

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

Примечание 3 — Например, можно использовать интеллектуальный усилитель для генерации и выдачи как логарифмического, так и линейного электрического сигнала, каждый из которых может быть использован в качестве сигнала аварийного останова реактора. Эти две функции формируют набор основных функций (и для целей настоящего стандарта к этому набору применим термин «основная функция»), тогда как функция изменения уровня выходного сигнала или фильтрования выходных сигналов является вспомогательной функцией. Другие функции, не являющиеся необходимыми для выбора устройства, такие как локальное изображение или дистанционная сигнализация посредством сетевого соединения, являются избыточными функциями.

Примечание 4 — Например, интеллектуальный датчик может обеспечивать вывод сигнала, представляющего поток или уровень, через аналоговый канал диапазона от 4 до 20 мА или посредством HART протокола.

[1)] *Согласно Глоссарию МАГАТЭ по вопросам безопасности издания 2018 г.: «группа безопасности (safety group): Совокупность оборудования, предназначенная для выполнения всех необходимых действий в случае конкретного исходного события с целью предотвращения превышения пределов, установленных в проектных основах для ожидаемых при эксплуатации событий и проектных аварий».*

[2)] *Согласно НП-001-15, приложение № 2, пункт 97: «Элементы АС (элементы) — строительные конструкции, оборудование, приборы, трубопроводы, средства измерения, контроля, управления и автоматики, кабели и другие изделия, обеспечивающие выполнение заданных функций самостоятельно или в составе систем и рассматриваемые в проекте АС в качестве структурных единиц при выполнении анализов надежности и безопасности». В НП-001-15 элементы АС разделены на важные для безопасности и остальные, не влияющие на безопасность.*

[3)] *Согласно НП-001-15, приложение № 2, пункт 9: «Безопасность АС (ядерная и радиационная безопасность АС) — свойство АС обеспечивать надежную защиту персонала, населения и окружающей среды от недопустимого в соответствии с федеральными нормами и правилами в области использования атомной энергии радиационного воздействия».*

Если проектировщик в области применения ядерной энергии решает в целях безопасности использовать сигнал от 4 до 20 мА, то это будет основной функцией датчика, а другие возможности вывода сигнала будут избыточными.

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

Примечание 1 — Квалификационные требования обусловлены определенным классом СКУ и конкретным случаем применения.

Примечание 2 — Как правило, СКУ реализуют на основе взаимодействующих комплектов оборудования. Такое оборудование может быть разработано при проектировании или уже существовать (быть разработанным в рамках предыдущего проекта или являться готовым COTS). Как правило, присвоение оборудованию квалификации «СКУ» осуществляют поэтапно: сначала проводят квалификацию отдельных единиц уже существующего оборудования (обычно в начале процесса реализации системы); а на втором этапе проводят квалификацию комплексной СКУ (окончательно реализованного конструктивного исполнения).

[МЭК 61513-2011, пункт 3.38]

3.20 **качество** (quality): Степень соответствия набора собственных характеристик требованиям.

[ИСО 9000:2005]

3.21 **обеспечение качества** (quality assurance): Функция системы менеджмента, которая обеспечивает уверенность в том, что установленные требования будут выполнены.

[Глоссарий МАГАТЭ по вопросам безопасности, 2007]

3.22 **требование** (requirement): Выражение, содержащееся в документе, сообщающее критерии, которые должны быть выполнены в случае необходимости соблюдения соответствия документу, отклонение от которого недопустимо.

[Директивы ИСО/МЭК, часть 2, 2011, пункт 3.3.1]

Примечание 1 — В документах ПК 45А МЭК различают следующие типы требований:

- требования безопасности — требования, предписываемые органами власти (законодательными, контрольно-надзорными или органами по стандартизации) и проектными организациями в отношении обеспечения безопасности АС на протяжении ее жизненного цикла с точки зрения воздействия на человека, общество и окружающую среду;
- функциональные требования и требования к рабочим характеристикам — функциональные требования устанавливают, какие действия должна выполнять система в ответ на конкретные сигналы или условия, а требования к рабочим характеристикам указывают значения параметров, например времени отклика и точности;
- эксплуатационные требования — требования к производственной мощности и возможностям АС, предъявляемые собственником;
- требования к проектированию АС — технические требования к общему проектированию АС, соблюдение которых обеспечивает выполнение требований безопасности и эксплуатационных требований;
- требования к проектированию системы — требования к проектированию отдельных систем, соблюдение которых обеспечивает соответствие проекта всей АС требованиям к проектированию АС;
- требования к оборудованию — требования к отдельным единицам оборудования, соблюдение которых обеспечивает соответствие требованиям к проектированию системы.

Примечание 2 — В Глоссарии МАГАТЭ по вопросам безопасности, издания 2007 г., приведено следующее определение:

Требуемый, требование — требуемый (национальными или международными) законодательными или нормативными актами, или основами безопасности, или требованиями безопасности МАГАТЭ.

Это определение удобно для использования в публикациях МАГАТЭ, но слишком узко для применения в техническом стандарте. Оно соответствует термину «требования безопасности», применяемому в документах ПК 45А МЭК, приведенному в примечании 1.

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

Примечание 4 — При наличии отклонений от требований к устройству эти отклонения и их обоснование должны быть четко документально зафиксированы в EAR, чтобы потенциальный пользователь устройства мог обосновать его применение или выбор альтернативного устройства.

[МЭК 61513-2011, пункт 3.44]

3.23 **ограниченная возможность изменения конфигурации** (restricted configurability): Возможность конфигурировать устройства только очень ограниченными способами, выбирая из относительно малого числа вариантов, каким образом устройство будет функционировать в предполагаемом применении.

3.24 **защищенность** (security): Способность компьютерной системы защитить информацию и данные так, чтобы неавторизованные системы и лица не могли прочесть или изменить существующую информацию, выполнить или приостановить выполнение действий по управлению и отказать в доступе к информации авторизованным системам и лицам.

Примечание — В настоящем стандарте для интерпретации термина «защищенность» следует заменить выражение «компьютерная система» на выражение «цифровое устройство, содержащее программное обеспечение или конструктивные исполнения цифровых схем, созданных с помощью языков описания аппаратных средств».

[МЭК 61513-2011, пункт 3.48]

3.25 **самоконтроль** (self-supervision): Автоматическое испытание производительности аппаратных средств системы и непротиворечивости программного обеспечения компьютеризированных СКУ.

Примечание 1 — Употребляемое в настоящем стандарте определение имеет более широкий смысл, выходящий за рамки только испытаний, который включает автоматические функции, выполняемые программируемым устройством, разработанным для обнаружения (главным образом) отказов аппаратных средств, могущих по своей природе быть как безопасными, так и опасными (отказами, которые препятствуют выполнению устройством своей функции обеспечения безопасности), с целью преобразовать ситуацию в безопасную путем оповещения об отказе или побуждения устройства вернуться в безопасное состояние.

Примечание 2 — См. также «контрольное испытание», которое не может быть инициировано автоматически.

Примечание 3 — Выражение «контрольное самотестирование» является синонимом.

[МЭК 60671:2007, пункт 3.8]

3.26 **программное обеспечение** (software): Программы (наборы упорядоченных инструкций), данные, правила и любая относящаяся к ним документация, касающиеся эксплуатации компьютерной СКУ.

[МЭК 61513-2011, пункт 3.51]

3.27 **анализ критичности программного обеспечения** (software criticality analysis): Анализ программного обеспечения с целью классификации каждой заложенной в нем функции с точки зрения его потенциальной способности вызывать опасные отказы.

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

[МЭК 61513-2011, пункт 3.53]

3.29 **избыточная функция** (superfluous function): Все функции, выполняемые потенциально применимым устройством, которые не относятся к требуемым.

Примечание 1 — Например, основной функцией может быть восприятие сигнала диапазона от 4 до 20 мА о распространении давления и передача его на другое устройство; вспомогательной функцией может быть функция, обеспечивающая настройку параметров фильтрования этого выходного сигнала для достижения желательного безопасного функционирования, а избыточной функцией может быть получение второго выходного сигнала, например сигнала напряжения, не требующегося для безопасного функционирования.

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

3.30 **контрольное испытание** (surveillance test): Инициируемое вручную сквозное испытание функции безопасности. Оно может быть проведено как однократное сквозное испытание или как серия перекрывающих друг друга испытаний. Испытание инициируют вручную, но в нем может быть задействовано автоматическое или полуавтоматическое испытательное оборудование для выполнения испытания и/или регистрации результатов испытания. Контрольные испытания выполняют для основной(ых) функции(ий) безопасности устройства.

Примечание 1 — МЭК 60671 дает следующее определение термина «контрольное испытание»: «полный объем действий для подтверждения сохранения функциональных способностей СКУ и оборудования, важных для безопасности, а также подтверждения соблюдения проектных требований». Настоящий стандарт обращает внимание на то, что автоматические контрольные самотестирования являются требованием МЭК 61508 для более высоких уровней обеспечения безопасности и что такие испытания отличаются от инициированных вручную испытаний вследствие большой разницы в частоте инициирования и полноте испытаний.

Примечание 2 — Синонимом является термин «контрольная проверка».

Примечание 3 — См. также «самоконтроль» («контрольное самотестирование»), который инициируют автоматически.

3.31 **систематический отказ** (systematic fault): Отказ, однозначно обусловленный определенной причиной, который может быть исключен только путем внесения изменений в проект или в процесс изготовления, изменений эксплуатационных операций, документации или другими подобными действиями.

[МЭК 61513-2011, пункт 3.60]

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

АВПДО — анализ видов, последствий и диагностики отказов (failure modes effects and diagnostic analysis, FMEDA);

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

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

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

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

КМ — компенсирующая мера (compensatory measure, CM);

ОК — обеспечение качества (quality assurance, QA);

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

ПЛК — программируемый логический контроллер (programmable logic controller, PLC);

ППЗУ — программируемое постоянное запоминающее устройство (programmable read only memory, PROM);

СКУ — система контроля и управления (Instrumentation and control system, I&C system);

ЧМИ — человеко-машинный интерфейс (human machine interface, HMI);

ЭМП — электромагнитные помехи (electromagnetic interference, EMI);

ASIC — специализированная интегральная схема (application specific integrated circuit);

СВ — компьютерный, компьютеризированный (computer-based);

COTS — коммерческое изделие серийного производства (commercial off the shelf, COTS);

CPU — центральный процессор (central processing unit);

EAP — план оценки и применения (evaluation and application plan);

EAR — отчет об оценке и применении (evaluation and application report);

HART — протокол взаимодействия с удаленным датчиком с шинной адресацией [highway addressable remote transducer (protocol)];

HAZOP — возможные риски и надежность функционирования (hazard and operability);

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

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

I/O — вход/выход (input/output);

VHDL — язык описания аппаратного обеспечения на быстродействующих интегральных схемах (very high speed integrated circuit hardware description language).

5 Общие требования

5.1 Общие положения

Основная проблема, связанная с цифровыми устройствами, заключается в том, что они очень часто бывают сложными, и эта сложность создает потенциальную возможность систематических отказов в их конструктивном исполнении, особенно в их программном обеспечении или HDL-программируемом устройстве. Такие отказы могут оказаться необнаруженными до возникновения функционального нарушения вследствие того, что подобное событие не было предусмотрено испытаниями. В связи с этим главная цель настоящего стандарта состоит в установлении критериев оценки конструктивного исполнения цифрового устройства для обеспечения соразмерного с классом назначенного применения уровня гарантии того, что в условиях применения задействованное устройство не окажется неспособным выполнять свою функцию из-за систематических отказов.

С этой целью в 5.2.2 изложены конкретные требования, которым должно удовлетворять устройство, чтобы к нему можно было применять настоящий стандарт. Далее настоящий стандарт устанавливает процедуру и требования для оценки потенциально применимого устройства, основанные на пригодности его функций и уровне уверенности в корректности его конструктивного исполнения и функционирования, а во вторую очередь — на уверенности в неизменности проектных технических требований к устройству. Также рекомендуется учитывать вероятность долгосрочной поддержки эксплуатации устройства.

5.2 Применение настоящего стандарта

5.2.1 Общие положения

Целью данного подраздела является обеспечение помощи в применении настоящего стандарта тем, кто осуществляет оценку пригодности промышленного устройства для использования в системах, важных для безопасности АС.

В настоящем подразделе приведены:

- критерии принятия решения о применимости настоящего стандарта;
- принципы, используемые при определении применимости данного стандарта.

5.2.2 Критерии применимости настоящего стандарта

Цифровое устройство, к которому может быть применим настоящий стандарт, должно соответствовать следующим критериям:

a) Устройство представляет собой уже существующее цифровое устройство, которое содержит ранее разработанное программное обеспечение или программируемую логику (например, HPD) и является кандидатом для применения в системах, важных для безопасности.

b) Основная выполняемая функция четко определена и применима только к одному типу функций в системе контроля и управления, например: измерение температуры или давления, установление положения клапана, управление скоростью механического устройства или обеспечение аварийной сигнализации.

c) Основная выполняемая функция концептуально проста и ограничена (хотя способ ее выполнения устройством может быть сложным).

d) Устройство не предназначено ни для перепрограммирования после изготовления, ни для изменения его функций обычным способом так, чтобы оно выполняло концептуально иную функцию: пользователи могут конфигурировать только предустановленные параметры.

e) Если основную функцию устройства можно настроить или конфигурировать, то эта возможность ограничена параметрами процесса (технологический диапазон процесса), эксплуатационными характеристиками (быстродействие или привязка ко времени), настройкой интерфейса сигналов (например, выбор диапазона напряжения или тока) или коэффициентами усиления (например, настройка зоны пропорциональности).

Примечание 1 — Предпочтение отдают устройствам без вспомогательных функций и, в частности, без избыточных функций. Если устройство обладает такими функциями, то их идентифицируют и оценивают с точки зрения вероятности создания ими помех для основной функции устройства согласно 6.3 и 6.5 соответственно.

Примечание 2 — Необходимо исключить устройства, обеспечивающие возможность устанавливать функциональность с использованием либо универсального языка, например языка С, либо языка, ориентированного на конкретное приложение, например на многозвенные логические схемы или функциональные блоки.

Примечание 3 — Невозможно определить все устройства, подпадающие под действие настоящего стандарта, но перечисленные ниже функции служат примерами при условии, что они обеспечивают возможность конфигурирования, соответствующую заявленной в области применения настоящего стандарта:

- датчики давления и температуры;
- интеллектуальные датчики (например, датчик давления);
- механизмы установки положения клапана;
- электрозащитные устройства, такие как реле максимального напряжения/тока;
- пусковое устройство двигателя;
- специализированное устройство индикации (например, многосегментный светодиодный дисплей);
- выделенные простые интерфейсы связи.

