ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61226— 2011

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления

IEC 61226:2009
Nuclear power plants —
Instrumentation and control systems important for safety —
Classification of instrumentation and control functions
(IDT)

Издание официальное

Москва
Стандартинформ
2011

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ФГУП «ВНИИНМАШ») и Автономной некоммерческой организацией «Измерительно-информационные технологии» (АНО «Изинтех») на основе аутентичного перевода на русский язык указанного в пункте 4 стандарта, который выполнен Российской комиссией экспертов МЭК/ТК 45

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 сентября 2011 г. № 336-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61226:2009 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления» (IEC 61226:2009 «Nuclear power plants — Instrumentation and control systems important for safety — Classification of instrumentation and control functions»).

Международный стандарт МЭК 61226:2009 был подготовлен в подкомитете 45А «Контроль и управление на ядерных объектах» Технического комитета 45 «Ядерное приборостроение».

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

© Стандартинформ, 2011

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 и назначение . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Сокращения . . . 5
5 Схема классификации . . . 5
5.1 Основные положения . . . 5
5.2 Общая информация . . . 5
5.3 Описание категорий . . . 6
5.4 Критерии присвоения категорий . . . 7
6 Процедура классификации . . . 9
6.1 Общая информация . . . 9
6.2 Определение основ проекта . . . 9
6.3 Идентификация и классификация функций . . . 10
7 Установление технических требований по категориям . . . 11
7.1 Общие требования . . . 11
7.2 Требования, относящиеся к функциям . . . 11
7.3 Требования, относящиеся к системам контроля и управления . . . 12
7.4 Требования к оборудованию . . . 14
7.5 Требования, связанные с аспектами качества . . . 15
Приложение А (справочное) Примеры и категории . . . 18
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 20

Введение

a) Технические положения, основные вопросы и структура стандарта

Настоящий стандарт соответствует требованию[1)] Международного агентства по атомной энергии (МАГАТЭ) о классификации систем контроля и управления АС в зависимости от их важности для безопасности. При широком использовании компьютерных систем контроля и управления для систем контроля и управления атомных станций функции, важные для безопасности, распределены по нескольким системам или подсистемам. Таким образом, цель настоящего стандарта:

- классификация функций контроля и управления, важных для безопасности, по категориям в зависимости от их вклада в предотвращение и ослабление постулированных исходных событий (ПИС) и разработка требований, которые соответствуют важности для безопасности каждой из категорий;
- введение требований для спецификации и проектирования соответствующего оборудования и систем контроля и управления, выполняющих классифицированные функции.

Согласно рекомендациям МАГАТЭ[2)] методы классификации прежде всего основаны на детерминистском анализе безопасности и там, где это необходимо, их следует дополнять вероятностными методами. Несколько возможных подходов к применению вероятностной оценки безопасности (ВАБ) при классификации описаны в техническом отчете МЭК 61838:

«Атомные станции. Контроль и управление, важные для безопасности. Применение вероятностной оценки безопасности при классификации функций».

Настоящая редакция стандарта позволяет частично принять во внимание количественную оценку.

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

В МЭК 61513 имеется прямая ссылка на МЭК 61226, поэтому МЭК 61226 является документом второго уровня ПК 45А, посвященным категоризации функций и классификации систем.

Более подробная информация о структуре серии стандартов ПК 45А дана в подпункте d) настоящего введения.

c) Рекомендации и ограничения по применению настоящего стандарта

Корректная классификация функций направлена на привлечение необходимого внимания проектировщиков станций, разработчиков и изготовителей оборудования систем управления, операторов и контролирующих органов к техническим характеристикам, проектированию, аттестации, обеспечению качества, изготовлению, установке, обслуживанию и испытаниям систем, которые обеспечивают функции безопасности.

Настоящий стандарт устанавливает критерии и методы, применяемые для отнесения функций контроля и управления АС к трем категориям — А, В и С в зависимости от важности функции для безопасности, а также для отнесения функций, не имеющих непосредственной важности для безопасности, к категории «неклассифицированная». Настоящий стандарт описывает общие характерные требования для каждой категории и устанавливает основные технические требования по таким вопросам, как обеспечение качества, надежность, испытания и обслуживание.

Категория, которая присваивается функции, определяет общие и специальные технические требования. Общие требования для каждой функции основаны на обеспечении такого доверительного уровня, который гарантировал бы выполнение функции по запросу при требуемом уровне эксплуатационных характеристик и надежности. Это касается аспектов функционального назначения, надежности, эксплуатационных характеристик, стойкости к воздействию окружающей среды и обеспечения качества. Доверительный уровень для каждого из этих аспектов должен соответствовать важности функции для безопасности:

[1)] МАГАТЭ NS-R-1, требование 5.1.

[2)] NS-R-1, подраздел 5.2, содержит следующее требование: «метод классификации важности для безопасности структуры, системы или компонента должен, в первую очередь, основываться на детерминистских методах, дополненных, где это необходимо, вероятностными методами и взвешенной технической оценкой, учитывающей факторы, такие как:

a) выполняемые функции безопасности;

b) последствия отказа выполнения функции безопасности;

c) вероятность того, что система контроля и управления должна будет выполнить функцию безопасности; период времени после постулированного исходного события, по прошествии которого должна сработать система контроля и управления.

i) обеспечение функционального назначения достигается созданием полной и всесторонней спецификации требований и применением соответствующих стандартов и правил;

ii) обеспечение надежности достигается выбором соответствующих компонентов, структур и степеней резервирования и разнообразия в сочетании с физическим разделением и/или барьерами, электрической изоляцией и периодическими испытаниями во время эксплуатации;

iii) обеспечение эксплуатационных характеристик достигается созданием перечня требуемых характеристик, применением процедур обеспечения качества, верификацией и валидацией на стадии проектирования и производства, предэксплуатационными испытаниями отдельных и интегрированных систем и оборудования и их испытаниями во время эксплуатации;

iv) обеспечение стойкости к воздействию окружающей среды устанавливается программами аттестации оборудования для того, чтобы эксплуатационные характеристики оборудования не стали ниже требуемых вследствие эффектов старения и влияния окружающей среды, воздействующей на оборудование во время его работы;

v) обеспечение того, что аспекты функционального назначения, эксплуатационных характеристик, стойкости к воздействию окружающей среды и надежности были надлежащим образом приняты во внимание на каждом этапе, начиная от создания концепции и затем в процессе проектирования, изготовления, испытаний, установки, пусковых работ и кончая вводом в эксплуатацию, достигается проведением каждого этапа работ под контролем соответствующей программы обеспечения качества.

В настоящем стандарте термин «должен» обозначает требования, являющиеся обязательными для обеспечения соответствия с настоящим стандартом, термин «следует» обозначает требования, не являющиеся обязательными для обеспечения соответствия с настоящим стандартом и имеющие рекомендательный характер, а термин «может» подразумевает необязательные требования.

d) Описание структуры серии стандартов ПК 45А и взаимосвязь с другими документами МЭК и документацией других организаций (IAEA, ISO)

Документом высшего уровня серии стандартов ПК 45А является МЭК 61513. Этот стандарт предусматривает общие требования к системам контроля и управления, важным для безопасности АС, и он лежит в основе серии стандартов ПК 45А.

В МЭК 61513 имеются непосредственные ссылки на другие стандарты ПК 45А по общим вопросам, связанным с категоризацией функций и классификацией систем, оценкой соответствия, разделением систем, защитой от отказов по общей причине, аспектам программного обеспечения компьютерных систем, аспектам технического обеспечения компьютерных систем и проектированию залов управления. Те стандарты, на которые имеются непосредственные ссылки, рекомендуется использовать на этом втором уровне совместно с МЭК 61513 в качестве согласованной подборки документов.

На третьем уровне стандартов ПК 45А, на которые в МЭК 61513 нет непосредственных ссылок, находятся стандарты, связанные с конкретным оборудованием, техническими методами или конкретной деятельностью. Обычно эти документы, в которых по общим вопросам имеются ссылки на документы второго уровня, могут использоваться самостоятельно.

Четвертому уровню, продолжающему серию стандартов ПК 45А, соответствуют технические отчеты, которые не являются нормативными документами.

Для МЭК 61513 принята форма представления, аналогичная форме представления базовой публикации по безопасности МЭК 61508, с его структурой общего жизненного цикла безопасности и структурой жизненного цикла системы, и в нем дана интерпретация общих требований МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 для применения в ядерной области. Соответствие МЭК 61513 способствует достижению соответствия с требованиями МЭК 61508, интерпретированными для ядерной области. В этой связи, МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 в применении к ядерной области.

В МЭК 61513 есть ссылки на стандарты ИСО, а также на документ МАГАТЭ 50-С-QA (в настоящее время замененный документом МАГАТЭ GS-R-3) по вопросам, связанным с обеспечением качества.

В серии стандартов ПК 45А последовательно реализуются и подробно излагаются принципы и базовые аспекты безопасности, предусмотренные Правилами МАГАТЭ по безопасности атомных электростанций, а также серией документов МАГАТЭ по безопасности, в частности Требованиями NS-R-1 «Безопасность атомных электростанций: Проектирование» и Руководством по безопасности NS-G-1.3 «Системы контроля и управления, важные для безопасности атомных электростанций». Термины и определения, используемые в стандартах ПК 45А, согласуются с терминами и определениями, используемыми в МАГАТЭ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления

Nuclear power plants. Instrumentation and control systems important for safety. Classification of instrumentation and control functions

Дата введения — 2012—01—01

1 Область применения и назначение

Настоящий стандарт устанавливает метод классификации управляющих и информационных функций для атомных станций (далее — АС), а также классификации систем контроля и управления, оборудования, которые обеспечивают эти функции, в категории, обозначающей важность функции для безопасности. В соответствии с полученной классификацией затем определяют критерии проекта.

Критерии проекта — это меры качества, с помощью которых обеспечивается адекватность каждой функции по отношению к ее важности для безопасности АС. В настоящем стандарте эти критерии относятся к функциональности, надежности, эксплуатационным характеристикам, стойкости к воздействию окружающей среды (включая сейсмическое воздействие) и обеспечению качества.

Настоящий стандарт применим ко всем информационным и управляющим функциям, а также к системам и оборудованию контроля и управления, обеспечивающим эти функции. Рассматриваемые в настоящем стандарте функции, системы и оборудование обеспечивают автоматическую защиту, управление по замкнутому и разомкнутому контурам и представление информации обслуживающему персоналу. Они обеспечивают ведение технологических процессов на энергоблоке в пределах безопасных рабочих диапазонов и осуществляют автоматические действия или действия персонала, смягчающие или предотвращающие аварию или минимизирующие радиоактивные выбросы на территории АС или за ее пределы в окружающую среду. Функции контроля и управления, выполняющие эти задачи, защищают здоровье и безопасность персонала АС и населения.

Настоящий стандарт соответствует принципам, изложенным в правилах безопасности МАГАТЭ NS-R-1 и руководстве по безопасности NS-G-1.3, и определяет структурированный метод применения руководств, содержащихся в правилах и стандартах, к системам контроля и управления, выполняющим функции, важные для безопасности АС. При реализации требований МЭК 61508 настоящий стандарт следует изучать совместно с руководствами МАГАТЭ и МЭК 61513.

2 Нормативные ссылки

Приведенные ниже документы необходимы при применении настоящего стандарта. Если указана дата публикации, то именно данное издание должно использоваться. При отсутствии даты используется последнее издание документа (включая любые изменения).

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

МЭК 60709 Атомные станции. Системы контроля и управления, важные для безопасности. Разделение (IEC 60709 Nuclear power plants — Instrumentation and Control systems important to safety — Separation)

Издание официальное

МЭК 60780 Атомные станции. Электрическое оборудование систем безопасности. Аттестация (IEC 60780 Nuclear power plants — Electrical equipment of the safety system — Qualification)

МЭК 60812 Техника анализа надежности систем. Метод анализа вида и последствий отказа (АВПО) (IEC 60812 Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA))

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

МЭК 60964 Проектирование пунктов управления атомных станций (IEC 60964 Design for control rooms of nuclear power plants)

МЭК 60965 Дополнительные пункты управления для останова реактора без доступа в главный пункт управления (IEC 60965 Supplementary control points for reactor shutdown without access to the main control room)

МЭК 60980 Рекомендуемая практика аттестации на сейсмостойкость электрооборудования системы безопасности для атомных станций (IEC 60980 Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations)

МЭК 60987 Программируемые цифровые компьютеры, важные для безопасности атомных станций (IEC 60987 Programmed digital computers important to safety for nuclear power stations)

МЭК 61000-4 (все части) Электромагнитная совместимость. Методы проведения испытаний и измерений (IEC 61000-4 (all parts), Electromagnetic compatibility — Testing and measurement techniques)

МЭК 61000-6-2 Электромагнитная совместимость (EMC). Часть 6-2. Общие стандарты. Стойкость к промышленной окружающей среде (IEC 6100-6-2 Electromagnetic compatibility (EMC) — Part 6-2: Generic standards — Immunity for industrial environments)

МЭК 61513:2001 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования (IEC 61513 Nuclear power plants — Instrumentation and control for systems important to safety — General requirements for systems)

МЭК 61771 Атомные станции. Главный пункт управления. Верификация и валидация проекта (IEC 61771 Nuclear power plants — Main control room — Verification and validation of design)

МЭК 61772 Атомные станции. Главный пункт управления. Применение систем визуального отображения информации (IEC 61772 Nuclear power plants — Main control room — Application of visual display units (VDU))

МЭК 61839 Атомные станции. Проектирование главного пункта управления. Функциональный анализ и назначение (IEC 61839 Nuclear power plants — Design of control rooms — Functional analysis and assignment)

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

МАГАТЭ NS-R-1:2000 Безопасность атомных электростанций. Проектирование (IAEA NS-R-1:2000 Safety of Nuclear Power Plants: Design)

МАГАТЭ SG-R-3:2006 Система управления объектами и деятельностью (доступно только на английском языке) (IAEA SG-R-3:2006 The management system for facilities and activities (available in English only))

МАГАТЭ NS-G-1.3:2002 Системы контроля и управления, важные для безопасности атомных электростанций (IAEA NS-G-1.3:2002 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **ожидаемое при эксплуатации событие** (anticipated operational occurrence): Отклонение эксплуатационного процесса от нормальной эксплуатации, которое, как ожидается, произойдет как минимум один раз в течение срока эксплуатации (эксплуатационного ресурса) установки, но которое благодаря соответствующим предусмотренным в проекте мерам не нанесет значительного повреждения узлам, важным для безопасности, и не приведет к аварийным условиям.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.2 **отказ по общей причине;** ООП (common cause failure (CCF)): Отказ двух или более конструкций, систем или компонентов вследствие единичного конкретного события или единичной конкретной причины.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.3 **проектная авария;** ПА (design basis accident (DBA)): Аварийные условия, с учетом которых проектируется установка в соответствии с установленными проектными критериями и при которых повреждение топлива и выбросы радиоактивного материала находятся в разрешенных (санкционированных) пределах.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.4 **проектное событие;** ПС (design basis event (DBE)): Термин применяется для обозначения группы проектных аварий и ожидаемых при эксплуатации событий.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

Примечание — Смотри также 3.13.

3.5 **разнообразие** (diversity): Наличие двух или более резервных систем или резервных элементов для выполнения одной определенной функции, при котором разные системы или элементы наделяются различными признаками таким образом, чтобы уменьшалась возможность отказа по общей причине, включая общий отказ.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

Примечание — В МЭК 60880 дано следующее определение для термина «разнообразие»: Наличие двух или более путей или средств достижения установленной цели. Разнообразие специально создается как защита от отказа по общей причине. Оно может быть достигнуто наличием систем, которые физически отличаются одна от другой, или с помощью функционального разнообразия, если аналогичные системы достигают установленной цели различными путями.

3.6 **оборудование** (equipment): Одна или несколько частей системы; элемент оборудования является единицей продукции производства, способной выполнять заданные функции самостоятельно или в составе системы.

(МЭК 61513, статья 3.17, модифицированное)

3.7 **функция** (function): Конкретная цель или предназначенная для выполнения задача, которая может быть установлена или описана без ссылок на физические средства ее достижения.

3.8 **функциональность** (functionality): Характеристика функции, которая определяет процедуры переработки входной информации в выходную информацию.

(МЭК 61513, статья 3.25)

3.9 **программа по инженерной психологии** (human factor engineering program): Программа, описывающая, как минимум, организацию, роль и задачу отдельных специалистов, группы, специалистов, работающих в области учета человеческого фактора, мероприятия, направленные на учет человеческого фактора и интеграцию этих мероприятий в процессе проектирования и валидации, описывающая перечень отчетных материалов, предоставляемых на каждом этапе программы.

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

Элементы, важные для безопасности, включают:

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

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

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

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

Примечание — Элементы, важные для безопасности, которые рассматриваются в настоящем стандарте, в основном являются системами контроля и управления, важными для безопасности.

3.11 **безопасное контролируемое состояние** (non-hazardous stable state): Состояние станции, при котором достигнута стабилизация любых переходных процессов, реактор находится в подкритичном состоянии, обеспечен необходимый отвод тепла и ограничен выход радиоактивности.

Примечание — Переходной режим считается стабилизированным, когда для всех значащих для безопасности параметров имеющийся запас (например, разность между интенсивностями теплоотвода и выделения

тепла) либо стабилен, либо возрастает, либо остается достаточный запас, охватывающий все ожидаемые физические процессы.

3.12 **эксплуатационные характеристики** (performance): Эффективность, с которой выполняется заданная функция (например, время реагирования, точность, чувствительность к изменению параметров).