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

- ПЛК;
- устройства с программируемым языком независимо от их ограниченного характера [в смысле количества функциональных блоков (или эквивалентных элементов) или входов и выходов], если в проектах таких устройств

заложена возможность конфигурирования более чем для одного применения (например, одноконтурный цифровой контроллер с языком функциональных блоков).

5.3 Общие требования к процессу оценки

5.3.1 Процесс оценки

Настоящий подраздел определяет основные шаги, которые следует предпринять при выборе и оценке потенциально применимого устройства, предназначенного для целевого применения. Данные шаги показаны на рисунке 1 и описаны ниже.

Процесс оценки и определения сценария применения состоит из следующих шагов:

a) Необходимым условием при осуществлении оценки и определении применения является наличие документации, содержащей все функциональные требования и требования к рабочим характеристикам, предъявляемые к устройству с учетом его целевого назначения. Это может повлечь за собой изменение предусмотренного проектом применения[1)]. При определении требований к потенциально применимому устройству необходимо рассмотреть следующие аспекты:

- достаточно подробное описание назначения целевой системы или сценария применения устройства, касающееся их роли в обеспечении безопасности, с целью категоризации функции целевого применения в соответствии с МЭК 61226 или путем равнозначного процесса в соответствии с МЭК 61226, утвержденного государственными органами;
- категорию безопасности функции целевого применения и класс системы, задействованной в этом целевом применении;
- основные функции, требуемые от устройства, включая функциональные требования и требования к рабочим характеристикам, например времени отклика, в соответствии с критериями, приведенными в 5.2.2;
- все прочие конкретные свойства и характеристики безопасности, требуемые от изделия, как указано в разделе 6.

b) Необходимо подготовить план оценки и применения (EAP), в котором документально зафиксировать функциональные требования и требования к рабочим характеристикам в соответствии с 5.3.2 и 5.3.4 и, при необходимости, определить стратегию в отношении многоцелевого применения рассматриваемого устройства (выполнять ли единую оценку для всех намеченных видов применения или оценивать их отдельно).

При выполнении EAP может потребоваться его пересмотр, исходя из полученных результатов или наличия подтверждения его корректности.

c) Потенциально применимое устройство выбирают и оценивают в соответствии с настоящим стандартом только в том случае, если оно отвечает требованиям 5.2.2.

В случае замены устройства для уже разработанной системы функциональные требования и требования к рабочим характеристикам устройства в целом уже известны, тогда как для новой системы требования могут быть более гибкими из-за большей степени свободы при определении интерфейсов между устройствами. При разработке новых систем разработчики, скорее всего, заранее рассматривают вероятность успешной оценки каждого потенциально применимого устройства и возможные последствия его применения в целевой системе, сужая таким образом выбор устройств. Это приводит к стиранию границ между процессами выбора и оценки устройств, но не может быть причиной несоблюдения предписанных для этих процессов процедур.

d) Каждое потенциально применимое устройство необходимо оценивать в соответствии с EAP (описанным в 5.3.2) и 5.3.4 для подтверждения соответствия устройства требованиям настоящего стандарта.

e) Результаты оценки необходимо документально зафиксировать в отчете об оценке и применении (EAR). В этом отчете должно быть документально зафиксировано следующее:

1) оценка потенциально применимого устройства на соответствие каждому требованию для целевого применения в соответствии с EAP; и

[1)] Несмотря на то, что настоящий стандарт применим к замене любого устройства цифровым, необходимо учитывать некоторые частные проблемы, возникающие при замене аналоговых устройств цифровыми, например частоту выборки и теорему о выборке, аналого-цифровое преобразование и помехи, обусловленные младшим разрядом. Все это может поставить под вопрос возможность обнаружения какого-либо события цифровым устройством. Но, с другой стороны, возможное улучшение фильтрации при использовании цифровых технологий позволяет цифровому устройству обнаруживать событие, к которому аналоговое устройство было бы невосприимчиво. Такие вопросы необходимо учитывать при изменении проектных основ и требований к цифровому устройству.

2) четкий вывод о его применимости с указанием того, что устройство применимо как есть, применимо при некоторых конкретных условиях и/или ограничениях или неприменимо.

При написании EAR либо ссылаются на точно и полно изложенные требования в уже существующих и доступных документах, либо включают в него задокументированные установленные требования.

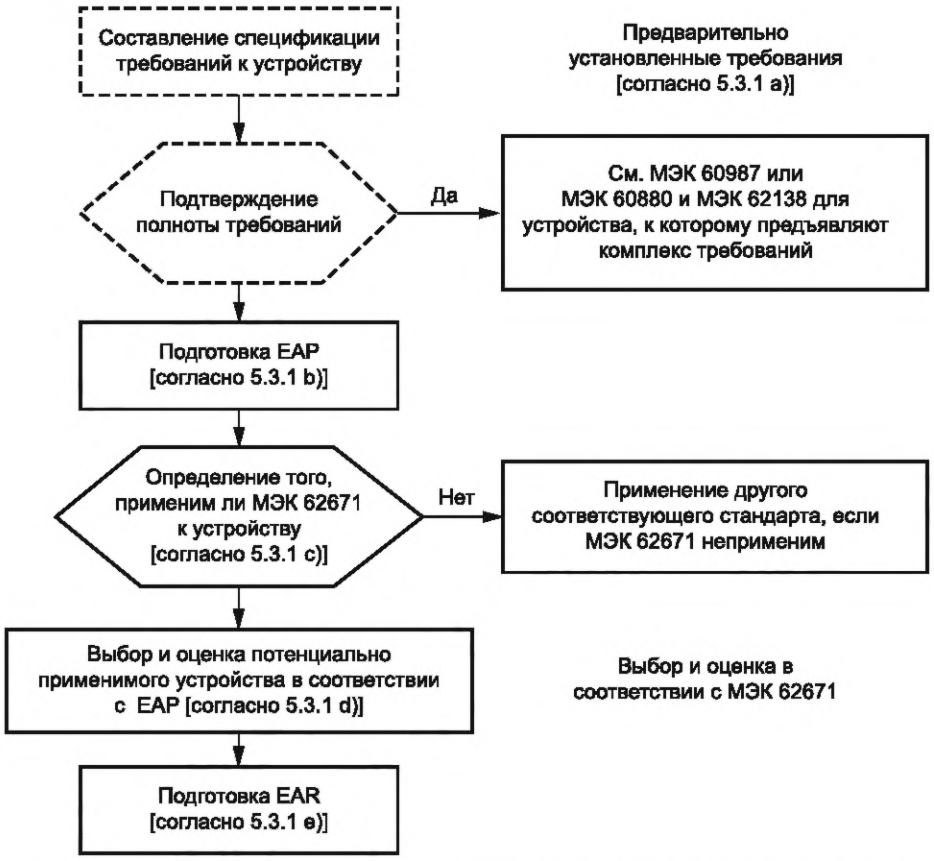

Рисунок 1 — Процесс выбора и оценки потенциально применимого устройства

5.3.2 План оценки и применения (EAP)

Целью настоящего пункта является установление назначения и содержания EAP.

EAP должен:

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

b) определять объем и актуальность работ по оценке в части:

- применения (функция безопасности) или применений и соответствующего класса или классов систем;
- при рассмотрении более одного применения устанавливать, проводить ли квалификацию только для наивысшего класса или для каждого;
- определения потенциально применимого устройства, которое следует поместить в EAR;

c) определять технические ресурсы и их квалификацию, необходимую для выполнения работ по оценке, например:

- специалистов по безопасному применению для обеспечения полноты спецификации требований, особенно при осуществлении модернизации;
- специалистов по программному обеспечению для проверки восприимчивости программного обеспечения к систематическим отказам;
- специалистов по определенным аппаратным средствам для квалификационной оценки на электромагнитную совместимость и влияние ЭМП и т. д.;

d) определять, какие критерии, установленные в подразделах раздела 6, относятся к целевому применению;

e) определять рекомендуемые (если сказано «следует») критерии, приведенные в подразделах раздела 7, которые необходимо применять, и обосновывать отказ от этих критериев и необходимость принятия компенсирующих мер, допускаемых в разделе 7;

f) определять критерии выбора и их относительную значимость, которая может повлиять на выбор потенциально применимых устройств, например:

- необходимый срок службы устройства при целевом применении;
- объем оказываемой поставщиком поддержки, которая может потребоваться, и на какой период;
- степень необходимости модификации целевой системы, в которую может быть интегрировано устройство, чтобы использовать устройство с учетом его функций и режимов отказа и т. д.;

g) устанавливать перечень требований для EAR.

5.3.3 Отчет об оценке и применении (EAR)

Настоящий пункт устанавливает рамки и содержание EAR.

В EAR необходимо:

a) задокументировать результаты проведенной оценки;

b) задокументировать причины, по которым обосновано применение настоящего стандарта, исходя из критериев применимости, приведенных в 5.2.2;

c) указать область и применимость работ по оценке и следующие данные об этой работе:

- конкретное целевое применение (функция безопасности) и класс системы;
- более высокий класс, по которому оценено устройство, если таковое имело место;
- характеристику потенциально применимого устройства, вошедшего в EAR, включая точную идентификацию устройства, содержащую название изделия, номер версии программного обеспечения, а также компонентов аппаратных средств, конфигурации и любых других компонентов или опций, имеющих отношение к оценке;

d) изложить или привести ссылки на основные функциональные требования и требования к рабочим характеристикам (включая те, которые пришлось изменить), повлиявшие на оценку приемлемости устройства, класс в соответствии с целевым назначением, режим(ы) безопасного(ых) отказа(ов) и критерии внешних условий эксплуатации.

Примечание — Если имели место любые отклонения от требований, эти отклонения и их обоснование также должны быть четко задокументированы в EAR, чтобы потенциальный пользователь устройства мог обосновать его применение или выбрать альтернативное устройство;

e) задокументировать пределы надежности, достигаемые устройством самостоятельно или в дублируемой конфигурации;

f) указать критерии отбора, установленные в EAP;

g) внести все документы, использованные для верификации каждого этапа разработки устройства, включая стратегию верификации и проведенные испытания, или, как вариант, включить ссылки на эти документы при условии, что ссылочные документы доступны стороннему эксперту;

h) указать, как в соответствии с 5.3.4 применены критерии, приведенные в подразделах разделов 6—9, и обосновать распределение этих критериев по значимости или их исключение;

i) указать компенсирующие меры, требуемые для рассматриваемого целевого применения, чтобы учесть ситуации, когда образец устройства отвечает не всем требованиям соответствия, или первоначальное свидетельство о соответствии признают недостаточным.

Возможные компенсирующие меры могут включать дополнительные испытания, доработку документации, дополнительные контрольные испытания на этапе эксплуатации, строгие ограничения на использование устройства (например, использование только в системах с определенными функциональными свойствами), отключение определенных опций или модификации целевой системы либо ограниченные модификации самого устройства, как указано в разделе 8;

j) определить все модификации, описанные в 8.3 и 8.4, которые могут понадобиться устройству или целевой системе для интеграции потенциально применимого устройства в целевую(ые) систему(ы) и сохранения приемлемости в соответствии с предыдущими пунктами. Любые такие модификации устройства необходимо ограничить по объему; они не должны касаться программного обеспечения или конструктивного решения HDL-программируемых устройств, чтобы устройство сохраняло свою изначальную функцию. В противном случае устройство перестанет быть стандартным промышленным устройством, подпадающим под действие настоящего стандарта.

Примечание — Примерами такой модификации может служить замена резистора согласования импедансов, изменения крепежного кронштейна или замена подключающего элемента в переключателе или потенциометре;

k) указать все ограничения на использование устройства в каждом виде применения и класс системы, для применения в которой устройство приемлемо;

l) установить меры (и их достаточность), рекомендуемые для доказательства того, что при применении устройства соблюдаются все ограничения и рекомендации, приведенные в EAR;

m) представить окончательное заключение о приемлемости потенциально применимого устройства (устройств) для каждого вида целевого применения в следующих выражениях:

- устройство применимо как есть; или
- устройство применимо при соблюдении указанных условий; или
- устройство неприменимо.

5.3.4 Применение положений настоящего стандарта

Настоящий пункт устанавливает, как применять требования, указанные в разделах 6—9, при оценке цифровых устройств узкоспециализированной функциональности, определяемой в 3.7, с точки зрения возможности их использования в рамках заданного вида применения.

a) Необходимо обосновать применимость настоящего стандарта, исходя из критериев применимости, приведенных в 5.2.2.

b) Оценку потенциально применимого устройства следует выполнять на основе предполагаемой функции и ее категории или предполагаемого применения и его класса.

c) Необходимо документально зафиксировать подтверждение функциональной и эксплуатационной пригодности устройства, как указано в разделе 6, основываясь на всех применимых критериях указанного раздела.

d) Необходимо документально зафиксировать подтверждение корректности на основе комбинированной качественной оценки всех применимых критериев, указанных в разделе 7, согласно EAP.

e) В ходе оценки необходимо установить все ограничения, необходимые для использования устройства только в рамках, документально засвидетельствованных согласно разделу 7.

f) В ходе оценки необходимо установить все ограничения, необходимые для безопасного использования устройства в рамках целевого применения (см. раздел 8).

g) Необходимо продемонстрировать свидетельства того, что результаты оценки могут быть действительными на протяжении достаточного периода времени, учитывая срок службы AC и соответствующие планы по замене оборудования, опираясь при этом на все применимые критерии, указанные в разделе 9.

6 Критерии функциональной и эксплуатационной пригодности

6.1 Общие положения

Критерии функциональной и эксплуатационной пригодности учитывают следующие вопросы:

- выполняет ли потенциально применимое[1)] устройство требуемые функции;
- выполняет ли устройство только требуемые функции (или, как вариант, устройство обладает также нетребуемой функциональностью, которая, как показано, не препятствует выполнению требуемых функций);
- выполняет ли устройство свои функции с приемлемым уровнем надежности и определенными приемлемыми режимами отказа;
- зафиксирована ли эта функциональность документально надлежащим образом.

Соответствие каждому применимому критерию должно быть подтверждено надлежащим образом путем анализа и/или испытаний и проверкой технических характеристик сопрягаемых устройств. Эти мероприятия необходимо задокументировать.

[1)] Как правило, потенциально применимые устройства оценивают на основе предполагаемого соответствия функциональным требованиям к рассматриваемому применению. В этом разделе даны рекомендации по поводу того, как проверяют, все ли соответствующие критерии были учтены при оценке потенциально применимого устройства.