3.13 **состояния станции** (plant states):

<table>
<tr><td colspan="2">Эксплуатационные состояния</td><td colspan="4">Аварийные условия</td></tr>
<tr><td rowspan="2">Нормальная эксплуатация</td><td colspan="3">Проектные события</td><td colspan="2">Запроектные аварии</td></tr>
<tr><td>Ожидаемые при эксплуатации события</td><td>a)</td><td>Проектные аварии</td><td>b)</td><td>Тяжелые аварии</td></tr>
<tr><td colspan="4"></td><td colspan="2">Управление авариями</td></tr>
</table>

a) Аварийные условия, которые детально не рассматриваются в качестве проектных аварий, но тем не менее включаются в них.

b) Запроектные аварии без значительного разрушения активной зоны.

Примечание — Данное определение согласуется с определением Глоссария МАГАТЭ по вопросам безопасности. В нем лишь указано место концепции «проектного события» по отношению к другим концепциям.

3.14 **постулированное исходное событие;** ПИС (postulated initiating event (PIE)): Событие, определяемое на стадии проектирования как способное привести к ожидаемым при эксплуатации событиям или аварийным условиям.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.15 **резервирование** (redundancy): Использование альтернативных (одинаковых или неодинаковых) конструкций, систем и элементов таким образом, чтобы все они могли выполнять требующуюся функцию независимо от эксплуатационного состояния или отказа любого из них.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.16 **группа безопасности** (safety group): Группа оборудования, предназначенная для выполнения всех действий, требующихся в случае конкретного постулированного исходного события, с целью обеспечить невозможность превышения пределов, установленных в проектных основах для ожидаемых при эксплуатации событий и проектных аварий.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.17 **система, связанная с безопасностью** (safety related system): Система, важная для безопасности, которая не является частью системы безопасности.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.18 **система безопасности** (safety system): Система, важная для безопасности, обеспечивающая безопасный останов реактора или отвод остаточного тепла из активной зоны либо ограничивающая последствия ожидаемых при эксплуатации событий и проектных аварий.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.19 **единичный отказ** (single failure): Отказ, который приводит к потере способности системы или элемента выполнять предписанные им функции безопасности, а также любые последующие отказы, являющиеся результатом этого.

(Глоссарий МАГАТЭ по вопросам безопасности:2007)

3.20 **система** (system): Конфигурация взаимодействующих в соответствии с проектом составляющих, в которой элемент системы может сам представлять собой систему, называемую в этом случае подсистемой.

(МЭК 61513, статья 3.61)

3.21 **типовое испытание** (type test): Испытание на соответствие, проводимое на одном или более образцах, представляющих продукцию.

(IEV 394-40-02)

3.22 **недопустимые последствия** (unacceptable consequences): Последствия эксплуатационного состояния или ПИС, превышающие установленные пределы соответствующих состояний станции по выбросам на территорию АС или за ее пределы в окружающую среду.

Примечание — На государственном уровне могут быть также установлены дополнительные пределы, такие как недопустимое повреждение топлива или повреждение других основных компонентов. Это может быть

большой, неконтролируемый выброс, вызванный событиями с периодичностью, находящейся за пределами основ проекта АС, или же событиями, периодичность которых находится в рамках основ проекта, но которые приводят к величинам, превосходящим установленные пределы. Могут быть также установлены такие дополнительные пределы, как недопустимое повреждение топлива. Это может быть повреждение оболочки топлива, которое ведет к недопустимому повышению активности теплоносителя первого контура или структурному повреждению топлива, что снижает его охлаждающую способность.

4 Сокращения

Сокращение (англ.)	Сокращение (рус.)	Полное название
ALARA	—	Разумно достижимый низкий уровень
DBA	ПА	Проектная авария
DBE	ПС	Проектное событие
FAT	ПИ	Приемочные испытания
FMEA	—	Анализ характера и последствий отказа
HMI	ЧМИ	Интерфейс человек — машина
IAEA	МАГАТЭ	Международное агентство по атомной энергии
I&C	—	Контроль и управление
NPP	АС	Атомная станция
PIE	ПИС	Постулированное исходное событие
PRA	ВОР	Вероятностная оценка риска
QA	—	Обеспечение качества
SAT	—	Приемочные испытания на месте установки

5 Схема классификации

5.1 Основные положения

Функции, выполняемые системами контроля управления, должны быть отнесены к категориям в соответствии с их важностью для безопасности. Важность функции для безопасности должна быть определена путем оценки последствий ее отказа тогда, когда требуется ее выполнение, а также оценки последствий в случае ложного срабатывания. Категория определяет требования к проекту и качеству систем и оборудования контроля и управления. Эти требования должны быть определены независимо от технического решения применяемого оборудования. В 5.2 содержится основная информация по схеме классификации.

В 5.3 описаны три категории, применяемые для классификации функций. За основу взяты категории, первоначально установленные в первом издании МЭК 61226, опубликованном в 1993 г.

В 5.4 представлены критерии присвоения каждой категории.

В разделе 6 приведено руководство по процессу классификации.

В разделе 7 представлены технические требования к каждой из трех категорий.

Основная часть требований применяется к системам и оборудованию, выполняющим функции, однако некоторые требования применяются только к функциям.

В приложении А приведены характерные примеры классификации функций контроля и управления АС. Эти примеры даны только для информации, т.к. классификация может зависеть от типа реактора.

5.2 Общая информация

В основу проекта безопасности АС закладывается жесткое требование соблюдения принципа защиты в глубину. Основная мысль заключается в том, что должно быть несколько слоев или эшелонов, защиты для предотвращения небезопасных условий и что предпочтение всегда отдается предотвращению небезопасных условий, нежели смягчению их последствий. Так как для эксплуатации АС и поддержания ее безопасности требуется большое количество функций, которое еще более возрастает

вследствие применения принципа защиты в глубину, важно знать значение каждой функции для безопасности.

Серия стандартов МАГАТЭ по безопасности NS-R-1 устанавливает понятие о классификации систем АС в соответствии с их важностью для безопасности и дает примеры классификации основных систем нескольких типов АС. Все устройства, системы и компоненты, включая программное обеспечение для контроля и управления, являющиеся элементами, важными для безопасности, должны быть определены, а затем классифицированы на основании выполняемой функции и важности для безопасности. Они должны проектироваться, создаваться и обслуживаться таким образом, чтобы их качество и надежность соответствовали данной классификации.

Руководство по безопасности NS-G-1.3 предоставляет инструкции по классификации систем в соответствии с важностью для безопасности выполняемых функций. В руководстве вводятся факторы времени, такие как:

- требуемая продолжительность работы системы КиУ с момента ее начала;
- время, за которое могут быть предприняты альтернативные шаги;
- сроки своевременного выявления и устранения скрытых дефектов.

Настоящий стандарт расширяет стратегию классификации, представленную в Руководстве по безопасности МАГАТЭ NS-G-1.3, и устанавливает критерии и способы, которые должны применяться при отнесении функций контроля и управления АС к одной из трех категорий А, В и С в зависимости от их важности для безопасности или к неклассифицированной категории для функций, не играющих непосредственной роли в обеспечении безопасности. Функции контроля и управления, вписывающиеся в рамки систем безопасности, будут в основном отнесены к категории А или В. Функции контроля и управления, определенные как связанные с безопасностью, большей частью будут отнесены к категории В или С.

Важность для безопасности и соответствующие требования к различным частям систем безопасности и систем контроля и управления, связанных с безопасностью, будут различными, поэтому необходимо относить их к различным категориям безопасности. Некоторые системы контроля и управления могут оказывать значительное влияние на безопасность и, следовательно, требуют соответствующего внимания. Другие системы контроля и управления имеют среднее, низкое значение или не имеют существенного значения для безопасности. Соответственно к ним предъявляют менее строгие требования по обеспечению эксплуатационных характеристик и обоснованию безопасности и, следовательно, другие технические требования.

При применении принципов и критериев настоящего стандарта на национальном уровне может устанавливаться другая номенклатура для категорий А, В и С. Применение документа на национальном уровне должно соответствовать принципам, критериям и требованиям, приведенным в настоящем стандарте, что должно включать установление и документальное подтверждение необходимого соответствия определенным категориям.

5.3 Описание категорий

5.3.1 Основные положения

Системы контроля и управления АС выполняют функции, имеющие разные уровни важности для безопасности. Важность для безопасности каждой функции контроля и управления зависит от ее роли в достижении и поддержании безопасности, потенциальных последствий отказа функции в момент, когда необходимо ее выполнение, а также вероятности этих последствий. Поэтому первоначальный анализ безопасности конкретного проекта АС должен быть завершен до классификации функций контроля и управления. Тяжесть потенциальных последствий в случае постулированного отказа функции контроля и управления определяет доверительный уровень, необходимый при обеспечении различных характеристик систем и оборудования, выполняющих функцию, особенно функциональности, эксплуатационных характеристик и надежности.