6.2 Функциональная состоятельность основной функции

Основная функция или функции потенциально применимого устройства должны отвечать функциональному(ым) требованию(ям), вытекающему(им) из требований к АС и системе. Если устройство предназначено для целевого применения, то:

a) устройство должно быть способно работать в пределах всего используемого на АС диапазона технологических сигналов и во всей рабочей области, определенной для предполагаемого применения;

b) устройство должно обеспечивать требуемую точность и повторяемость параметров в пределах всего указанного диапазона;

c) устройство должно демонстрировать требуемую скорость отклика и приемлемый уровень обработки цифровых сигналов (установленный исходя из соответствующих критериев, например, частоты выборки, времени запаздывания, времени нарастания сигнала, полосы пропускания, характеристик фильтра, таких как частота излома, шумоподавление и т. д.);

d) если речь идет о функции преобразования частотного диапазона (например, для применения в системах с обратной связью), устройство должно демонстрировать надлежащий уровень усиления и сдвига фазы в пределах всего рассматриваемого диапазона частот;

e) необходимо четко определить режимы отказа, и в этих режимах значения выходных сигналов должны соответствовать значениям при заданных выходных состояниях (например, при обрыве цепи — увеличение или уменьшение выходного сигнала, либо статичное состояние «как есть»), которые либо заведомо безопасны для целевого применения, либо их можно обнаружить и преобразовать в состояние, безопасное для применения, а если их нельзя ни обнаружить, ни преобразовать в состояние, безопасное для применения, то эти состояния должны быть в достаточной степени маловероятны;

f) для выполнения условий вышеприведенного пункта e) необходимо проанализировать режимы отказа с точки зрения влияния потенциально применимого устройства на систему, в которой оно будет установлено, учитывая при этом все факторы, которые могут повлиять на режимы отказа (см. также 6.7). Особое внимание следует уделять отказам по общей причине, особенно имеющим отношение к другим устройствам (возможно, других классов), которые в анализе безопасности играют роль защиты от такого развития событий.

6.3 Вспомогательные функции

К вспомогательным функциям потенциально применимого устройства относятся функции, не являющиеся частью его основной функции, но необходимые для настройки параметров основной функции, чтобы устройство могло выполнять требующуюся от него функцию безопасности, или функции, повышающие надежность устройства, например функция самоконтроля.

a) Для видов применения классов 1 и 2 необходимо продемонстрировать посредством анализа (и/или испытаний, если можно получить достоверные результаты), что ни действие, ни режим отказа вспомогательных функций не могут препятствовать выполнению основных функций, за исключением специально оговоренных случаев (например, путем внесения вручную изменений уставок), или не могут перевести устройство в состояние, небезопасное в рамках заданного применения.

Примечание — Режим отказа, который считается безопасным, зависит от применения и не всегда заключается в срабатывании контакта аварийной остановки или разрыве цепи при неисправности. Некоторые примеры отказов приведены в 7.2.

b) Вспомогательные функции, связанные с настройкой параметров основных функций, должны отвечать требованиям, приведенным в 6.4.

c) Для видов применения класса 3, для которых два или более устройств признаны эквивалентными во всех прочих отношениях, необходимо выбрать устройство, в наименьшей степени подверженное негативному влиянию отказов вспомогательной функции. Число, вероятность и серьезность постулированных отказов вспомогательной функции являются факторами для сравнения.

d) Если для связи с потенциально применимым устройством используют внешнее устройство более низкого класса, то ни работа, ни отказ внешнего устройства не должны непредусмотренным образом препятствовать выполнению основной функции потенциально применимого устройства.

Примечание — Данное требование основано на требовании к обеспечению связи, установленном МЭК 61513, согласно которому не допускается непредусмотренная зависимость системы более высокого класса от системы более низкого класса. Таким образом, связь между устройствами разных классов, как правило, является односторонней (например, связь с системой контроля, которая не отражается на классе системы) или дей-

ствующей временно. Кроме того, систему более высокого класса обычно подвергают испытаниям после короткого периода двусторонней связи, а управление двусторонней связью выстраивают таким образом, чтобы в одно время был подключен только один канал системы более высокого уровня.

6.4 Возможность изменения конфигурации

Функции потенциально применимого устройства, поддающиеся конфигурированию, и вспомогательные функции, обеспечивающие возможность конфигурирования, должны вместе соответствовать следующим требованиям:

a) Параметры конфигурации основных функций необходимо ограничить в части возможности включения/отключения (активации/деактивации) настроек или масштабирующих настроек, таких как калибровка технологического диапазона и выходного сигнала, настройки усиления или затухания и т. д.

b) При применении устройств в системах классов 1 и 2 защита конфигурации должна включать заранее продуманные при проектировании меры, чтобы понадобилось более одного неверного действия, прежде чем случится ошибка в установке параметра конфигурации.

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

c) Параметры конфигурации основных функций должны быть защищены от случайного, злонамеренного или несанкционированного изменения в соответствии с общим планом обеспечения безопасности ядерной установки (см. МЭК 61513, 5.4.2). Такая защита должна включать защиту паролем, если ее поддерживает потенциально применимое устройство.

Незащищенным допускается только доступ для чтения параметров конфигурации, при условии соблюдения требований, что этому доступу нет препятствий со стороны вспомогательной функции, как указано в нижеупомянутом пункте d).

Для систем класса 1 ограничения физического доступа включают такие ограничения, как запирающиеся шкафы или аппаратные залы. (Данное требование применимо к процессу монтажа, а не к потенциально применимому устройству, и за его соблюдение отвечает конечный пользователь.)

d) При необходимости конфигурирования вспомогательных или избыточных функций таким образом, чтобы они не мешали работе основных функций, параметры конфигурации должны быть защищены, как указано в пунктах b) и c).

e) Необходимо обеспечить возможность проверки устройства после того, как были изменены его параметры конфигурации, чтобы убедиться в корректности внесенных изменений.

f) Если устройство предоставляет операторам визуальный доступ к параметрам конфигурации или доступ с возможностью изменения параметров, то этот доступ должен быть обеспечен только к тем параметрам конфигурации, которые необходимы операторам для выполнения своих служебных обязанностей.

g) Если устройство предоставляет операторам доступ к параметрам конфигурации с возможностью их изменений, то все входные данные от оператора должны подвергаться проверке в отношении применяемых диапазонов и достоверности и/или ограничениям значений, соответствующих применению.

h) Если требуется, чтобы параметры конфигурации и любые обязательные сопутствующие логические состояния автоматически восстанавливались после частичного или полного сбоя электропитания, и это свойство поддается конфигурированию, то параметры конфигурации должны быть защищены, как указано в пунктах b) и c).

Составные части фильтров или ПИД-контроллеры являются типичными причинами всплеска выходного сигнала при возобновлении работы после переходных энергетических режимов.

i) Если устройство должно работать в канализированной системе, необходимо предусмотреть, чтобы единовременно только один канал резервной системы мог быть подвергнут изменениям конфигурации.

Примечание — Данное требование типично для систем классов 1 и 2.

6.5 Избыточные функции

К избыточным функциям потенциально применимого устройства относятся те функции, которые не входят ни в состав обязательной функции безопасности устройства, ни в состав его необходимых

вспомогательных функций. Несмотря на то, что избыточные функции часто являются неотъемлемыми характеристиками устройства, их присутствие предполагает возможную излишнюю сложность и дополнительные потенциальные режимы отказа, нежелательные для видов применения более высоких классов.

a) Для видов применения классов 1 и 2 необходимо продемонстрировать путем анализа (и/или экспериментально, если есть уверенность в достоверности результатов), что ни один из режимов отказа избыточных функций не может препятствовать выполнению основной функции.

b) Для видов применения классов 1 и 2 необходимо продемонстрировать путем анализа (и/или экспериментально, если есть уверенность в достоверности результатов), что при всех эксплуатационных условиях избыточные функции могут быть конфигурированы (или изначально функционировать) так, чтобы они не могли препятствовать выполнению основной функции.

c) Для видов применения класса 3 там, где два или более устройств определены как эквивалентные во всех прочих отношениях, следует выбирать устройство, на работу которого в наименьшей степени влияют любые избыточные функции или их отказы. Число, вероятность и серьезность постулированных отказов избыточной функции являются факторами для сравнения.

d) Для видов применения классов 1 и 2, если нельзя показать отсутствие вмешательства избыточной функции в работу основной функции согласно пунктам b) и c), избыточная функция должна отвечать всем требованиям к проектированию системы обеспечения безопасности в той же степени, что и основная(ые) функция(и).

e) Для видов применения классов 1 и 2 необходимо продемонстрировать путем анализа (и/или экспериментально, если есть уверенность в достоверности результатов), что при всех эксплуатационных условиях ни работа, ни отказ внешнего устройства, взаимодействующего с потенциально применимым устройством, не смогут непредусмотренным образом влиять на основную функцию потенциально применимого устройства. Если это невозможно продемонстрировать, то следует обеспечить проведение испытаний основной функции потенциально применимого устройства после осуществления его коммуникации с внешним устройством.

Примечание — См. примечание после 6.3 d).

f) Предпочтительно исключать избыточные функции вместо того, чтобы сокращать число вспомогательных функций.

Примечание — Требования, изложенные в 8.3, применяют к модификациям устройства.

6.6 Эксплуатационная надежность аппаратных средств

Эксплуатационную надежность аппаратных средств оценивают в ходе функциональной квалификации и квалификации на внешние воздействия (называемых также квалификацией аппаратных средств). Такая оценка необходима для гарантии того, что потенциально применимое устройство будет выполнять свои функции в любых условиях окружающей среды, в которых оно должно функционировать (как при нормальной эксплуатации АЭС, так и во время аварии и после нее).

МЭК 61513 рассматривает эксплуатационную надежность аппаратных средств в 6.4.2.1, а также приводит ссылки на МЭК 60780 и МЭК 60980, в которых, в свою очередь, даны ссылки на другие стандарты в соответствующих случаях. МЭК 61513 допускает проведение квалификации устройств, используемых в классе применения 3, в промышленных условиях, но требует при этом документального подтверждения заявленных требований на эксплуатацию в аномальных условиях окружающей среды. Одним из способов соблюдения этого требования является применение МЭК 60780.

Примечание — В МЭК 61513 также дана ссылка на МЭК 60987, устанавливающий требования к заказным компьютерным системам для видов применения классов 1 и 2.

a) Эксплуатационную надежность потенциально применимого устройства следует оценивать по воздействию всех условий окружающей среды (температуры, давления, влажности, излучения, ЭМП) и продолжительности этих условий, под влиянием которых устройство может находиться при выполнении им предназначенной функции (сюда могут входить аварийные условия внутри защитной оболочки).

b) Для проведения квалификации потенциально применимого устройства необходимо оценить его эксплуатационную надежность в соответствии с требованиями указанных ниже стандартов. Если соответствие стандарту документально не оформлено, необходимо провести анализ, подтверждающий соответствие, или указать компенсирующие меры, руководствуясь следующим:

- воздействие температуры и влажности в соответствии с МЭК 60780 для применения классов 1 и 2 и в соответствии с МЭК 61513 для применения класса 3;
- воздействие излучения;
- воздействие вибрации и сейсмических условий в соответствии с МЭК 60980;
- невосприимчивость к электромагнитным помехам в соответствии со стандартами серии МЭК 61000.

Примечание — МЭК 62003 рассматривает электромагнитные помехи и распространяется на системы, важные для безопасности АС, а также содержит ссылки на многие части МЭК 61000-4. МЭК 61000-6-2 является обычным промышленным стандартом;

- воздействие пыли и взвешенных в воздухе частиц.

c) При проведении квалификации потенциально применимого устройства необходимо также учитывать его влияние на другие устройства в системе, где оно будет установлено. При этом может потребоваться внесение изменений в устройство или проведение оценки других устройств в соответствии с пунктом a), приведенным выше, с учетом нахождения в их рабочей зоне потенциально применимого устройства. Необходимо учитывать следующее:

- вибрацию, вызываемую потенциально применимым устройством;
- тепло, выделяемое потенциально применимым устройством;
- электромагнитные помехи, вызываемые потенциально применимым устройством;
- влияние на сейсмическую квалификацию конструкции, на которую эти устройства будут установлены.

6.7 Надежность, ремонтопригодность и тестируемость

Надежность, ремонтопригодность и тестируемость являются взаимосвязанными свойствами устройства, так как частота проведения испытаний в значительной мере определяется частотой случайных отказов, присущих рассматриваемому устройству или системе, и требуемой вероятностью отказов по запросу. Ремонтопригодность имеет значение для сокращения времени ремонта и позволяет избежать ошибок в ходе технического обслуживания, которые могут привести к отказам.

Требования к выполнению периодических испытаний и самодиагностики (самоконтроля) установлены МЭК 60671. Настоящий подраздел делает акцент на значении тестируемости и ремонтопригодности для выбора, оценки и определения сценария применения потенциально применимого устройства.

АВПО и его расширенные версии, такие как АВПДО и АВПКО, являются широко распространенными методами систематического анализа устройства, используемыми для определения режимов отказов его аппаратной части, частоты отказов и оказываемого ими влияния. К другим используемым методам относится АДО.

Потенциально применимое устройство должно быть оценено и по результатам этой оценки должен быть составлен документ, касающийся перечисленных ниже критериев.

a) Должен быть выполнен анализ для определения (или подтверждения) режимов отказа устройства и для установления их безопасности или опасности в контексте предполагаемого применения.

Режимы отказа интерпретируют исходя из назначения устройства и его влияния на безопасность АС. При этом может потребоваться проанализировать отличающиеся режимы, такие как отказ под напряжением и при отключении питания, отказ при нарастании, снижении или стабильности значений, или немедленное оповещение об отказе, чтобы оперативный персонал мог оценить его влияние на безопасность АС.

b) Для предполагаемых видов применения классов 1 и 2 анализ должен показать, что достаточная доля режимов отказа аппаратных средств четко определена, может быть обнаружена и что оповещение об отказах обеспечено.

c) Для предполагаемых видов применения классов 1 и 2 анализ должен показать, что отказы, которые могут быть опасны для данного вида применения, имеют приемлемо низкую вероятность возникновения при этом применении.

d) Для таких видов применения, которые требуют численного ограничения частоты отказов, необходимо использовать количественный анализ для определения частоты отказов. Анализ должен показать, что приемлемая доля видов отказов аппаратных средств, которые могут быть опасны для данного применения, обнаружима и обеспечена оповещением или может быть в установленное время преобразована в безопасные отказы, а также является маловероятной, что позволяет соблюсти требования для данного вида применения.

Примечание 1 — Примерами количественных методов анализа могут служить АДО и АВПДО. См. также 5.3 в МЭК 60987.

Примечание 2 — Руководство по указанным методам приведено в таких стандартах, как, например, серия стандартов МЭК 61508.

Примечание 3 — Важность обнаружения отказа за установленное время заключается в том, что это позволяет выполнить корректирующее действие вручную и произвести замену устройства на исправное в течение достаточно короткой задержки, соответствующей целевому показателю доступности функций безопасности.

e) Проектные решения, касающиеся самоконтроля и периодических контрольных испытаний устройства, не должны создавать риски возникновения непреднамеренного препятствия защите основной функции устройства от негативного влияния вспомогательных или избыточных функций, или риски ненадлежащего изменения параметров конфигурации.

f) Если устройство обладает возможностью самоконтроля, то при обнаружении отказа оно должно подавать аварийный сигнал, оповещать о его возникновении или реагировать путем перевода выходных сигналов в состояние, безопасное в контексте назначенного применения.

g) Периодические испытания, направленные на демонстрацию продолжающейся готовности устройства к работе, должны быть запланированы таким образом, чтобы максимально повысить возможность обнаружения отказов, не выявляемых при самоконтроле.

h) При выполнении оценки следует продумывать условия испытаний потенциально применимого устройства, особенно, если необходимы комплексные испытания, учитывая следующие критерии:

- процедуры и периодичность технического обслуживания и контрольных испытаний;
- сложность и частота проведения необходимых испытаний;
- целесообразность проведения испытаний на оборудовании под напряжением;
- оценка программных инструментов, необходимых для проведения испытаний.

i) Необходимо определить компоненты с ограниченным сроком службы (например, алюминиевые или электролитические конденсаторы) для обоснования замены компонента или устройства прежде, чем ожидаемая частота отказов устройства предоставит доказательство окончания их срока службы.

Примечание — На компоненты в большей или меньшей степени влияют различные условия (температура, излучение, вибрация и т. д.), в результате чего набор компонентов с ограниченным сроком службы может быть разным в зависимости от конкретного применения.

6.8 Информационная безопасность

Потенциально применимое устройство и его конфигурацию, техническое обслуживание или инструментальные средства испытаний необходимо включить в оценку информационной безопасности системы, в которую интегрировано устройство.

Примечание 1 — Требования к программам информационной безопасности установлены в МЭК 62645.

Примечание 2 — МЭК 61513 устанавливает требования к обеспечению информационной безопасности на уровне архитектуры контроля и управления, а также на уровне отдельной СКУ.

Примечание 3 — В МЭК 60880 установлены требования к обеспечению информационной безопасности программного обеспечения для видов применения класса 1, а в МЭК 62138 — для видов применения классов 2 и 3.

6.9 Пользовательская документация по безопасности

Потенциально применимое устройство должно сопровождаться проектной документацией и документацией по верификации (см. 7.4.6), а также инструкциями по его безопасному использованию. Безопасное использование устройства означает соблюдение требований безопасности, предусмотренных для предполагаемого применения, при условии, что установка, конфигурация и обслуживание устройства будут проводиться в соответствии с документацией, предоставленной его поставщиком.

a) Пользовательская документация по безопасности состоит из следующих документов:

- руководство по технике безопасности — документ или перечень документов, в которых приведены все требования к безопасному обращению с устройством и его безопасному применению, включая точную идентификацию устройства и идентификатор его версии;
- инструкция по установке — документ, определяющий, как следует устанавливать устройство и подключать к другим устройствам, чтобы обеспечить его функционирование в соответствии с функциональной спецификацией;

- руководство пользователя или руководство по эксплуатации — документ, определяющий взаимодействие пользователя на рабочем месте с устройством (например, как оператор АС должен считывать отображаемые данные и изменять параметры, которые ему разрешается менять);
- руководство по техническому обслуживанию — документ, в котором рассмотрены все аспекты обслуживания устройства на рабочем месте: меры безопасности для персонала, меры безопасности для системы, испытания устройства на месте, вывод устройства из эксплуатации и возврат в рабочее состояние.

Примечание — Точные требования к документации, например конкретное название или область применения каждого документа, зависят от конкретной эксплуатирующей организации.

Настоящий стандарт не устанавливает требований к конкретному названию или области применения каждого документа, но требует, чтобы весь предметный материал был отражен в комплекте документов.

b) Для корректного и безопасного использования устройства документы, указанные выше, в пункте a), должны содержать следующую информацию:
- полные сведения о версии;
- полную информацию, касающуюся основной функции, а именно: общая функциональность системного блока, включая конкретные последствия использованных параметров конфигурации, интерфейсы устройства, поведение при включении питания и при прерывании питания, последствия отказа, отклик во временном и частотном диапазонах (если применимо), скорость исполнения команд, входные и выходные сопротивления и диапазоны и др.;
- полный комплект документов, касающийся основной функции с точки зрения режимов отказа и индикации отказов;
- полный комплект документов по функциональности, относящейся к вспомогательным и избыточным функциям, включая, если применимо, информацию о способах конфигурации, позволяющих предотвратить их влияние на основную функцию;
- требования к функциональной целостности, такие как самоконтроль для выявления отказов аппаратных средств и действия при обнаружении отказа (в отличие от функциональных требований);
- ограничения внешних условий и эксплуатационной надежности устройства, а также компоненты, ограничивающие срок службы;
- все процедуры технического обслуживания и соответствующие меры предосторожности;
- все процедуры эксплуатации и соответствующие меры предосторожности;
- все требования и процедуры периодических контрольных испытаний и соответствующие меры предосторожности;
- любая иная информация, важная для безопасного использования устройства, и соответствующие меры предосторожности.

7 Критерии функциональной надежности и доказательства корректности

7.1 Общие положения

Настоящий подраздел предоставляет рекомендации в отношении:
- сбора и оценки доказательств того, что потенциально применимое устройство пригодно к использованию в системах, важных для безопасности АС, на основании процессов, используемых при его проектировании и изготовлении;
- способов компенсации любых недостатков таких доказательств корректности.

Примечание — Оценка сведений, подтверждающих корректность устройства, как правило, является качественной, поскольку общепризнанные количественные характеристики отсутствуют и не всегда есть возможность получить все виды доказательств, указанные в настоящем разделе. Подтверждение корректности основано на сбалансированной оценке элементов изделия и процесса, документально зафиксированных в ходе проектирования и изготовления, с учетом того, что некоторые элементы доказательств корректности индивидуально или совместно друг с другом могут компенсировать отдельные недостатки других доказательств, как описано в соответствующих подразделах.

Доказательство корректности устройства осуществляют путем:

- оценки процессов разработки изделия и реализации его проекта (в том числе верификации и валидации как текущего конструктивного исполнения, так и его модификаций);
- оценки документации по разработке устройства;
- оценки процессов изготовления изделия;
- оценки параметров самого изделия.

Доказательства корректности, относящиеся к процессам проектирования и изготовления, рассмотрены отдельно, поскольку способы компенсации недостатков доказательств корректности для проектирования и производства также отличаются.

Кроме того, определенные компенсирующие меры нельзя применять во всех случаях одинаково: конкретные компенсирующие меры применимы только к конкретным недостаткам основных элементов доказательства корректности устройства.

Основные элементы доказательства корректности проектирования устройства включают:

- свидетельство упорядоченного жизненного цикла разработки и сопровождения процесса проектирования;
- свидетельство наличия инструментов, используемых для поддержания упорядоченного жизненного цикла (например, контроль изменений, управление конфигурацией);
- свидетельство соответствующей независимости от возможных систематических отказов;
- анализ документации по разработке проекта, в том числе по верификации и валидации;
- анализ документации по конструкции и использованию устройства.

Примечание — Если выполнена общая предварительная оценка или аттестация потенциально применимого устройства, она может служить полезным источником сведений, подтверждающих корректность устройства, или содержать полезные результаты анализа.

Способы, которые можно использовать для компенсации некоторых недостатков основных элементов доказательства корректности конструкции устройства, включают:

- пригодный и заслуживающий доверия опыт эксплуатации, который можно использовать там, где это оправдано, для компенсации недостатков других элементов доказательств;
- свидетельство стабильности (малая частота изменений) изделия на протяжении значительного времени изготовления и использования изделия;
- проведение дополнительных конкретных испытаний устройства для восполнения пробелов в существующей документации по испытаниям или для расширения области распространения результатов испытаний в соответствии с предполагаемым применением и для получения других элементов доказательства корректности,
- компенсационные меры, принимаемые на системном уровне для снижения количества отказов устройства или преобразования их в безопасные отказы;
- доработку документации, изначально предоставленной проектировщиком.

Основные элементы доказательства корректности изготовления устройства включают:

- свидетельство упорядоченного жизненного цикла разработки и сопровождения процесса изготовления изделия, включая контроль изменений и управление конфигурацией;
- анализ документации по изготовлению и применению устройства.

Способы, которые могут быть использованы для компенсации недостатка элементов доказательства корректности изготовления, включают:

- свидетельство стабильности (малая частота изменений) изделия на протяжении значительного времени изготовления и использования изделия;
- конкретные проверки устройства, функциональные испытания и испытания на старение, пригодные для компенсации недостатка элементов доказательства корректности изготовления устройства;
- закупку достаточного количества устройств из одной производственной партии, чтобы обеспечить необходимый объем запчастей на весь срок службы АС.

EAP (см. 5.3) устанавливает и обосновывает распределение требований нижеприведенных подразделов в соответствии с их значимостью, а также — какие из допустимых компенсирующих мер будут рассмотрены.

В некоторых нижеприведенных подразделах использованы таблицы, помогающие наиболее четко определить требования к трем классам применения и допустимые компенсирующие меры. В этих таблицах применены следующие условные обозначения:

а) «О» указывает на обязательный характер критерия, что соответствует использованию слов «должен/необходимо» в изложении требования;

b) «Р» указывает на рекомендуемый характер требования, что соответствует использованию слова «следует» в изложении требования;

c) в столбцах с обозначением «КМ» должны быть указаны доступные компенсирующие меры, где:

- «СИ» обозначает, что можно использовать стабильность изделия в соответствии с 7.6, чтобы в некоторой степени компенсировать недостаток основного доказательства корректности;
- «ОЭ» обозначает, что можно использовать опыт эксплуатации в соответствии с 7.7, чтобы в некоторой степени компенсировать недостаток основного доказательства корректности;
- «ДТ» обозначает, что можно использовать дополнительное тестирование и/или анализ в соответствии с 7.8, чтобы в некоторой степени компенсировать недостаток основного доказательства корректности;
- «ПД» обозначает, что можно использовать поправки к документации в соответствии с 7.9, чтобы в некоторой степени компенсировать недостаток основного доказательства корректности.

Показанная возможность применения компенсирующих мер не подразумевает пренебрежения основными формами доказательств корректности, наоборот, указанную в таблицах возможность применения компенсирующих мер необходимо использовать нечасто.

Примечания

1 Необходимость частого применения компенсирующих мер указывает на отсутствие четко определенного процесса разработки или соблюдения заявленного процесса, а это может исключить возможность принятия потенциально применимого устройства.

2 Так, например, наличие обозначения «О» в колонке «Класс 3» и обозначения «ДТ» в колонке «КМ» для класса 3 означает, что критерий обязателен для класса 3, но некоторые недостатки в соблюдении проектировщиком или производителем требований данного подраздела можно компенсировать путем добавления документов, разработанных в ходе дополнительных испытаний и/или анализа в соответствии с 7.8.

7.2 Предварительная аттестация

В большинстве случаев значительным преимуществом при выборе обладает устройство, которое было ранее аттестовано на соответствие применимому стандарту безопасности. Для таких устройств, как правило, четко определены режимы отказа, они разработаны в соответствии с упорядоченным процессом разработки программного обеспечения и/или HPD, и потому, скорее всего, на такие устройства уже существует сопроводительная документация, хотя она может быть защищена правом собственности.

Примечание — Применимым стандартом безопасности является МЭК 61508.

Зачастую ситуация совсем иная для неаттестованных изделий, потому что их, как правило, разрабатывают с целью быстрого вывода на рынок и подвергают частым изменениям для добавления новых функций. Таким образом, неаттестованные изделия могут обладать функциональными возможностями, которые не требуются для предполагаемого применения в области ядерной энергетики. Более того, изделия могут обладать функциональными возможностями, которые не только не требуются, но и не определены явно (то есть функциональность скрыта) в спецификации изделия. Напротив, устройства, разработанные в соответствии со стандартами безопасности, как правило, обладают конкретной, четко определенной функциональностью.

Второе преимущество аттестации изделий на соответствие стандарту безопасности по сравнению с неаттестованными изделиями состоит в большей уверенности, что при выборе изделия будут доступны необходимые доказательства корректности, так как установление соответствия таким стандартам требует последующего составления документации, аналогичной той, что разрабатывают при установлении соответствия стандартам по ядерной безопасности.

Примечание — Стандартами по ядерной безопасности, содержащими такой вид требований к документации, являются МЭК 62138 и МЭК 60880.

Тем не менее необходимо проявлять осторожность при оценке как ранее аттестованных, так и неаттестованных устройств на предмет режимов отказа. Даже при том, что режимы отказа устройств, аттестованных по неядерному стандарту безопасности, могут быть четко определены, они обычно подразумевают прекращение технологического процесса, например аварийный останов реактора, тогда как в разных случаях ядерного применения может быть востребовано сохранение работоспособности в случае отказа, а не аварийный останов при отказе. Примерами могут служить контроллеры дизельного генератора и компрессора, от которых требуется продолжение исправного функционирования после

возникновения аварии. В таких случаях контроллер устройства должен просто сигнализировать о возникших условиях, например о высокой вибрации, при которой в случае неядерного применения требовалось бы выключение устройства.

В общем можно заключить, что оценка промышленного устройства облегчается и упрощается, если оно аттестовано по неядерному стандарту безопасности, но по сути этого недостаточно и необходимо учитывать определенные условия при применении аттестации.