Для процедур проектирования, оценки и лицензирования определены категории А, В и С с соответствующими наборами технических и качественных требований к системам контроля и управления, применяемых при проектировании и внедрении систем контроля и управления и оборудования, важных для безопасности.

5.3.2 Категория А

Категорию А используют для обозначения тех функций, которые играют основную роль в достижении или поддержании безопасности АС с целью предотвращения развития ПА до недопустимых последствий. Такая роль функций жизненно важна в начале переходного процесса, когда невозможно предпринять альтернативные действия, даже в случае выявления скрытых дефектов. Эти функции требуются для стабилизации переходного процесса, т.е. приведения станции в безопасное контроли-

руемое состояние, при котором реактор находится в подкритичном состоянии, обеспечен отвод тепла, а радиоактивные выбросы ограничены[3]. Если для достижения безопасного контролируемого состояния предусмотрены определенные неавтоматические действия, то должны быть рассмотрены следующие факторы: доступность резервных, прошедших валидацию информационных источников, задержка по времени, достаточная для проведения оператором оценки альтернативных источников информации, а также — являются ли действия, осуществляемые ручным управлением, единственной возможностью для смягчения данной цепи событий с целью сохранения безопасности АС.

К категории А также относят функции, отказ которых может непосредственно привести к аварийным условиям, которые могут вызвать недопустимые последствия, если аварийные условия не смягчены другими функциями категории А. К функциям категории А применяются повышенные требования к надежности. Следовательно, может потребоваться ограничение их функциональности и сложности.

5.3.3 Категория В

К категории В относят функции, которые играют дополнительную роль по отношению к функциям категории А в достижении или поддержании безопасности АС, в особенности функции, необходимые для эксплуатации после достижения безопасного контролируемого состояния с целью предотвращения развития ПС до недопустимых последствий или для смягчения последствий ПС. Выполнение функций категории В может исключить необходимость выполнения функции категории А. Функции категории В могут улучшить или дополнить выполнение функций категории А в процессе смягчения последствий ПС таким образом, что повреждение станции или оборудования или выброс активности могут быть исключены или сведены к минимуму.

К категории В также относят функции, отказ которых может вызвать ПС или увеличить его тяжесть. Из-за наличия функции категории А для обеспечения полного предотвращения или смягчения ПС требования по безопасности к функции категории В могут быть не такими строгими, как для функции категории А. Это позволяет, в случае необходимости, функциям категории В иметь более высокую функциональность по сравнению с функциями категории А в отношении метода определения необходимости срабатывания или в отношении их последующих действий.

5.3.4 Категория С

К категории С относят функции, которые играют вспомогательную или косвенную роль в достижении или поддержании безопасности АС. Категория С включает в себя те функции, которые имеют определенное значение для обеспечения безопасности, но не относятся к категории А или В. Эти функции могут быть частью реагирования на ПС, но при этом они могут не включаться непосредственно в ослабление физических последствий аварии или быть функциями, необходимыми для реагирования на запроектные аварии.

5.4 Критерии присвоения категорий

5.4.1 Основные положения

Ниже представлены критерии, применяемые для присвоения функциям категорий А, В и С.

Если функция не удовлетворяет ни одному из указанных выше критериев, то она должна быть отнесена к «неклассифицированным» (НК).

Если функция может быть отнесена к нескольким категориям, то в результате ей должна быть присвоена высшая из соответствующих категорий.

Окончательная категория, присваиваемая функции, может измениться при использовании вероятностных методов в соответствии с принципами, изложенными в 6.3.

5.4.2 Категория А

К категории А должны быть отнесены:

a) функции, требуемые для достижения безопасного контролируемого состоянии с целью предотвращения развития ПС до недопустимых последствий или для их смягчения;

b) функции, отказ или ложное срабатывание которых может привести к недопустимым последствиям, когда не существует другой функции категории А, смягчающей эти последствия;

---

[3] Для того чтобы справиться с быстрыми переходными режимами, на этой фазе над станцией осуществляется автоматический контроль. При более медленных переходных режимах стабильные условия могут быть достигнуты с помощью ручного управления при условии, что выполнение этих действий подразумевается с некоторой задержкой по времени. Эта задержка по времени представляет собой проектное требование к станции, соответствующее запаздыванию обнаружения и действия, и основано на учете человеческого фактора. Это не означает, что в это время нельзя применять неавтоматические действия. В некоторых странах, а также для станций старой модификации, ограничением для категории А может служить это время задержки, а не контролируемое состояние.

c) функции, требуемые для обеспечения информации и возможностей управления, которые позволят предпринять определенные неавтоматические действия с целью достижения безопасного контролируемого состояния.

5.4.3 Категория B

К категории B должны быть отнесены (если они не отнесены к категории A):

a) функции, требуемые после достижения безопасного контролируемого состояния при ПС с целью предотвращения или смягчения недопустимых последствий;

b) функции, требуемые для обеспечения информации и возможностей управления, которые позволят предпринять определенные неавтоматические действия, требуемые при достижении безопасного контролируемого состояния при ПС с целью предотвращения или смягчения недопустимых последствий;

c) функции, отказ которых при нормальной эксплуатации потребует введения в действие функций категории A для предотвращения аварии, которая потребует анализа;

d) функции, значительно снижающие частоту ПС, как установлено при анализе безопасности;

e) функции управления технологическим процессом станции и действующие таким образом, что основные параметры процесса удерживаются в пределах, установленных при анализе безопасности, если эти функции управления являются единственным средством управления этими параметрами. Если предусмотрены различные средства, то могут быть применены требования перечисления a) 5.4.4;

f) функции, используемые для предотвращения или уменьшения радиоактивного выброса или повреждения топлива, превышающего пределы и условия, соответствующие нормальной работе, установленные при анализе безопасности;

Примечание —Это относится к функциям, которые не охвачены в анализе ПС, из которого вытекает присвоение им категории A.

g) функции, обеспечивающие непрерывные или периодические проверки или контроль функций категории A для демонстрации их непрерывной готовности к работе и привлечения внимания персонала пункта управления при их отказах, если не предусмотрены альтернативные способы (например, периодические испытаний) проверки их готовности[4)].

Примечание —Там, где функция контроля является единственным средством обнаружения отказов, не обнаруживаемых другими способами, присвоение функции категории B обеспечивает правильную классификацию оборудования, выполняющего эту функцию.

5.4.4 Категория C

К категории C должны быть отнесены (если они не отнесены к категории A или B):

a) функции управления технологическим процессом станции, действующие таким образом, чтобы основные параметры процесса удерживались в пределах, установленных при анализе безопасности, не охваченных в требованиях перечисления e) 5.4.3 . В случае использования комбинации функций категории C должно быть представлено обоснование достаточности.

Примечание — Возможное применение требований перечисления a) 5.4.4 состоит в сочетании функции регулирования и соответствующего ручного запуска на основе независимых сигналов при обосновании использования неавтоматизированных действий;

b) функции, применяющиеся для предотвращения или смягчения незначительного радиоактивного выброса или незначительного разрушения топлива — в рамках основ проекта АС;

Примечание — Незначительными выбросами или незначительными разрушениями считаются такие выбросы и разрушения, которые находятся в пределах и условиях, предусмотренных для нормальной работы (например, в пределах ограничений на выбросы).

c) функции, обеспечивающие непрерывную или периодическую проверку или контроль функций категорий A и B на их постоянную готовность и предупреждающие персонал пункта управления об отказах, если им не назначена категория B в соответствии с перечислением g) 5.4.3;

d) функции, необходимые для достижения вероятностных показателей безопасности, включая снижение ожидаемой частоты ПС;

[4)] В МЭК 60671 пункт 4.2.6 даны более подробные указания, касающиеся класса оборудования, используемого для реализации таких функций и, в частности, даны примечания о том, что там, где характер испытания может препятствовать правильному выполнению системой или оборудованием функции, важной для безопасности, им должна быть присвоена та же категория.

e) функции, снижающие потребности в функциях категории А, установленных при анализе безопасности;

f) функции контроля и действий по смягчению последствий, вызываемых внутренними опасностями, предусмотренными в основах проекта АС (например, пожаром, затоплением);

g) функции предупреждения или обеспечения безопасности персонала во время и после событий, которые связаны с выбросом радиоактивных продуктов на станции или приводят к таким выбросам, а также событий, связанных с риском радиационного облучения;

h) функции контроля и действий по смягчению последствий, вызываемых природными явлениями (например, землетрясением, ураганом);

i) функции, применяющиеся в целях улучшения стратегии управления авариями с целью достижения и поддержания безопасного состоянии при запроектных авариях;

j) функции, обеспечивающие минимизацию последствий тяжелых аварий;

k) функции, обеспечивающие управление доступом на АС.

6 Процедура классификации

6.1 Общая информация

Схема классификации приведена на рисунке 1.