Аттестация на соответствие неядерному стандарту безопасности может быть использована как подтверждение соблюдения критериев, указанных в разделе 7, и при этом аттестация должна отвечать следующим критериям:

a) если аттестация, используемая для подтверждения соответствия подразделу настоящего стандарта, выполнена по стандарту, который не является общепризнанным, то такое использование необходимо обосновать;

b) если аттестацию используют для подтверждения соответствия подразделу настоящего стандарта, то в ходе аттестации необходимо предоставить доказательство корректности, непосредственно относящееся к этому подразделу;

c) материал, на котором основано подтверждающее доказательство, предоставленное в ходе аттестации, должен быть доступен для ознакомления. Доказательство должно включать все элементы, необходимые для независимой оценки области и границ аттестации, в частности:

- оцениваемая документация;
- предположения об использовании устройства и его ожидаемом поведении во всех случаях использования;
- методы и инструменты аттестации;
- оцениваемые свойства устройства и результаты оценки (положительный результат оценки или нет);

d) аттестация должна быть проведена на современном уровне и применена к устройству следующим образом:

- для предполагаемых видов применения классов 1 и 2, где отказ потенциально применимого устройства вызвал бы отказ целевой системы (например, если бы оно было установлено во всех каналах системы с резервированием), должна быть проведена аттестация конкретной версии устройства, которая должна быть установлена;
- для предполагаемых видов применения классов 1 и 2, где отказ потенциально применимого устройства не вызвал бы отказа целевой системы, должна быть проведена аттестация версии, которая может отличаться от предназначенной для использования версии лишь незначительно, и эти малозначимые отличия четко задокументированы и утверждены и не оказывают влияния на основную функцию;
- для предполагаемых видов применения класса 3 проводят аттестацию версии, которая может иметь только такие отличия от предназначенной для использования версии, которые документально зафиксированы и утверждены;
- в случаях, когда предназначенная для использования версия устройства неидентична аттестованной(ым) версии(ям), вывод о том, что различия незначительны, необходимо обосновать путем надлежащего и контролируемого анализа. Различия, которые сказываются на основных проектных решениях, используемых в устройстве, например применяемый физический принцип, используемая технология и средства предотвращения систематических отказов, не являются незначительными. Различия в настройках параметров, которые относятся к диапазонам сигналов, вероятнее всего, являются незначительными;

e) условия использования, принятые при аттестации, должны соответствовать предполагаемым условиям использования в ядерной энергетике (см. также 7.7);

f) необходимо определить уполномоченную аттестующую организацию, независимую от проектировщика и производителя устройства;

g) аттестующая организация должна иметь достаточный уровень компетенции в части оцениваемых свойств и/или измерений, мнение о которой составлено на основе всей доступной информации о ее опыте и квалификации.

7.3 Предотвращение систематических отказов

Указанные в данном подразделе критерии используют, как правило, для предполагаемых видов применения классов 1 и 2, но они также могут быть рекомендованы для класса 3. Для устройств с программным обеспечением и HPD гарантия предотвращения систематических отказов может быть получена, главным образом, путем проведения анализа. В то же время условия окружающей среды также могут приводить к систематическим отказам, но для квалификации по этому признаку можно использовать анализ или испытания согласно МЭК 60780, как описано в 6.6.

Необходимо документальное подтверждение того, что возможные причины систематических отказов устройства отсутствуют. В данном подразделе оценка функциональной надежности устройств (отсутствия причин систематических отказов) представлена в виде таблиц, в которых приведены критерии оценки или необходимая для оценки информация для каждого класса, а также требования к применению критериев или информации (обязательные или рекомендуемые) и меры, компенсирующие недостаток информации. В этих таблицах символ «О» означает «обязательный», что соответствует слову «должен» в изложении требования, а символ «Р» означает «рекомендуемый», что соответствует слову «следует».

Функциональную надежность подтверждают путем оценки общей архитектуры устройства, чтобы гарантировать соблюдение приведенных ниже требований.

a) Должна быть выполнена оценка конструкции цифрового контроллера устройства (цифровой части устройства). В таблице 1 приведена необходимая информация, которая должна быть доступна при оценке для видов применения каждого класса.

Таблица 1

Необходимая доступная информация	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
1 Общее функционирование цифрового контроллера устройства в штатных и нештатных условиях (в том числе в аварийных условиях)	О	ПД	О	ПД	О	ПД
2 Общая архитектура цифрового контроллера устройства, определяющая и устанавливающая роли компонентов главного цифрового аппаратного обеспечения (в том числе программируемых интегральных схем) и программного обеспечения	О	ПД	О	ПД	Р	ПД
3 Все документы, необходимые для верификации соответствия требованиям раздела 6, в том числе содержащие стратегию верификации и информацию о проведенных испытаниях или анализе	О	ДТ	О	ДТ	О	ДТ
4 Все документы, необходимые для того, чтобы показать, что выполнена верификация каждого этапа разработки устройства, в том числе содержащие стратегию верификации и информацию о проведенных испытаниях или анализе	О	ДТ	О	ДТ	Р	ДТ

Примечание 1 — Толкование обозначений «О», «Р», «ПД» и «ДТ» приведено в 7.1.

Примечание 2 — Если указано «ПД», это означает, что поправки к документации, внесенные в соответствии с 7.9, представляют собой потенциальную компенсирующую меру для уточнения конструктивного исполнения системы.

Примечание 3 — Если указано «ДТ», это означает, что задокументированные дополнительные испытания или анализ в соответствии с 7.8 представляют собой потенциальную компенсирующую меру для устранения недостатка документации по верификации.

b) Информация, касающаяся общего функционирования цифрового устройства, должна содержать сведения, приведенные в таблице 2, где указаны также требования к применению этих сведений для каждого класса.

Таблица 2

Необходимая доступная информация	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
1 Общий подход к проектированию (например, проектирование на основе времени или на основе события, статическое или динамическое управление ресурсами, проектирование с помощью синхронных и асинхронных электронных средств)	О	ПД	О	ПД	Р	ПД
2 Входные (в том числе на прерывания) и выходные сигналы контроллера устройства	О		О		О	
3 Как происходит обработка входных сигналов для получения выходных сигналов	О	ДТ	О	ДТ	О	ДТ
4 Четкое определение и характеристика всех факторов, которые могут повлиять на поведение устройства при его эксплуатации	О	ДТ	О	ДТ	Р	ДТ
5 Различные задачи (в том числе обработка прерываний), выполняемые устройством	О		О			
6 Установление последовательности и синхронизация задач	О		О			
7 Защита/разделение задач, составляющих основную и вспомогательные функции устройства	О		О		Р	
8 Факторы, влияющие на время отклика и изменчивость времени отклика основной функции	О		О		Р	
9 Оперативные и автономные испытательные и диагностические возможности, предоставляемые устройством	О		О		Р	
10 Условия пуска, останова и сброса, в том числе мощностные переходные процессы, включая потерю электропитания и перезапуск, а также отклик устройства	О		О	ДТ	О	ДТ

Примечание 4 — Толкование обозначений «О», «Р» и «ДТ» приведено в 7.1.

c) Для видов предполагаемого применения каждого класса должны быть получены доказательства наличия информации или соответствия критериям, приведенным в таблице 3.

Таблица 3

Необходимая доступная информация или критерий, которому должно соответствовать устройство	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
1 Никакие условия прерывания не оказывают негативного воздействия на основную функцию	О		О		Р	ДТ
2 Документальное подтверждение того, что проектирование любых мер самоконтроля проведено таким образом, что при обнаружении нарушений мерами самоконтроля устройство подаст тревожный сигнал или перейдет в состояние безопасного отказа	О		О	ДТ	О	ДТ
3 Обнаружение нарушений, влияющих на основную функцию, обеспечено мерами самоконтроля или другими способами, такими как периодические контрольные испытания	О	ДТ	О	ДТ	Р	ДТ

Окончание таблицы 3

Необходимая доступная информация или критерий, которому должно соответствовать устройство	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
4 Проведен анализ, результаты которого задокументированы, который определяет возможные остаточные механизмы отказа и режимы отказа (например АДО, АВПО или анализа критичности) и демонстрирует, что при этом выявлены меры, принятие которых снижает вероятность сохранения механизмов отказа и режимов отказа	О		О			

Примечание 5 — Ко второму пункту таблицы. Ссылка на «безопасный отказ» основана на требованиях пункта е) в 6.2.

Примечание 6 — К четвертому пункту таблицы. Возможные меры могут включать узконаправленные дополнительные испытания, ограничения в использовании устройства или внешний контроль.

Примечание 7 — К четвертому пункту таблицы. В приложении А приведены рекомендации по некоторым особенностям проектирования программного обеспечения, которые могут оказаться проблематичными при соблюдении требований данного подраздела.

7.4 Свидетельства, подтверждающие качество устройства в процессе проектирования

7.4.1 Общие положения

Критерии, представленные в данном подразделе, обеспечивают уверенность в том, что проектирование проведено системно и соответствует общим принципам, происходящим из жизненных циклов и определенным в соответствующих ядерных стандартах.

Во всех случаях необходимо придерживаться следующего общего подхода:

- получить от проектировщика устройства свидетельства, подтверждающие применение цикла разработки, основанного на качестве;
- сравнить имеющиеся свидетельства с соответствующими требованиями МЭК 61513, настоящего стандарта и других соответствующих стандартов МЭК, разработанных специально для АС;
- определить, приемлемы ли любые упущения, неточности или расхождения и могут ли компенсирующие меры (при наличии), указанные для каждого требования, дополнить свидетельства, чтобы можно было сделать заключение о приемлемости потенциально применимого устройства.

В последующих пунктах приведены критерии, на соответствие которым необходимо проверять процесс проектирования.

7.4.2 Программа обеспечения качества, предоставляемая проектировщиком изделия

В таблице 4 приведены требования к программе обеспечения качества проектирования, изложенные в виде информации, которую должна содержать программа, или критериев, которым она должна соответствовать. Требования необходимо применять, заменяя знак «___» словом «должен» (или «необходимо») там, где указан символ «О», и словом «рекомендуется» (или «следует») там, где указан символ «Р».

Таблица 4

Необходимая доступная информация или критерий, которому должна соответствовать программа	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
а) Проектировщик ___ иметь заданную документально оформленную программу обеспечения качества (и продолжать ей следовать), которая ___ быть оценена на соответствие требованиям к обеспечению качества, установленным МЭК 61513. Данная оценка ___ идентифицировать любые пробелы и указывать их или обосновывать их наличие	О		О		Р	

Окончание таблицы 4

Необходимая доступная информация или критерий, которому должна соответствовать программа	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
b) Если части, касающиеся процессов разработки программного обеспечения или аппаратных средств (включая HPD), изложены в отдельных документах о качестве, не входящих в программу обеспечения качества, то эти документы (например, план обеспечения качества программного обеспечения) ___ быть совместимы с общей программой обеспечения качества	О		О		Р	
c) Если части, касающиеся процессов разработки программного обеспечения или аппаратных средств (включая HPD), изложены в отдельных документах о качестве, не входящих в программу обеспечения качества, то требования настоящего подраздела ___ быть применимы в одинаковой степени к этим вспомогательным документам по обеспечению качества	О		О		Р	
d) Программа обеспечения качества на протяжении всего процесса проектирования и разработки должна предъявлять следующие требования, учитывая их уровень обязательности, обозначенный «О» или «Р»:	—		—		—	
1) лица, осуществляющие деятельность по проектированию и разработке, ___ быть компетентны в области порученной им работы	О		О	ОЭ ДТ	Р	ОЭ ДТ
2) окончательный вариант проекта ___ пройти независимую валидацию, и уровень независимости должен соответствовать классу предполагаемого применения	О		О		О	
3) каждый этап проектирования и разработки ___ включать верификацию соблюдения требований, предъявляемых к данному этапу	О		О		Р	
4) управление конфигурацией ___ выполнять в обычном порядке в соответствии с 7.4.4	О		О		О	
5) управление изменениями ___ выполнять в соответствии с 7.4.5	О		О		О	
6) ведение документации ___ выполнять в соответствии с 7.4.6	О		О		О	
e) Если при проектировании и разработке используют инструменты, то в программе обеспечения качества, создаваемой проектировщиком, должно быть приведено обоснование их назначения в соответствии с уровнем обязательности, обозначенным «О» или «Р». Если проводящий квалификационную оценку сотрудник или разработчик приложения считает обоснование инструментов недостаточным, он должен продумать, какие компенсирующие меры могут быть и будут применены:	—		—		—	
1) история использования инструментов, их стабильность, пользовательская документация, уведомления о неисправностях и др.	О	ДТ ОЭ	Р	ДТ ОЭ		
2) вероятность того, что вследствие применения инструмента возможно ошибочное определение или отказ определения недостатков проекта устройства, а также вероятность отказа самого инструмента, выявляемые другими способами	О	ДТ	О	ДТ		
f) Если проектировщик и/или изготовитель допускает участие субподрядчиков, все требования настоящего стандарта, применимые к изготовителю или проектировщику устройства, ___ в равной степени относиться и к субподрядчикам	О		О		О	

Примечание — К пункту e) таблицы. Инструмент, применение которого может привести к ошибке, не обнаруживаемой другими способами (например, осмотром человеком), требует обоснования, сопоставимого с классом предполагаемого применения устройства, проект которого зависит от данного инструмента. Инструмент, который может не обнаружить ошибку, но применение которого не вызывает ошибки, может быть отнесен к классу ниже.

7.4.3 Процесс проектирования и разработки

В таблице 5 приведены требования к процессу проектирования и разработки, представленные в виде необходимой информации или критериев, которым должен соответствовать процесс. Требования необходимо применять, заменяя знак «___» словом «должен» (или «необходимо») там, где указан символ «О», и словом «рекомендуется» (или «следует») там, где указан символ «Р».

Таблица 5

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
a) Планы разработки программного обеспечения и аппаратных средств (в том числе HPD) ___ подразумевать, что процесс проектирования и разработки следует жизненному циклу, который делит проектирование и разработку на этапы	О		О		Р	
b) На каждом этапе жизненного цикла проектирования и разработки в плане обеспечения качества ___ документировать следующее: - цели, - входные и выходные данные, - используемые инструменты	О		О		Р	
c) ___ быть обеспечено доказательство, подтверждающее соблюдение всех вышеуказанных требований при разработке конкретного устройства. Это доказательство ___ задокументировано в формате, позволяющем извлечение и пересмотр	О		О		Р	

Примечание — К стандартам, устанавливающим требования соответствия жизненным циклам, относятся: МЭК 61513 (для проектирования на системном уровне), МЭК 62138 и МЭК 60880 (для программного обеспечения), МЭК 60987 (для заказных аппаратных средств на основе компьютеров), МЭК 61508 (для программного и аппаратного обеспечения), МЭК 62566 (для HPD).

7.4.4 Управление конфигурацией конструктивного исполнения

В таблице 6 приведены требования, относящиеся к управлению конфигурацией конструктивного исполнения, представленные в виде необходимой информации или критериев, которым должен соответствовать процесс. Требования необходимо применять, заменяя знак «___» словом «должен» (или «необходимо») там, где указан символ «О», и словом «рекомендуется» (или «следует») там, где указан символ «Р».

Таблица 6

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
a) ___ задокументированы свидетельства использования системы управления конфигурацией в отношении разработки потенциально применимого устройства, его программного обеспечения и аппаратных средств (в том числе HPD). Эта система управления конфигурацией ___ включать всю проектную документацию, описание процедур валидации, отчеты об испытаниях, которые ___ быть увязаны с версиями аппаратных средств, программного обеспечения и HPD	О	ДТ	О	ДТ	О	ДТ

Окончание таблицы 6

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
b) Система управления конфигурацией ___ действовать с самого начала разработки устройства в отношении всех компонентов (документов, анализа проекта, проектов программного обеспечения и HPD, чертежей оборудования, результатов испытаний и др.)	P		P			
c) Система управления конфигурацией ___ действовать с самого начала этапа валидационных испытаний устройства в отношении всех компонентов (документов, анализа проекта, проектов программного обеспечения и HPD, чертежей оборудования, результатов испытаний и др.)	O		O		O	

7.4.5 Контроль изменений проекта

Необходимо иметь документально подтвержденное свидетельство того, что проектировщик устройства до настоящего времени поддерживает систему контроля за внесением изменений, включая процедуры и компьютерные программные средства, в степени, соответствующей классу применения и обозначенной «O» или «P», как показано в таблице 7.

Таблица 7

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
a) Поддерживает и требует созыва комиссии по принятию изменений, действующей в рамках управляемого процесса по рассмотрению и утверждению изменений, которая должна давать разрешение на все изменения и регистрировать принятые ею решения	O		O		O	
b) Поддерживает и требует, чтобы все изменения проектов и документации, касающиеся аппаратного, программного обеспечения и HPD, были подтверждены ссылкой на разрешение изменения	O		O		P	
c) Систематически собирает и отслеживает отчеты о проблемах на местах использования, о производственных проблемах изготовителя, влияющих на конструктивное исполнение устройства, а также об отклонениях при испытаниях, получая таким образом исходные данные для осуществления контроля над внесением изменений. Примечание — Настоящий стандарт не может предписывать цепочку обратной связи на основании отчетов с мест, в которых конечный пользователь сообщает о проблемах, имеющих отношение к дистрибьютору, изготовителю или проектировщику. Важным является предоставление конечному пользователю информации о контактном лице, которое обеспечивает связь со стороной, способной наилучшим образом решить изложенную проблему	O		O		P	
d) Отслеживает все версии и редакции программного обеспечения, а также конструктивного исполнения HPD или конфигурации оборудования, и может сообщать об изменениях, которые были выявлены и скорректированы в каждой версии или редакции	O		O		P	

Окончание таблицы 7

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
e) Поддерживает и требует проведения анализа последствий каждого предлагаемого изменения и использует результаты этого анализа в процессе утверждения изменений. Анализ последствий должен включать рассмотрение масштабов изменения, его влияния на основные функции потенциально применимого устройства, возможности негативного влияния изменения на надежность основных функций, его участия в реализации жизненного цикла, где должна начаться работа, а также масштаба и тщательности необходимых валидационных испытаний						
f) Обеспечивает и требует повторного анализа утвержденного изменения комиссией по принятию изменений, чтобы разрешить его внедрение в производство. При повторном анализе комиссия должна обосновать разрешение на внедрение изменения результатами проверки полноты и точности: - документации по изменениям; - документации по повторной валидации; - пользовательской документации	О		Р			
g) Система контроля за внесением изменений действует с начала разработки конкретной модели устройства	Р		Р			
h) Система контроля за внесением изменений действует с начала валидационных испытаний конкретной модели устройства			О		О	

Вполне возможна разработка процесса контроля за внесением изменений, включающего два уровня комиссии по рассмотрению изменений, при условии существования четких процедур и правил, позволяющих комиссии нижнего уровня признать, что рассмотрение изменения относится к ведению комиссии более высокого уровня. Эти правила могут учитывать класс системы, на которую влияет изменение, величину изменения или иные подходящие критерии.

7.4.6 Проектная документация

Проектная документация входит в состав документации по безопасности, которую рассматривают в ходе проведения оценки. Другая часть документации по безопасности, предоставляемая пользователям, которые будут проектировать системы с использованием устройств или эксплуатировать и обслуживать эти системы, рассмотрена в 6.9.

В таблице 8 приведены требования к проектной документации, представленные в виде необходимой информации или критериев, которым должна соответствовать документация. Требования необходимо применять, заменяя знак «___» словом «должен» (или «необходимо») там, где указан символ «О», и словом «рекомендуется» (или «следует») там, где указан символ «Р».

Таблица 8

Необходимая доступная информация или критерий, которому должна соответствовать документация	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
a) Все документы ___ быть проверены и утверждены уполномоченными лицами	О		О		Р	
b) Все документы ___ быть полными, правильными и непротиворечивыми	О	ПД	О	ПД	О	ПД

Продолжение таблицы 8

Необходимая доступная информация или критерий, которому должна соответствовать документация	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
c) Документация по функциональным требованиям Документ по функциональным требованиям определяет функции устройства, реализуемые аппаратными средствами, программным обеспечением или HPD. Этот документ, используя явно определенный язык, указывает основные, вспомогательные и избыточные функции (если таковые имеются), а также любые ограничения на использование рассматриваемого устройства. Проектировщик устройства должен подготовить документацию по функциональным требованиям, содержащую следующую информацию в соответствии со степенью обязательности, обозначенной «О» или «Р»:	—		—		—	
1) основные, вспомогательные и избыточные функции, выполняемые устройством	О		О		О	
2) если применимо, средства для обеспечения защиты основных функций от всех преднамеренных и непреднамеренных действий со стороны вспомогательных и избыточных функций	О		О		Р	
3) обеспеченность функциями самоконтроля и их действия, направленными на обнаружение отказов	О		О		Р	
4) внутренние интерфейсы между модулями устройства	О		Р		—	
5) внешние интерфейсы устройства	О		О		О	
6) роли, типы, форматы, диапазоны и ограничения входных, выходных сигналов, тревожных сигналов, параметров и данных конфигурации, где применимо	О		О		О	
7) различные режимы поведения и соответствующие условия перехода	О		О		О	
8) любые ограничения, которые необходимо соблюдать при использовании устройства	О		О		О	
9) время отклика, пропускная способность и другие динамические параметры, необходимые для полного понимания функций и ограничений устройства	О	ДТ	О	ДТ	О	ДТ
10) ограничения условий окружающей среды (см. 6.6)	О	ДТ	О	ДТ	О	ДТ
11) если применимо, требования информационной безопасности для защиты настроек от случайного или злонамеренного изменения	О	ПД	О	ПД	О	ПД
d) Документация, касающаяся принципа эксплуатации В документации приводят описания теории, лежащей в основе принципа действия устройства, конструкции устройства и общей функциональности аппаратных средств, программного обеспечения и HPD, достаточно детальные, чтобы можно было оценить эффективность верификации и валидации устройства	О	ПД	О	ПД	О	ПД
e) Документация на аппаратные средства В документации на аппаратные средства приводят описание общей структуры аппаратных средств, функций и свойств их компонентов (в том числе свойств, характеризующих эксплуатационную надежность, см. 6.6), используемых при проектировании и взаимодействии с программным обеспечением или HPD, со степенью детализации, необходимой для проведения квалифицированной модификации аппаратного средства с целью его использования в качестве заменяющего компонента, не идентичного оригиналу	О	ПД	О	ПД	О	ПД

Окончание таблицы 8

Необходимая доступная информация или критерий, которому должна соответствовать документация	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
f) Описание программного обеспечения и HPD Данная документация содержит описание общей структуры функциональной логики, реализованной в программном обеспечении или HPD, ее разбивки до модульного уровня, на котором могут быть востребованы навыки технического обслуживания или модификации, а также подробное описание взаимодействия между обычными аппаратными средствами и программным обеспечением или HPD	О	ПД	О	ПД	Р	ПД
g) Протоколы верификации и испытаний на каждом этапе проектирования. В случае программного обеспечения и HPD данная документация включает протоколы поузловых испытаний (для класса 1), комплексных испытаний и валидационных испытаний	О	ДТ	О	ДТ	Р	ДТ
h) Идентификационные сведения о версии, подлинность которых может быть подтверждена во время установки на площадке	О		О		О	
i) Пользовательская документация по безопасности в соответствии с 6.9	О	ПД	О	ПД	О	ПД
j) Журнал выполнения модификаций, представляющий собой описание или отчет, извлекаемый из системы управления конфигурацией, в котором указана история изменений версий изделия в соответствии с требованиями 7.4.4	О		О		Р	

7.5 Свидетельства обеспечения качества при изготовлении

Обеспечение качества при изготовлении является важным фактором, так как это может послужить основанием для принятия решения о применении устройств одинаковых или схожих моделей, которые могут быть произведены позже, несмотря на то, что такие факторы, как доступность идентичных компонентов, могут влиять на производство устройства.

В таблице 9 приведены требования к доказательствам обеспечения качества при изготовлении, представленные в виде необходимой информации или критериев, которым должен соответствовать процесс. Требования необходимо применять, заменяя знак «___» словом «должен» (или «необходимо») там, где указан символ «О», и словом «рекомендуется» (или «следует») там, где указан символ «Р».

Таблица 9

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
a) ____ документально зафиксировать доказательства того, что поставщик поддерживает программу обеспечения качества при изготовлении, сопоставимую с требованиями ИСО 9001	О		О		О	ОЭ СИ
b) _____ документально зафиксировать доказательства соответствия программе обеспечения качества при изготовлении	О		О		Р	

Окончание таблицы 9

Необходимая доступная информация или критерий, которому должен соответствовать процесс	Класс 1		Класс 2		Класс 3	
		КМ		КМ		КМ
c) _____ документально зафиксировать доказательства того, что изготовитель поддерживает программу квалификационной оценки поставщика, в рамках которой: - выполняет входной контроль; - выполняет контрольную проверку и/или испытание первой партии продукции; - осуществляет контроль вносимых изменений и замены компонентов; - сообщает проектной организации о вносимых изменениях и замене компонентов	О		О		Р	ОЭ
d) _____ документально зафиксировать доказательства того, что изготовитель выполняет необходимые эксплуатационные испытания устройства и испытания на принудительный отказ. Примечание — «ДТ» в данном случае относится к выполнению конечным пользователем испытаний на принудительный отказ	Р	ДТ	Р	ДТ	Р	ДТ
e) _____ документально зафиксировать версии и серийные номера испытательного оборудования, используемого при проведении функциональных испытаний, и подтвердить соответствие калибровки этого оборудования надлежащим стандартам по калибровке	О	ДТ	О	ДТ	Р	ДТ
f) _____ документально зафиксировать доказательства того, что соблюдены условия, гарантирующие, что при изготовлении в устройство устанавливают только известные и верифицированные программное обеспечение и конфигурации HPD	О		О		О	
g) _____ документально зафиксировать доказательства того, что изготовитель ведет записи даты производства, полной информации о версии, а также серийных номеров устройств сразу после их изготовления	О		О		Р	
h) _____ документально зафиксировать доказательства того, что каждое поставляемое изделие изготовитель сопровождает полной информацией о версии или редакции этого изделия (это может быть удобочитаемая этикетка на изделии или внутренний параметр, считываемый электронным способом)	О		О		О	
i) _____ документально зафиксировать доказательства того, что изготовитель обеспечивает подготовку отчетов о проблемах на местах, связанных с устройством, систематически собирает и отслеживает отчеты о проблемах, связанных с конструктивным исполнением устройства, и сообщает об этих проблемах проектировщику устройства. Примечание — Настоящий стандарт не может предписывать цепочку обратной связи на основании отчетов с мест, в которых конечный пользователь сообщает о проблемах, имеющих отношение к дистрибьютору, изготовителю или проектировщику. Важным является предоставление конечному пользователю информации о контактном лице, которое обеспечивает связь со стороной, способной наилучшим образом решить изложенную проблему	О		О		Р	
j) _____ учитывать влияние стабильности процесса изготовления	О	ОЭ СИ ДТ	О	ОЭ СИ ДТ	Р	ОЭ СИ ДТ

7.6 Стабильность изделия

В настоящем подразделе приведены критерии, позволяющие оценивать свидетельство зрелости изделия, вероятность его неизменности, а также то, что поставщик сможет осуществлять его поддержку на протяжении всего срока его службы после установки на АС. Указанные критерии также служат мерой тщательности, с которой выполняют анализ последствий в ходе контроля за внесением изменений и строгости подхода к проектированию изменений, в том числе в ходе регрессивного тестирования. Стабильность изделия тесно связана с опытом его эксплуатации, и в случае, когда опыт эксплуатации используют как фактор оценки, стабильность изделия играет существенную роль.

a) Стабильность изделия необходимо оценивать с точки зрения объема изменений основной функции, объема изменений, которые могут оказывать влияние на основную функцию, объема изменений, оказывающих влияние на другие функции, влияния любых изменений на основную функцию и причин внесения этих изменений (например, исправление программных ошибок, замена устаревших частей, изменения законодательства и др.).

Примечание — Малая частота внесения корректирующих изменений за значительный период использования изделия может указывать на степень стабильности изделия, а также на корректность и/или надежность его конструктивного исполнения.

b) Оценка, проводимая в соответствии с пунктом a), должна быть основана на записях о техническом обслуживании совместно с записями об инструментах и процедурах процессов контроля изменений и управления конфигурацией, отвечающих требованиям 7.4.4, 7.4.5 и 7.5.

c) Стабильность изделия необходимо оценивать с учетом объема работ по установке и интенсивности использования и доверять этой оценке только в том случае, если имеются свидетельства существенного объема производства и применения изделия.

d) В случае применения такой характеристики, как стабильность изделия, ее используют в поддержку слабых или недостаточных доказательств конкретных критериев, приведенных в 7.3, 7.4 или 7.5, где допускается применять характеристику стабильности изделия и где для ее поддержки используют опыт эксплуатации.