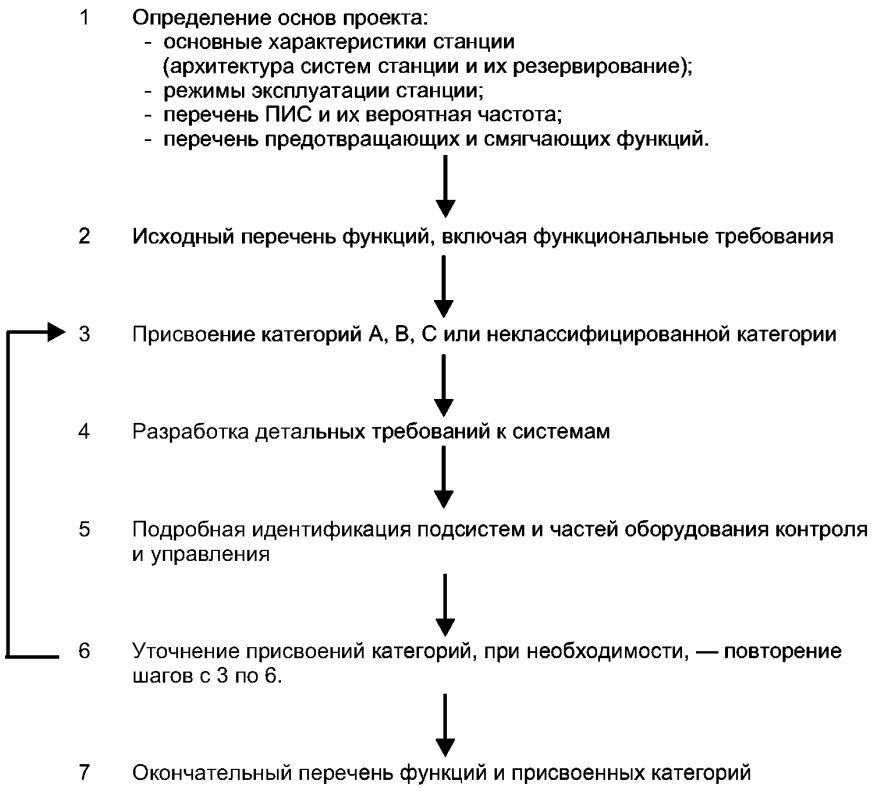


Рисунок 1 — Классификация

6.2 Определение основ проекта

Главная исходная информация для процесса классификации — вид АС и тип реактора (например, PWR — реактор с водой под давлением, BWR — реактор с кипящей водой или другой тип реактора), соответствующие ПИС, основные критерии проекта по резервированию механических и электрических

систем и оборудования. Кроме того, существенная информация — идентификация для каждого ПИС основных смягчающих функций и поддерживающих их функций.

Оценка частоты и последствий ПИС ведет к определению ПС, представляющих основы проекта станции. При рассмотрении технических особенностей проекта станции необходимо отобразить установленные диапазоны эксплуатационных состояний и аварийных условий, а также определенных радиологических пределов. Отдельные принципы безопасности, составляющие вместе «интегрированный комплексный подход к безопасности», обеспечивают безопасность станции. Данные принципы применяют при проектировании путем рассмотрения определенных ПС и последовательных физических барьеров для поддержания радиационного облучения в разрешенных пределах. ПС и критерии основ проекта станции (резервирование, разделение, и т.д.) так же, как и определение функций по предотвращению и смягчению, их вспомогательные функции являются основными вводными данными в процессе классификации.

Важность для безопасности каждой функции контроля и управления зависит от ее роли при достижении и поддержании безопасности станции, а также потенциальных последствий отказа функции. Поэтому первоначальный анализ безопасности конкретного проекта АС должен быть завершен до начала классификации функций контроля и управления.

6.3 Идентификация и классификация функций

Существенные для безопасности функции должны быть определены на ранних стадиях проектирования АС. Процесс идентификации этих функций и отнесения их к функциям контроля и управления или к действиям операторов должны проводиться в соответствии с МЭК 60964. После этой предварительной идентификации функции, каждой функции должна быть присвоена категория согласно разделу 5.

Метод классификации важности функции для безопасности должен основываться на детерминистском анализе безопасности и может быть дополнен вероятностными методами и техническим обоснованием, при этом следует учитывать:

- функцию(ии) безопасности, которую(ые) должна(ы) быть выполнена(ы);
- роль функции в предотвращении или смягчении постулированных исходных событий;
- роль функции при любых режимах эксплуатации (например, пуске, нормальной эксплуатации, перезагрузке топлива т.д.);
- роль функции после ПИС, таких как природные явления (например, сейсмическое воздействие, затопление, ураган, удар молнии), а также после внутренних угроз (например, пожара, затопления, ракетного удара, радиоактивного выброса на прилегающем энергоблоке или химический выброс с других станций или предприятий других отраслей);
- последствия отказа функции контроля и управления;
- результаты ложного срабатывания функции контроля и управления;
- вероятность того, что будет необходимость задействовать функцию, важную для безопасности;
- промежуток времени после ПС, за который или во время которого необходимо задействовать функцию;
- стратегию технического обслуживания, ремонта и испытаний.

На ранней стадии процесса проектирования невозможно определить подробно все функции, так как характеристики АС еще не полностью определены. Следовательно, процесс идентификации и присвоения категорий функциям должен быть итерационным и продолжаться в течение всего этапа проектирования. Там, где предварительное распределение функций по категориям не ясно, необходимо добавить пояснительное примечание к категоризации.

Поскольку отдельные функции могут быть вовлечены в выполнение нескольких аспектов спецификации требований, такие функции могут быть отнесены к нескольким категориям. В таком случае функция должна быть отнесена к высшей из применяемых категорий.

Так как резервирование, разнообразие и другие технические требования к функциям уточняются, например, в процессе анализа безопасности и разработки рабочих процедур, классификационный перечень должен пересматриваться и уточняться для получения окончательного перечня. Этот перечень должен быть оформлен документально и поддерживаться в рамках управления конфигурацией, так как он будет востребован проектировщиками станции/контроля и управления, разработчиками системы контроля управления в течение срока эксплуатации станции. Этот перечень может также потребоваться регулирующим органам.

7 Установление технических требований по категориям

7.1 Общие требования

В данном пункте представлены технические требования для каждой из категорий А, В и С. Требования должны по необходимости применяться к следующим этапам жизненного цикла функции контроля и управления: спецификации, проектированию, валидации, аттестации, изготовлению, установке, эксплуатации и техническому обслуживанию. Технические требования составляют четыре группы:

- требования, применяющиеся к функциям, касающимся спецификации и валидации функциональности, эксплуатационных характеристик и надежности;

- требования, применяющиеся при проектировании функций контроля и управления, связанных с характеристиками проекта такими, как резервирование, разнообразие, контролируемость и разделение. Эти характеристики в первую очередь определяют надежность соответствующих функций. Эти требования также включают в себя требования к ИЧМ;

- требования, касающиеся характеристик оборудования, связанных с обеспечением сейсмической стойкости и стойкости к воздействиям окружающей среды, а также электромагнитной совместимости;

- требования, связанные с обеспечением качества, верификацией и техническим обслуживанием, которые применяются к функциям, системам и оборудованию.

В большинстве случаев данные требования уже детально изложены в соответствующих правилах и стандартах. Правила, руководства и стандарты, перечисленные в разделе 2, являются нормативными ссылками и поэтому предоставляют четкие требования в отношении категорий безопасности контроля и управления, устанавливаемых настоящим стандартом. Взаимосвязь между категориями и стандартами, которые должны применяться, представлена в таблице 1. Детальные требования этих стандартов не повторяются в настоящем стандарте. В той же таблице обобщены основные типы требований для каждой категории. Ниже приведены некоторые дополнительные подробности.

По возможности, следует применять оборудование, имеющее документальное подтверждение надежной работы в прошлом в атомной промышленности и других отраслях экономики, имеющих аналогичные требования к оборудованию по стойкости к внешним воздействующим факторам.

7.2 Требования, относящиеся к функциям

7.2.1 Основные требования

Основные требования обеспечения функциональности — это наличие четких, всесторонних и однозначных функциональных требований и спецификаций проекта, на соответствие которым должны проверяться функции во время проектирования, изготовления, при аттестации, валидации, установке и эксплуатации и которые должны использоваться в качестве справочной информации для любых модификаций в процессе эксплуатации.

Надежность, требуемая от любой функции категорий А, В или С, следует определять либо с помощью количественной вероятностной оценки АС, либо с помощью качественного технического обоснования, и она должна быть включена в спецификацию. Эксплуатационные характеристики, требуемые от любой из функций категорий А, В или С, должны определяться соответствующим анализом и быть отражены в спецификации. Такие анализы должны проводиться структурировано в соответствии с рядом утвержденных процедур и должны быть документально оформлены.

Несмотря на то, что требования к надежности функций различных категорий могут быть идентичными, доверительный уровень того, что функция достигнет установленного уровня надежности, будет различным для трех категорий, при этом высший уровень обеспечения требуется для категории А.