7.7 Опыт эксплуатации

Критерии, приведенные в настоящем подразделе, позволяют оценивать свидетельство эксплуатационной надежности изделия в составе работающего оборудования и в условиях эксплуатации, аналогичных и по крайней мере не менее сложных, чем в предполагаемом применении. Такое свидетельство является важным, так как характеризует действие устройства в условиях эксплуатации, что может дополнить испытания потенциально применимого устройства, выводя их за пределы ограниченного числа тестовых сценариев, осуществленных в ходе разработки.

a) Все принимаемые во внимание свидетельства опыта эксплуатации должны быть контролируемыми.

b) Идентификационные данные организации или организаций, предоставляющих отчет, должны быть документально зафиксированы.

c) Свидетельства опыта эксплуатации должны быть сопоставимы с точно известными версиями программного обеспечения и HPD.

d) Свидетельства опыта эксплуатации должны быть сопоставимы с известными параметрами конфигурации аппаратных средств, программного обеспечения и HPD.

e) В случае, когда опыт эксплуатации подтвержден для версий программного обеспечения, HPD или аппаратных средств, отличных от версий в планируемом применении, необходимо провести анализ отличий этих версий с целью определения, в какой степени может быть применим опыт эксплуатации каждой версии устройства.

Для подтверждения возможности применения более ранних версий программного обеспечения и HPD могут быть использованы результаты дополнительных испытаний, проведенных для получения опыта эксплуатации.

f) При анализе свидетельств опыта эксплуатации необходимо учитывать, выполняет потенциально применимое устройство конкретные функции непрерывно или периодически по требованию. В первом случае основой свидетельства служат часы фактической эксплуатации; а во втором — число циклов запуска (включая контрольные испытания) без отказа функций, вызываемых по требованию.

g) Опыт эксплуатации должен охватывать все аспекты функций потенциально применимого устройства в рамках целевого применения.

h) Охват и объем опыта эксплуатации должны быть достаточными для обеспечения уверенности в соответствии устройства классу его целевого применения.

i) Охват и объем опыта эксплуатации должны быть достаточными для обеспечения уверенности в соответствии устройства необходимой сложности, принимая во внимание программное обеспечение и HPD, а также другие аппаратные средства.

j) Если опыт эксплуатации является главным или очень весомым критерием для свидетельства корректности устройства, объем и охват опыта эксплуатации крайне важны, поэтому объем и источник необходимых данных, получаемых из опыта эксплуатации, должны быть обоснованы.

Достаточное время эксплуатации следует определять в каждом конкретном случае на основе технической оценки. При такой оценке в первую очередь следует учитывать ожидаемый уровень надежности, требуемый на системном уровне для выполняемых устройством функций.

Для целевого применения класса 1 опыт эксплуатации должен быть основан на нескольких случаях применения в ряде организаций, предоставляющих отчет.

Отсутствует требование о том, чтобы опыт эксплуатации был получен на объекте использования атомной энергии. Устанавливаемое требование заключается в том, чтобы охват и объем опыта эксплуатации были тщательно задокументированы (что может не относиться к промышленным условиям), а опыт эксплуатации потенциально применимого устройства был получен в условиях целевого применения [см. пункт k) ниже].

Примечание — Информация об объеме опыта эксплуатации, необходимого для установления критериев надежности, приведена в приложении D МЭК 61508-7.

k) Учитываемый опыт эксплуатации должен быть получен в условиях не менее сложных, чем при целевом применении. Эти условия должны включать следующее (если применимо):

- условия технологического процесса (например, температура, давление, вязкость, содержание частиц и т. д.) для смачиваемых устройств, таких как клапаны или датчики (см. 6.6);
- внешние условия эксплуатации аппаратных средств (например, температура, влажность, вибрация, ЭМП, излучение) (см. 6.6);
- профиль эксплуатации или метод использования (например, скорость переходных процессов, таких как пуск компрессора или гармоники, характерные для инвертора, питаемого от генератора, а не от электросети), если это может каким-либо образом повлиять на эксплуатацию потенциально применимого устройства с точки зрения загрузки программного обеспечения;
- интерфейсы с другими устройствами.

l) Необходимы документально зафиксированные доказательства того, что создана и используется надежная система оповещения об отказах, что позволяет оценивать опыт эксплуатации с высокой степенью достоверности. Если система оповещает не обо всех отказах или нарушениях штатной эксплуатации, то оцениваемый опыт эксплуатации должен быть сужен, чтобы отражать неопределенность в точности работы системы оповещения об отказах.

Например, если не существует точных доказательств того, что получены оповещения обо всех отказах, часы эксплуатации можно сократить на 30 % в течение гарантийного периода и на 50 % или более — после него.

m) Когда опыт эксплуатации обнаруживает эпизоды очевидных случайных аппаратных отказов с частотой, превышающей прогнозируемую, необходимо рассмотреть возможность того, что имеют место систематические отказы устройства, обусловленные, например, ошибкой в программном обеспечении или HPD, негативным влиянием внешних факторов на работу компонента изделия и т. д.

n) Для оценки устройства такую характеристику, как опыт эксплуатации, следует применять в поддержку слабых или недостаточных доказательств соответствия критериям, приведенным в 7.3, 7.4 или 7.5, где сказано о допущении использования опыта эксплуатации.

7.8 Дополнительные испытания и/или анализ (верификация)

Дополнительные испытания могут быть проведены по ряду причин. Такими причинами могут быть подтверждение применимости опыта эксплуатации более ранних версий устройства, подтверждение модификаций устройства, устранение пробелов в валидационных испытаниях, компенсация недостаточности опыта эксплуатации, подтверждение корректности или надежности в соответствующих условиях эксплуатации.

Дополнительные испытания можно также использовать для восполнения пробелов в процессе проектирования (или недостатка данных при проектировании), в проектной документации (особенно пробелов в функциональных требованиях и валидационных испытаниях), в документации об откликах на конкретные входные состояния (например, на аномальные входные сигналы), а также при нехватке конкретного опыта эксплуатации путем детального изучения отклика на конкретные входные условия или на испытание устойчивости устройства к стрессовым нагрузкам.

Примерами дополнительных испытаний могут быть:

- испытания с имитацией отказа для подтверждения того, что функции самоконтроля обнаруживают каждый отказ и обеспечивают формирование выходных сигналов отказоустойчивого устройства;
- специальные испытания для подтверждения выполнения функций с малой частотой запроса или функций, не востребованных в штатных условиях (то есть ожидающих обнаружения конкретного события в отличие от непрерывно работающих функций), для которых трудно накопить опыт эксплуатации в нормальных условиях;
- испытания для подтверждения тех областей функционального поведения устройства, которые задокументированы не полностью или неоднозначно;
- особые испытания, связанные с модификацией устройства, подтверждающие допустимость включения опыта эксплуатации предшествующих версий в опыт эксплуатации модифицированного устройства;
- особые испытания для определения отклика устройства на входные сигналы, выходящие за пределы установленного диапазона, или неисправные входные сигналы (например, входной сигнал менее 4 мА при установленном диапазоне от 4 до 20 мА или монотонное понижение напряжения, подаваемого от источника питания на аналоговый вход и контур измерительного прибора), а также для определения приемлемости этого отклика при целевом применении устройства;
- статистически обоснованные выборочные испытания, подобные приведенным в МЭК 61508-7, приложение D. Необходимо отметить, что выполнить предварительные условия для такого испытания довольно трудно;
- дополнительные испытания для подтверждения того, что в конкретной конфигурации(ях) и в условиях целевого применения устройство отвечает функциональным и техническим требованиям;
- особые испытания для подтверждения отсутствия отклонений в выполнении основной функции, вызванных избыточными или вспомогательными функциями;
- особые испытания для подтверждения эффективности механизмов обеспечения информационной и ядерной безопасности.

Примечание — По поводу безопасности отказа см. требования 6.2, пункт e).

При использовании дополнительных испытаний для оценки потенциально применимых устройств, их документировании и обеспечении доступности для ознакомления должны быть соблюдены указанные ниже требования.

a) Документация по испытаниям должна содержать идентификационные сведения о точной версии испытываемого изделия.

b) Необходимо документально зафиксировать подвергаемые испытаниям функции (включая информацию о процедуре испытаний, данных испытаний, а также ожидаемых и полученных результатах испытаний).

c) Испытания следует разрабатывать с учетом целевого применения устройства, чтобы можно было показать соответствие поведения устройства требованиям к данному виду применения, включая предельные и исключительные условия.

d) Результаты испытаний следует проанализировать с учетом целевого применения устройства, чтобы показать соответствие поведения устройства требованиям к данному виду применения.

e) Внешние условия испытаний должны быть типичными для целевого применения, в противном случае причины допущения отклонений должны быть документально зафиксированы.

f) Если целевое применение относится к классу 1 или классу 2, необходимо документально зафиксировать базовые данные испытаний, чтобы стало понятно, какие результаты испытаний демонстрируют соответствие требованиям (например, сюда можно включить анализ или модель программного обеспечения, HPD или конструктивные особенности аппаратных средств, подвергаемых испытаниям).

g) Необходимо документально зафиксировать идентификационные сведения об организации, проводящей испытания.

h) Дополнительные испытания или анализ следует применять для получения недостающих доказательств соответствия конкретным критериям, приведенным в 7.3, 7.4 или 7.5, там, где указана допустимость применения дополнительных испытаний или анализа.

7.9 Доработка документации

Во многих случаях можно восполнить недочеты в документации, полученной от проектировщика или производителя, путем внесения поправок в документацию в процессе оценки или в соответствии с EAR.

Один из видов доработки документации часто называют «преобразованием документации». Оно основано на использовании результатов дополнительных испытаний для осуществления своего рода обратного проектирования, нацеленного на уточнение конструкторской спецификации и процедуры валидационного испытания. При преобразовании документации в конечное изделие не вносят никаких изменений и разрабатывают проект спецификации изделия по принципу «черного ящика» на основе всей доступной информации, включающей также информацию от проектировщиков. По этому проекту спецификации разрабатывают процедуру и проводят испытание. Различия между ожидаемыми и фактическими результатами испытания используют для внесения необходимых изменений в проект спецификации изделия и в спецификацию испытания, и весь процесс повторяют многократно, пока точность спецификации не будет подтверждена успешными испытаниями.

Доработка документации, используемая в качестве компенсирующей меры, должна подчиняться указанным ниже требованиям.

a) Для внесения поправок в документацию должна существовать созданная ранее прочная основа, состоящая из полного описания функционала или из комбинации описаний программного и аппаратного обеспечения и принципов их работы.

Примечание — Суть состоит в том, чтобы опираться на документацию, подготовленную проектировщиком, а не создавать ее с нуля. Дело в том, что значительная нехватка согласующейся документации, правильно объясняющей принципы работы изделия, является признаком недостаточно строгого подхода проектировщика, что ставит под сомнение сам проект.

b) Все поправки к документации, касающиеся функциональности конструкции, должны быть отрецензированы проектировщиком потенциально применимого устройства.

Примечание — Суть состоит в том, чтобы гарантировать техническую корректность поправок в критических аспектах проекта изделия, которые являются ключевыми в обеспечении защиты основной функции от воздействия вспомогательных или избыточных функций при всех требуемых режимах.

c) Если дополнительные испытания используют как часть процедуры преобразования документации, то эти испытания должны соответствовать требованиям 7.8.

d) Доработку документации следует применять для поддержки недостаточно строгих описаний конкретных критериев, приведенных в 7.3, 7.4 или 7.5, там, где указана допустимость применения доработки документации.

8 Критерии интеграции устройства с целью применения. Пределы и условия использования

8.1 Общие положения

В настоящем разделе рассмотрены допустимые пределы и условия, которые могут ограничивать использование потенциально применимого устройства. Возникновение условий и пределов может являться результатом оценки пригодности, или они могут быть продиктованы необходимостью квалификации устройства по частям для использования в заданных пределах и условиях. Все ограничения необходимо документально зафиксировать в EAR (см. 5.3.3) и пользовательской документации по безопасности (см. 6.9), относящихся к потенциально применимому устройству.

8.2 Ограничения применения

Потенциально применимое устройство может быть признано аттестованным для определенного применения при условии, что решен вопрос о конкретных ограничениях и условиях его использования.

В EAR необходимо указать следующее:

- самый высокий класс вида применения, для которого аттестовано устройство;
- особые случаи использования, для которых аттестовано устройство (где применимо);
- пределы надежности, которых устройство может достигнуть самостоятельно или в дублированной конфигурации;
- конкретные опции или вторичные функции, которые необходимо разрешить или блокировать, включая конкретные настройки параметров, требуемые для каждого класса;
- допустимые внешние условия эксплуатации (в соответствии с 6.6), для использования в которых аттестовано устройство;
- факторы, ограничивающие эксплуатационный срок службы (например, такие, как использование алюминиевых конденсаторов);
- любые особые меры, которые необходимо соблюдать во время эксплуатации или проведения испытаний для обеспечения безопасного использования устройства.

8.3 Модификации устройства, необходимые для его целевого применения

Потенциально применимое устройство может быть признано аттестованным для конкретного применения, если перед его использованием осуществлены определенные модификации аппаратных средств или самые незначительные модификации программного обеспечения устройства. Иногда это необходимо, например в случае применения в модернизированных системах, где важно соответствие форм или требуется согласование импедансов, но при этом принципиально важно, чтобы такие модификации не приводили к созданию нового устройства, так как в этом случае настоящий стандарт будет неприменим.

Например, некоторые потенциально применимые устройства обладают вторичными функциями, такими как HART, реализуемыми наложением высокочастотных сигналов на технологический сигнал диапазона от 4 до 20 мА. Может потребоваться блокировка этой опции или применение низкочастотного фильтра, чтобы высокие частоты не оказывали влияния на другие устройства целевой системы.

При необходимости любой модификации устройства следует соблюдать приведенные ниже требования.

a) В EAR необходимо:
- определить требующиеся изменения;
- подтвердить степень поддержки этих изменений проектировщиком устройства.

b) Все модификации конструкции устройства не должны приводить к признанию недействительным опыта эксплуатации, предоставленного для оценки устройства. Модификации не должны концептуально менять основную функцию устройства.

c) Все модификации должны быть невелики по своему масштабу, ограничены по объему и просты для верификации и валидации.

d) Все модификации должны быть выполнены в соответствии со всеми требованиями, указанными в 7.4, способом, предусмотренным классом целевого применения.

e) После осуществления модификаций необходимо внести уточнения в EAR с учетом всех факторов, которые могли повлиять на содержащиеся в отчете выводы.

8.4 Модификации системы для размещения устройства

Потенциально применимое устройство может быть признано аттестованным для конкретного применения, если перед его использованием осуществлены определенные модификации системы. Настоящий подраздел применим, в частности, в случаях, требующих усовершенствований, когда, например, может понадобиться использование промежуточного реле для обеспечения необходимых интерфейсов между потенциально применимым устройством и другими компонентами системы.