Функции различных категорий должны быть разделены соответствующим образом.

7.2.2 Специфические требования

7.2.2.1 Категория А

Проектирование должно выполняться в соответствии с требованиями общепризнанных правил, руководств и стандартов, которые соответствуют высокому доверительному уровню функциональности, требующемуся для функций категории А. Проектирование должно быть направлено на облегчение верификации и валидации конечной функциональности путем поддержания простоты. Следовательно, следует избегать реализации в системах категории А, не относящихся к ним функций низших категорий (например, специальные расчеты для отображения данных на дисплее и трансляцию протоколов обмена не следует выполнять с помощью программного обеспечения системы безопасности).

Требования по надежности для функций контроля и управления категории А — согласно 7.1. Для этого должны быть установлены требования по надежности выполнения функций для достижения при-

емлемо низкого уровня риска возникновения недопустимых последствий, а затем на основании этих данных должны быть установлены требования по надежности для функции контроля и управления.

7.2.2.2 Категория В

Процесс проектирования должен выполняться в соответствии с принятыми правилами, руководствами и стандартами; могут применяться системы и оборудование с документально подтвержденной предысторией удовлетворительной работы в подобной области применения.

7.2.2.3 Категория С

Проект должен быть проанализирован для проверки того, что системы и оборудование рассчитаны или испытаны на обеспечение указанных функций в полном диапазоне условий эксплуатации, включая наименее благоприятные ожидаемые условия эксплуатации или ожидаемые при эксплуатации события, при которых требуется выполнение функции.

7.3 Требования, относящиеся к системам контроля и управления

7.3.1 Основные требования

Требования к проектированию системы должны обеспечивать достижение установленной надежности для функции. Основные требования по обеспечению высокой надежности касаются необходимого резервирования, разнообразия и пространственного, физического и электрического разделения и эффективного ИЧМ. Для всех систем должны быть предусмотрены средства обнаружения дефектов и ремонта во время проектирования и последующих модификаций.

При оценке надежности и готовности должны приниматься во внимание сроки ремонта, испытаний и технического обслуживания, а также вероятность самообнаруживающегося и несамообнаруживающегося отказов. Допущения, сделанные при проведении анализа безопасности в отношении сроков технического обслуживания, испытаний и ремонта, должны проверяться в процессе эксплуатации, и, если выявлены расхождения, должны быть выполнены действия по корректировке.

Специальные требования, касающиеся человеческого фактора и ИЧМ, должны быть включены в процесс проектирования. Данные требования следует определять по результатам осуществления технической программы анализа человеческого фактора, реализуемой на ранних этапах проектирования.

Проект системы должен предоставлять возможность проведения оперативного контроля и/или периодических испытаний в процессе эксплуатации с целью демонстрации поддержания эксплуатационных характеристик. Требования к периодическим испытаниям и мероприятиям по техническому обслуживанию с целью обеспечения долгосрочной надежности систем контроля и управления, важных для безопасности, определены в 7.5.

Предпочтительно, чтобы необходимое информационное и управляющее оборудование было размещено в одном месте, физически отделенном и электрически изолированном от главного пункта управления так, чтобы реактор мог быть переведен в режим безопасного останова и мог поддерживаться в этом режиме при контроле существенных параметров — в случае потери возможности выполнения этих функций на главном пункте управления.

7.3.2 Специфические требования

7.3.2.1 Категория А

Система контроля и управления, выполняющая функции категории А, должна обладать резервированием. Должны применяться необходимые виды разделения, чтобы постулируемая в проекте единичная угроза не могла вывести из строя резервные части системы. Единичный отказ не должен привести к отказу функции безопасности даже во время профилактического технического обслуживания, периодических испытаний, инспекции или ремонта. Применение критерия единичного отказа должно соответствовать Правилам МАГАТЭ NS-R-1, 5.34 — 5.39.

Примечание — При рассмотрении ненормального срабатывания функции контроля и управления обычно учитывают только те ложные срабатывания (единичные или множественные), которые могут быть результатом единичного отказа в подсистемах контроля и управления или вспомогательных системах.

В случае, когда функции категории А должны выполнять операторы, должны быть обеспечены системы контроля и управления, спроектированные «под задачу», отделенные от других систем контроля и управления и имеющие приемлемое время отклика.

Должна быть оценена и сопоставлена со спецификацией надежность систем контроля и управления, выполняющих функции категории А. При наличии отклонений они должны быть устранены. При оценке надежности должны учитываться результаты отказов по общей причине, включая отказы технического обеспечения, отказы программного обеспечения, отказы, связанные с ошибкой операторов во время эксплуатации, обслуживания, а также во время проведения модификации и ремонта. Способы оценки этих результатов варьируются от чисто качественной технической оценки до детальных коли-

чественных расчетов, которые сами могут зависеть от качественных оценок. Вид выбранного анализа должен соответствовать требованию по надежности, причем, чем выше требование по надежности, тем более строгая должна быть методика.

Если рассмотрение результатов отказов по общей причине показывает, что требуемая надежность не может быть достигнута для резервных систем, то необходимо использовать разнообразие, реализованное в независимых системах (например, в соответствии с тем, как это определено с помощью вероятностных критериев). Для этой функции могут потребоваться две или более подсистемы, независимые друг от друга. При выполнении функции категории А двумя или более независимыми системами, эти системы должны принадлежать к классу 1. Если желательно использовать системы низших классов, то по крайней мере одна из систем должна удовлетворять требованиям к системам класса 1, а для систем, не удовлетворяющих этим требованиям, должно быть представлено обоснование безопасности, позволяющее оценить приемлемость такого применения.

Примечание — Для отдельной системы, разработанной и спроектированной в соответствии с наивысшими критериями качества, ориентировочная вероятность отказа порядка 10^{-4} отказов на запрос может быть принята за обоснованный предел надежности, когда учтены все потенциальные источники отказов, обусловленные техническими характеристиками, проектом, изготовлением, установкой, рабочей средой и порядком обслуживания. Эта цифра включает в себя риск отказов общего характера в резервных каналах системы и относится ко всей системе, начиная с датчиков обработки данных и заканчивая выходами к задействованному оборудованию. Требования к более высокой надежности, чем указанные, допускаются, но необходимо их специальное обоснование с учетом всех упомянутых факторов. В качестве альтернативы может быть использовано проектирование независимых систем контроля и управления, важных для безопасности с приемлемым уровнем разнообразия.

Во время испытаний может потребоваться подавление выходных сигналов или обеспечение байпасной аппаратуры. Если байпасная аппаратура включена в систему, то необходимо обосновать ее работоспособность с целью демонстрации того, что аппаратуру нельзя применить таким образом, чтобы система не смогла выполнить предназначенные для нее функции безопасности. Например, использование аппаратуры в каждый отдельный момент времени может быть ограничено до одной ее группы, принадлежащей резервной системе.

Для некоторых систем может потребоваться дополнительное резервирование, чтобы обеспечить возможность проведения контрольных испытаний во время эксплуатации станции. Это необходимо, например, когда испытание активного канала не может быть проведено на мощности, а испытания должны проводиться во время эксплуатации станции с целью обеспечения требуемой функциональной надежности. В подобных случаях нет необходимости вводить дополнительное резервирование для всей системы.

Электропитание должно резервироваться дополнительными источниками питания.

Для систем категории А формальный анализ отказа системы, например анализ характера и последствий отказа, должен проводиться с целью определения уязвимости компонентов к отказам и оценки соответствия проектных стратегий, применяемых для выявления подобных отказов или смягчения их последствий.

Если система оснащена встроенными устройствами для самоконтроля и они учитываются в анализе надежности функции, то анализы характера и последствий отказов должны также рассматривать эти устройства для оценки охвата самотестирования. Если анализы характера и последствий отказов покажут, что некоторые отказы могут быть не зарегистрированы и не показаны оператору устройствами самоконтроля системы, то должны быть разработаны контрольные испытания для выявления таких отказов. Периодичность проведения контрольных испытаний должна определяться исходя из вероятной частоты возникновения незарегистрированного отказа и требований по надежности функции.

Там, где данные по надежности отсутствуют, периодичность испытаний может быть выбрана путем сравнения с подобной системой. По мере накопления опыта периодичность испытаний функции может быть определена повторно.

7.3.2.2 Категория В

Надежность систем, выполняющих функции контроля и управления категории В, должна быть оценена и сопоставлена со спецификацией. Функционирование систем данной категории должно быть обеспечено резервированием и разделением, если не представлено обоснование обратного. Подобное обоснование может основываться, например, на способности систем выполнять свои задачи по надежности без указанных мер, допустимости последствий отказа функции или достаточности времени, необходимого для обеспечения альтернативного реагирования в случае отказа функции.

Электропитание должно дублироваться дополнительными источниками питания.

Используемые в оборудовании компоненты должны быть высококачественными и надежными, должны быть обеспечены средствами для быстрого обнаружения и устранения дефектов.

Главные цели функционального проектирования систем, необходимых для обеспечения информации или возможностей управления в пункте управления и позволяющих выполнить определенные неавтоматические действия, требуемые для смягчения последствий ПС, состоят в предоставлении оператору точной, полной и своевременной информации в отношении состояния станционного оборудования и систем при любых ПС, а также в минимизации действий оператора при контроле станции и ее управлении.

Оперативный контроль и/или периодические испытания эксплуатационных характеристик должны включать в себя подтверждение функциональной способности подсистем в особенности при испытании отдельных резервных групп.

7.3.2.3 Категория С

Система данной категории обычно не нуждается в резервировании или разделении. В случае необходимости это может быть предусмотрено для того, чтобы функция достигла требуемого уровня надежности. Может потребоваться сохранение работоспособности при внутренних и внешних угрозах.

Электропитание должно дублироваться дополнительными источниками в зависимости от конкретной ситуации.

Для систем категории С, когда резервирование необходимо для достижения определенной надежности, должна быть оценена готовность, а резервирование должно рассматриваться так же, как для категории В.

Там, где предусмотрено резервирование, должны быть включены периодические индивидуальные испытания функциональности всех резервных систем или подсистем. Осуществление оперативного контроля позволяет выполнить настоящее требование.

7.4 Требования к оборудованию

7.4.1 Основные требования

Необходимо обеспечить безотказную работу оборудования под воздействием условий окружающей среды во время и после ПИС. Это обеспечение может быть достигнуто с помощью аттестации оборудования. Аттестация может быть проведена с помощью одного метода или с помощью комбинации из нескольких разных методов: например, с помощью испытаний, анализа, комбинации того и другого или на основе имеющегося опыта эксплуатации.

7.4.2 Специфичные требования

7.4.2.1 Категория А

Меры, принятые для обеспечения того, чтобы оборудование категории А продолжало функционировать при любых ожидаемых эксплуатационных условиях, должны включать в себя аттестацию оборудования. Результаты испытаний должны фиксироваться и храниться в архиве АС. Любые отказы при проведении аттестационных испытаний должны быть исследованы, а их причины и устранение документально подтверждены.

7.4.2.2 Категория В

Оборудование категории В должно пройти аттестацию, аналогичную той, что проводятся для оборудования категории А.

7.4.2.3 Категория С

Для оборудования категории С в зависимости от выполняемой функции может потребоваться проведение аттестации. Следует систематически проводить анализ проекта оборудования в отношении спецификации требований для наихудших внешних условий, в которых оборудование должно работать.

Если оборудование новое или должно работать в условиях, для которых промышленное оборудование, как правило, не проектируется (таких как землетрясения или экстремальные условия окружающей среды), необходимо установить свод правил для проектирования оборудования или оценки существующего проекта. Данные правила должны быть основаны на опыте, полученном из специальных требований к проектированию оборудования категории А. Оборудование, предназначенное для выполнения функций, к которым применяют критерии перечислений i) и j) 5.4.4, следует специально проектировать для тех экстремальных процессов и условий, которые, как это следует из проведенного анализа, могут возникнуть. Правомерность применения оборудования, выполненного в соответствии с общепромышленными стандартами, для выполнения данных функций должна быть подвержена специальному анализу.

В остальных случаях оборудование категории С может быть принято по обычным общепромышленным стандартам по проектированию, если назначение оборудования не требует специальной аттестации, например, в отношении требований по сейсмостойкости, нераспрстранению пожаров,

стойкости к воздействию колебаний напряжения, электрических шумов или по предотвращению воздействия перенапряжения, или электрических шумов в оборудовании категории С вследствие выполнения функций категорий А и В. Возможность работы в аномальных условиях окружающей среды подтверждают документами.

7.5 Требования, связанные с аспектами качества

7.5.1 Основные требования

Общие требования связаны с обеспечением качества на этапах проектирования, изготовления, установки, ввода в эксплуатацию и эксплуатации с целью обеспечения правильного функционирования соответствующих систем и оборудования.

Цель обеспечения качества — это управление конфигурацией, контроль изменений и отслеживаемость. Проект должен иметь достаточно подробную документацию для обеспечения этапов производства, установки, ввода в эксплуатацию и эксплуатации АС, а также для проведения верификации после каждого шага. Следует уделить должное внимание обеспечению документацией, чтобы допустить в будущем возможность модификации проекта.

Кроме того, специальные усилия по обеспечению качества и испытаниям должны быть предприняты для разработок новых проектов или модификаций, пропорциональные их относительной новизне или сложности. Эта деятельность должна подтверждаться документами в соответствии с важностью функций для безопасности.

Должен быть подготовлен план обеспечения качества в соответствии с определенными правилами или стандартами. Для этого необходимо определить и верифицировать спецификацию требований к эксплуатационным характеристикам и испытаниям.

Испытание компонентов, модулей, подсистем и систем должно проводиться в соответствии с планом обеспечения качества с целью демонстрации удовлетворительности эксплуатационных характеристик во время изготовления, сборки и установки на месте эксплуатации в соответствии с категорией функции.

Испытания компонентов, модулей и подсистем должны проводиться с целью обеспечения того, что наряду с обеспечением качества изготовления, функции выполняются в соответствии со спецификацией требований. Комбинированные испытания установленных систем контроля и управления с механическими и жидкостными системами должны проводиться до эксплуатации АС в режиме, при котором требуется готовность функций безопасности, обеспечиваемых системой.

Цель испытаний на месте эксплуатации является общей для всех категорий, но требования к управлению качеством и документации меняются в зависимости от категории, как это указано ниже.

Испытания в процессе эксплуатации должны проводиться с целью демонстрации того, что состояние компонентов технического обеспечения контроля и управления, важного для безопасности, не подвержено деградации по причине неисправностей. Системы контроля и управления должны быть спроектированы таким образом, чтобы имелась возможность проведения соответствующих испытаний и выявления отказов оборудования. Выявленные дефекты должны быть устранены в соответствии с процедурой управления модификацией. Необходимо сохранять соответствующие записи об этих исправлениях. Там, где обеспечивается резервирование, необходимо ввести целевые проверки функциональности резервных каналов. Промежуток между испытаниями должен быть выбран таким образом, чтобы оценка частоты отказа или вероятности отказа в работе по запросу отвечала требованиям анализа надежности.

Там, где применяется компьютерное оборудование, необходимо реализовать программу контроля качества жизненного цикла программного обеспечения, соответствующую категории функции.

7.5.2 Специфичные требования

7.5.2.1 Категория А

Требования к обеспечению качества должны соответствовать стандарту МАГАТЭ по безопасности GS-R-3. Документация должна давать возможность установить историю компонентов оборудования, включая проектирование, изготовление и аспекты эксплуатации. Это должно касаться всего оборудования в пределах проекта, вплоть до модульного уровня. Конфигурация должна контролироваться до отслеживаемого элемента самого низкого уровня. Отслеживаемость номеров партии, материалов и т.д. должна охватывать всю систему до отдельных модулей.

Документация по обеспечению качества должна позволять уполномоченному лицу проследить обратную связь от элемента оборудования или программного обеспечения до спецификации, которая

устанавливает требования к нему, а также прослеживать связь между любым требованием спецификации и компонентами, которые его осуществляют.

Типовые испытания должны проводиться с целью демонстрации того, что оборудование, идентичное по конструкции оборудованию, устанавливаемому на АС, будет функционировать в соответствии с требованиями проекта в ожидаемых условиях эксплуатации.

Должны проводиться функциональные испытания компонентов, модулей, подсистем и, если возможно, целых систем.

Функциональные испытания могут проводиться на предприятии-изготовителе или на месте эксплуатации. Испытания, проводимые на предприятии-изготовителе и на месте эксплуатации, должны быть скоординированы таким образом, чтобы вместе они обеспечивали полный охват. Если невозможно подтвердить охват всех установленных функций, то необходимо предоставить специальное обоснование.

Испытания на месте эксплуатации должны показать, насколько это практически достижимо, что все функции безопасности, определенные для установленных систем и оборудования, могут быть реализованы при требуемых эксплуатационных характеристиках. Данные испытания должны учитывать изменения параметров эксплуатации — это приемочные испытания на месте эксплуатации.

Оперативный контроль или периодические испытания должны демонстрировать отсутствие ухудшения способности выполнения всех требуемых функций безопасности, включая все подсистемы, необходимые для выполнения этих функций. Промежутки между испытаниями должны определяться в зависимости от уровня самоконтроля таким образом, чтобы показатели надежности для функций контроля и управления, важных для безопасности, выполнялись с учетом ожидаемой или контролируемой частоты отказов компонентов контроля и управления.

7.5.2.2 Категория В

Требования к обеспечению качества должны соответствовать стандарту МАГАТЭ по безопасности GS-R-3. Документация должна давать возможность установить историю компонентов оборудования, включая проектирование, изготовление и аспекты эксплуатации. Степень детализации, с которой обеспечение качества применяется к функциям, системам или оборудованию категории В, может быть ниже той степени, которая применяется к функциям, системам или оборудованию категории А, хотя программа обеспечения качества должна быть согласована с программой для категории А.