В таких случаях при оценке устройства необходимо учесть и документально зафиксировать указанные ниже аспекты.

a) В EAR необходимо указать возможные изменения конструктивного исполнения системы, которые могут потребоваться, в том числе:
- дополнительное оборудование для контроля возникновения отказа;
- дополнительное резервирование или разнообразие;
- проверка соответствия межканальных связей;
- переназначение функции другой подсистеме;

- изменения, вызванные обеспечением защиты от условий окружающей среды, такие как дополнительное экранирование, вентиляция, охлаждение и др.;
- изменения в процедурах технического обслуживания и/или эксплуатации.

b) В EAR следует указать требования к обучению на системном уровне, необходимость которого обусловлена внедрением потенциально применимого устройства.

c) После осуществления модификаций необходимо внести уточнения в EAR с учетом всех факторов, которые могли повлиять на содержащиеся в отчете выводы.

8.5 Интеграция и ввод устройства в эксплуатацию в системах безопасности АС

Устройство, аттестованное для заданного применения, вводят в эксплуатацию, интегрируя его в новую конструкцию или в модифицированном виде в действующую систему безопасности АС.

Следует различать две ситуации:

- применения, в которых заново аттестованное устройство работает самостоятельно в таком режиме, который не несет риска полного отказа функции безопасности АС;
- применения, в которых заново аттестованное устройство задействовано во всех каналах системы или в отдельной точке, где возможны отказы, в связи с чем присутствует риск того, что данное устройство вызовет полный отказ функции безопасности АС, например отказ защитного устройства источника питания системы безопасности.

На основе EAR разрабатывают план ввода в эксплуатацию/интеграции, который должен:

a) включать соответствующие требования, приведенные в разделе 6 МЭК 61513;

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

c) во втором описанном выше случае или если остались аспекты функциональности устройства, требующие валидации, план ввода в эксплуатацию/интеграции должен также:

1) рассмотреть вариант поэтапного введения потенциально применимого устройства в систему, предусматривающий возможность начального периода валидации, когда устройство вводят в эксплуатацию только в одном канале или участке дублирующей системы, что позволяет оценить работу устройства в реальной целевой системе;

2) определить подходящие средства обеспечения и верификации корректных настроек параметров всех устройств, внедренных в систему, включая устройства, указанные в EAR;

3) определить тестовые сценарии ввода в эксплуатацию, основанные на динамических аспектах (переходных процессах) систем безопасности, имея в виду, что:

- выбор конкретных тестовых сценариев должен быть основан на моделировании и имитации работы системы;
- в рамках этих испытаний необходимо определить время отклика устройства, а также правильную последовательность и приоритет выполнения защитных действий;
- для устройств, обеспечивающих защиту систем электропитания, тестовые сценарии должны включать целиком последовательность запуска системы и нагрузочные испытания выбранных систем безопасности;

4) предусмотреть требование о регистрации следующей информации при вводе в эксплуатацию:

- все отклонения функции устройства от данных, указанных в EAR. Не следует пренебрегать малыми отклонениями, поскольку они могут указывать на серьезные недостатки в проектах программного обеспечения или HPD испытуемого устройства;
- значения всех настраиваемых параметров устройства;
- результаты всех испытаний, вплоть до окончательной интеграции устройства в систему.

9 Вопросы, связанные с сохранением приемлемости устройства

9.1 Общие положения

При оценке потенциально применимое устройство может оказаться идеальным с точки зрения функциональной пригодности и подтвержденной корректности работы, но следует учитывать такие факторы, как срок службы устройства и перспектива поддержки поставщика в силу длительных сроков службы ядерных установок.

В настоящем разделе приведены критерии оценки потенциально применимых устройств, учитывающие вышесказанное, и особенно перспективы обслуживания программного обеспечения и HPD.

9.2 Уведомления от проектировщика и изготовителя устройства

Необходимо принять соответствующие меры, гарантирующие официальное предупреждение пользователя о любых модификациях аттестованного устройства. В случае модификации программного обеспечения или HPD, встроенных в аппаратные средства, необходимо провести анализ влияния изменений, а устройство должно пройти повторную аттестацию в соответствии с настоящим стандартом.

Потенциально применимое устройство следует оценивать, учитывая уведомления изготовителя или проектировщика об отказах, имевших место после оценки опыта эксплуатации, если устройство находилось в эксплуатации. Информация об отказе на другой установке может быть использована для инициирования профилактического осмотра или замены устройства.

При проведении оценки следует рассмотреть следующие факторы и сообщить результаты попытки получить согласие изготовителя (и проектировщика):

- на своевременное уведомление о каждом отказе устройства на других установках;
- включение в уведомление анализа, который мог бы помочь установить, может ли дефект оказать влияние на основную функцию или снизить ее устойчивость к отказам вспомогательных и избыточных функций;
- предоставление доступа к актуальному перечню дефектов, в котором указаны возможные воздействия обнаруженных отказов, текущий статус их разрешения, а также точные версии, на которые они влияют;
- предоставление уведомления о каждом изменении — замене компонента аппаратных средств, изменении в процессе изготовления или изменении в программном обеспечении или HPD.

9.3 Процесс изготовления и срок поддержки текущей версии

Потенциально применимое устройство следует оценивать с учетом предполагаемого срока поддержки устройства, а также срока службы самого устройства. Что касается первого фактора, более продолжительный период поддержки предпочтительнее и может являться предметом обсуждения. Сведения о сроке службы устройства используют для планирования его замены до окончания срока службы.

В ходе оценки следует рассматривать и документально фиксировать в EAR следующие факторы:

- долгосрочные обязательства по производству текущей версии продукта и устройства в целом;
- срок службы текущей версии и устройства в целом;
- готовность изготовителя или проектировщика предупреждать о выводе из эксплуатации конкретной версии и устройства в целом;
- готовность поставщика принять обязательство по обеспечению совместимости разъемов при последующих заменах;
- готовность поставщика принять обязательство по обеспечению функциональной совместимости при последующих заменах;
- влияние необходимых для применения модификаций, выполненных по требованию заказчика.

9.4 Сохранение инструментов и документации, относящихся к техническому обслуживанию

Жизненный цикл АС намного длиннее жизненного цикла цифровых устройств, поэтому при оценке устройства следует учитывать фактор устаревания. В ходе оценки следует установить, согласен ли проектировщик устройства обеспечить договорное обязательство (например, заключить договор под отлагательным условием) или дать заверения в том, что если проектировщик или изготовитель решат прекратить поддержку потенциально применимого устройства, будет доступно следующее:

- установочные копии средств конфигурирования, таких как редактирующие программы, компилирующие программы;
- копия операционной среды для этих средств (например, конкретная версия Unix или Windows);
- копии всех исходных файлов, файлов построения, библиотек и т. д. из системы управления конфигурацией;
- специальные аппаратные средства (например, программаторы ППЗУ, логические анализаторы);
- технологические чертежи;
- копии всех документов (спецификации, отчеты об испытаниях и т. д.);

- подробное описание компьютерных технических средств и дополнительных приспособлений, необходимых для использования операционной системы, инструментов программного и аппаратного обеспечения или самого оборудования.

9.5 Рекомендации для конечного пользователя

С целью поддержки длительного использования потенциально применимого устройства компания, эксплуатирующая АС, помимо проведения оценки устройства должна следовать нижеуказанным рекомендациям:

- поддерживать систему управления конфигурацией независимо от поставщика, учитывая:
  1) все модификации параметров конфигурации;
  2) все исходные модификации, документально зафиксированные в EAR;
  3) все версии, полученные от поставщика, и статус их установки и конфигурации;
- обеспечивать работу системы контроля изменений с эффективным анализом влияния изменений;
- выполнять валидационные испытания после всех внесенных в конфигурацию изменений (даже изменений параметров);
- сохранять копии средств конфигурирования, например редактирующих программ, компилирующих программ;
- если устройство используют для видов применения разных классов, все действия по поддержке устройства должны соответствовать самому высокому классу.

Приложение А
(справочное)

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

В настоящем приложении приведены рекомендации по верификации выводов, сделанных при оценке устройства, касающиеся свойств, позволяющих избегать систематических отказов (см. 7.3).

Приведенная в настоящем приложении информация предназначена главным образом для видов применения класса 1 или класса 2, но может быть применена и к классу 3. Для программного обеспечения уверенность в предотвращении систематических отказов достигается главным образом путем проведения анализа. Причиной систематических отказов могут быть также условия окружающей среды, но при квалификационной оценке могут быть использованы анализ или испытания в соответствии с МЭК 60780, как описано в 6.6.

Как указано в 7.3, оценка надежности конструкции, позволяющей избегать систематических отказов, начинается с проверки общего проектного решения системы. В случае программного обеспечения это может быть реализовано в виде проверки возможных механизмов, заложенных в проекте, которые, как известно, являются источниками потенциальных проблем. Нижеприведенный перечень не является исчерпывающим, но может служить отправной точкой.

a) Чувствительность к профилю спроса может оказывать влияние на загрузку CPU, порядок обработки прерываний и т. д. Ниже приведены примеры возможных источников отказа устройства:

- взаимодействие между двумя или более входными сигналами;
- поведение сигнала (например, короткие выбросы за пределы установленного диапазона) вследствие ЭМП;
- перегрузка из-за каскадного роста числа сигналов на входах;
- наихудший случай нарушения временной синхронизации.

Примечание — МЭК 60880 (применительно к системам класса 1) устанавливает требование однозначной диспетчеризации работы программного обеспечения, а МЭК 62138 (применительно к системам класса 2) — прогнозируемого выполнения программ во времени. Настоящий стандарт фактически требует, чтобы анализ наихудшего варианта показывал, что электронный(ые) компонент(ы), обеспечивающий(ие) основную функциональность, будет(ут) всегда срабатывать вовремя или реагировать в пределах заданного времени.

b) Если архитектура конструктивного исполнения может предполагать наличие недостатков в основополагающем подходе, что снижает степень уверенности в соблюдении требуемых свойств системы (с учетом соответствия уровня уверенности и класса применения), целесообразно провести проверку конструктивного исполнения на наличие специфических конструктивных особенностей, могущих породить подобные сомнения.

Для видов целевого применения класса 1 следует обратить внимание на следующие особенности (факторы):

- упреждающее распределение задач;
- все причины, перечисленные для классов применения 2 и 3.

Для видов целевого применения класса 2 следует обратить внимание на следующие особенности (факторы):

- динамические объекты, создаваемые в режиме реального времени;
- сбор ненужных данных;
- любые, кроме простейших, операции с указателями (например, арифметические операции с указателями);
- асинхронный доступ к ресурсам или их блокировка;
- зависимости времени или даты, оказывающие влияние на основную(ые) функцию(и);
- все причины, перечисленные для класса применения 3.

Для видов целевого применения класса 3 следует обратить внимание на следующие особенности (факторы):

- перегрузки каналов связи, вызываемые другими устройствами (например, чат-узлом);
- неконтролируемое или неупорядоченное использование стековой или динамической памяти;
- оперативное управление в зависимости от входных данных;
- рекурсия;
- приоритеты динамических задач;
- высокая загрузка системы, измеряемая использованным временем или памятью CPU.

c) Для видов применения класса 1 трудно гарантировать, что основная функция сработает вовремя, если конструктивное исполнение рассчитано на любое, кроме простейшего, использование прерываний или если они использованы в конструктивном исполнении вторичных функций, где могут оказывать влияние на загрузку системы и таким образом косвенно влиять на основные функции.

d) Для видов применения классов 1 и 2 систематические отказы считаются менее вероятными, если программное обеспечение разработано с использованием:

- соглашения о присвоении имен;
- исключения потенциально опасных языковых конструкций, толкование которых компилятором или интерпретатором может быть нестандартным.

e) Для видов целевого применения классов 1 и 2 желательно использовать надлежащий статический анализ исходного кода.

f) Меры самоконтроля, такие как логический контроль исполнения программы, подтверждения и т. д., могут быть полезными, особенно если эти функции используют для выдачи сигнала тревоги или для безопасного отключения устройства.

Приложение ДА
(справочное)

Отличия в подходах к категоризации функций контроля и управления и классификации систем контроля и управления в зависимости от их важности для безопасности атомных станций, применяемых в МЭК и Российской Федерации

Таблица ДА.1 — Категоризация функций контроля и управления и классификация СКУ в зависимости от их важности для безопасности АС, применяемые в МЭК и РФ

МЭК/РФ	Функции/Системы	Категоризация функций и классификация систем контроля и управления			
		важных для безопасности АС			не влияющих на безопасность АС
МЭК	Функции (МЭК 61226)	Категория А (В, С)	Категория В (С)	Категория С	Не категоризированы
	Системы (МЭК 61513, МЭК 61226)	Класс безопасности 1	Класс безопасности 2	Класс безопасности 3	Не классифицированы
РФ	Функции (НП-026-16)	Категория А	Категория В	Категория С	Не категоризированы
	Системы (НП-001-15)	Класс безопасности 2		Класс безопасности 3	Класс безопасности 4

Приложение ДБ
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДБ.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 60671:2007	IDT	ГОСТ Р МЭК 60671—2021 «Системы контроля и управления, важные для безопасности атомных станций. Контрольные испытания»
IEC 60780	—	*
IEC 60880:2006	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
IEC 60980	—	*
IEC 60987:2007	—	*
IEC 61000 (all parts)	—	[1]
IEC 61226		ГОСТ Р МЭК 61226—2023 «Системы контроля и управления и электроэнергетические системы, важные для безопасности атомных станций, и выполняемые ими функции. Классификация»
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—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 62138:2004	IDT	ГОСТ Р МЭК 62138—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С»[2]

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

[2] Действует ГОСТ Р МЭК 62138—2021 «Программное обеспечение систем контроля и управления атомной станции, выполняющих функции безопасности категорий В и С. Общие требования», идентичный МЭК 62138:2018.

Окончание таблицы ДБ.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
ISO 9001:2008	IDT	ГОСТ Р ИСО 9001—2008 «Системы менеджмента качества. Требования»[1)]

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

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

- IDT — идентичные стандарты.

[1)] Действует ГОСТ Р ИСО 9001—2015 «Системы менеджмента качества. Требования», идентичный ИСО 9001:2015.

Библиография

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

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

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

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

IEC 62003:2020, Nuclear power plants — Instrumentation, control and electrical power systems — Requirements for electromagnetic compatibility testing

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

IEC 62645:2019, Nuclear power plants — Instrumentation, control and electrical power systems — Cybersecurity requirements

IAEA Safety Glossary Terminology Used in Nuclear Safety and Radiation Protection 2018 Edition

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

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; промышленные цифровые устройства; потенциально применимые устройства; оценка потенциально применимых устройств; критерии пригодности потенциально применимых устройств

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 25.07.2024. Подписано в печать 30.07.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 5,53.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

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