Оборудование, сходное по конструкции с устанавливаемым на АС оборудованием, должно пройти типовые испытания с проведением анализа, подтверждающего, что различия в оборудовании не сводят на нет результаты испытаний.

До начала эксплуатации должны быть проведены функциональные испытания с целью демонстрации того, что каждая конкретная функция может быть реализована системой, использующей оборудование, конструкция которого аналогична конструкции оборудования, устанавливаемого на АС. Часть или все испытания могут быть проведены на месте эксплуатации.

Приемочные испытания на месте эксплуатации должны продемонстрировать, насколько это практически достижимо, что все определенные для установленного оборудования функции безопасности могут быть реализованы. Испытания управляющего оборудования должны продемонстрировать способность правильно реагировать на переходные режимы и изменения по запросу. Испытания сигнально-аварийного оборудования должны включать в себя испытание с использованием соответствующих входных сигналов с целью демонстрации удовлетворительных эксплуатационных характеристик.

7.5.2.3 Категория С

Системы и оборудование категории С могут быть приняты с общепромышленным уровнем обеспечения качества.

Лицензиат может признать испытания производителя достаточными для демонстрации достижения установленных эксплуатационных характеристик. Данные испытания должны проводиться на аналогичном оборудовании. Специальные типовые и функциональные испытания должны проводиться при необходимости, но в общем случае не являются обязательными.

Приемочные испытания на месте эксплуатации должны проводиться с целью демонстрации того, что системы достигают установленные в отношении безопасности уровни функциональности и эксплуатационных характеристик.

Периодические испытания эксплуатационных характеристик для функций, не находящихся непрерывно в работе, могут быть ограничены проверками во время перезагрузки топлива или в других подобных периодах простоя.

Таблица 1 — Табличное представление взаимосвязи категорий с другими стандартами МЭК

Категория	Применяемые стандарты МЭК на		Основные требования для			
	системы	оборудование	функций	проекта систем	характеристик оборудования	общих вопросов
Общая	МЭК 61513, МЭК 60964, МЭК 60965, МЭК 61771, МЭК 61772, МЭК 61839, МЭК 60709	МЭК 61000-4, МЭК 61000-6-2	Функциональная спецификация	Контролируемость. Спецификации ИЧМ	Электромагнитная совместимость	Программа ОК. Управление качеством. Заводские приемочные испытания. Приемочные испытания на месте установки. Периодические испытания
A	МЭК 60812[5], МЭК 60880, МЭК 60987	МЭК 60780, МЭК 60980	Соответствующие правила, стандарты, руководства. Отделение от более низких категорий. Высокий уровень надежности	Критерий единичного отказа. Независимость, разделение. Проект защиты от внутреннего отказа по общей причине. Диверсификация, определяемая отдельно для каждого случая. Анализ характера и последствий отказа. Дублирующее электропитание	Аттестация на заданные условия окружающей среды и сейсмические условия	МАГАТЭ GS-R-3. Верификация на идентичном оборудовании. Комплексные приемочные испытания заводские/на месте установки. Частые периодические испытания
B	МЭК 60987, МЭК 62138	МЭК 60780, МЭК 60980	Соответствующие правила, стандарты, руководства. Отделение от более низких категорий	Критерий единичного отказа, разделение, по возможности, на функциональном уровне. Дублирующее электропитание	Аттестация на заданные условия окружающей среды и сейсмические условия, которые должно выдерживать оборудование	МАГАТЭ GS-R-3. Верификация на аналогичном оборудовании. Ограниченные приемочные испытания на месте установки и периодические испытания
C	МЭК 62138			Резервирование и разделение, определяемые отдельно для каждого случая	Аттестация, определяемая отдельно для каждого случая	Промышленный опыт штатного применения. Периодические испытания, если оборудование не используется постоянно

[5] Если анализом отказов является анализ характера и последствий отказа.

Приложение А
(справочное)

Примеры и категории

А.1 Общие положения

В данном приложении приведены примеры типичных функций и типичного оборудования категорий А, В и С. Следует отметить, что эти примеры необязательно могут быть применимы для всех типов реакторов.

А.2 Категория А

А.2.1 Типичные функции

Функции, относящиеся к категории А, необходимые для контроля и управления:

a) останова реактора и поддержания подкритичности;

b) изоляции защитной оболочки;

c) предоставления информации, необходимой для действий оператора;

d) отвода тепла на конечный теплообменник.

А.2.2 Типичные системы контроля и управления

К типичным системам контроля и управления относятся:

a) система управления и защиты реактора;

b) система аварийной и предупредительной защиты и вспомогательное оборудование системы;

c) основная аппаратура и дисплеи, обеспечивающие выполнение оператором предписанных действий, описанных в инструкциях по эксплуатации АС и необходимых для обеспечения в короткие сроки безопасности станции.

А.3 Категория В

А.3.1 Типичные функции

Функции контроля и управления, относящиеся к категории В, необходимые:

a) для охлаждения бассейна выдержки топлива;

b) для контура;

c) для системы послеаварийного мониторинга;

d) для автоматического управления состоянием первого и второго контуров АС, поддержания значений параметров в пределах, допустимых в анализе безопасности, а также предотвращения развития событий до уровня аварий;

e) для контроля/управления системы обращения с топливом в случаях, когда отказ может привести к радиоактивному выбросу или повреждению топлива, выходящими за пределы и условия нормальной эксплуатации.

А.3.2 Типичные системы контроля и управления

К типичным системам контроля и управления относят:

a) систему автоматического управления АС или систему превентивной защиты;

b) часть системы отвода остаточного тепла на конечный теплосъемник, не востребованный в краткосрочной перспективе;

c) аппаратуру, необходимую для применения оперативных процедур при ПС;

d) контуры безопасности и защитную блокировку системы обращения с топливом, применяемые при остановке реактора.

А.4 Категория С

А.4.1 Типичные функции

Функции контроля и управления, относящиеся к категории С, могут включать в себя:

a) контроль и управление эксплуатационными характеристиками отдельных систем и компонентов оборудования во время послеаварийного этапа с целью получения своевременного предупреждения о предстоящих сбоях, а также поддержания уровня радиоактивных выбросов на практически достижимом низком уровне;

b) ограничение последствий внутренних угроз;

c) функции, ошибки в работе которых могут привести к незначительным радиоактивным выбросам или создать радиоактивную угрозу для персонала АС;

d) функции, необходимые для предупреждения о внутренних или внешних угрозах (пожар, наводнение, взрывы, землетрясения и т.д.);

e) системы управления доступом;

f) системы оперативной связи для предупреждения о значительных выбросах на территории АС или вне ее территории с целью выполнения плана аварийной защиты АС.

А.4.2 Типичные системы контроля и управления

К типичным системам контроля и управления относят:

a) системы сигнализации;

b) системы блокировки и контроля потока радиоактивных отходов, система радиационного мониторинга территории;

c) система контроля доступа;

d) система аварийной связи;

e) система обработки данных пункта управления;

f) система пожаротушения;

g) система сейсмического контроля;

h) метеорологическая станция на площадке АС.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60671:2007	—	*
МЭК 60709	IDT	ГОСТ Р МЭК 60709—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
МЭК 60780	—	*
МЭК 60812	—	*
МЭК 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»
МЭК 60964	—	*
МЭК 60965	—	*
МЭК 60980	—	*
МЭК 60987	—	*
МЭК 61513	IDT	ГОСТ Р МЭК 61513–2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
МЭК 61771	—	*
МЭК 61772	—	*
МЭК 61839	—	*
МЭК 62138	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»

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

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

- IDT — идентичные стандарты.

Библиография

[1] МЭК 60050-394 — Международный электротехнический словарь. Часть 394. Ядерное приборостроение. Аппаратура, системы, оборудование и детекторы (IEC 60050-394 International Electrotechnical Vocabulary — Part 394: Nuclear Instrumentation — Instruments, systems, equipment and detectors)

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

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

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

[5] МЭК/ТО 61838 — Атомные станции. Контроль и управление, важные для безопасности. Использование вероятностных оценок безопасности для классификации функций (IEC/TR 61838, Nuclear power plants — Instrumentation and control important to safety — Use of probabilistic safety assessment for the classification of functions)

[6] Глоссарий МАГАТЭ по вопросам безопасности: 2007 — Терминология, используемая в области ядерной безопасности и радиационной защиты (IAEA Safety Glossary:2007, Terminology used in nuclear safety and radiation protection)

УДК 621.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; постулированное исходное событие; системы контроля и управления, важные для безопасности; категории функций безопасности; жизненный цикл; верификация; валидация; резервирование

Редактор *Р.Г. Говердовская*
Технический редактор *Н.С. Гришанова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 08.11.2011. Подписано в печать 06.12.2011. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,85. Тираж 94 экз. Зак. 1185.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru