ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61513 — 2011

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Общие требования

IEC 61513:2001
Nuclear power plants —
Instrumentation and control important to safety —
General requirements for systems
(IDT)

Издание официальное

Москва
Стандартинформ
2012

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, выполненного российской комиссией экспертов МЭК/ТК 45, 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 28 сентября 2011 г. № 377-ст

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

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, 2012

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 Применение: новые и существующие атомные станции . . . 1
1.3 Структура . . . 1
2 Нормативные ссылки . . . 3
3 Термины и определения . . . 5
4 Обозначения и сокращения . . . 13
5 Полный жизненный цикл безопасности контроля и управления . . . 13
5.1 Определение требований к контролю и управлению на основе технического проекта АСУТП АС 16
5.2 Выходная документация . . . 19
5.3 Проект полной архитектуры и распределения функций контроля и управления . . . 19
5.4 Общее планирование . . . 25
5.5 Выходная документация . . . 28
6 Жизненный цикл безопасности системы . . . 29
6.1 Требования . . . 32
6.2 Планирование системы . . . 41
6.3 Выходная документация . . . 45
6.4 Квалификация системы . . . 49
6.5 Сводка наиболее важных специальных требований к различным классам и категориям . . . 53
7 Общая интеграция и приемка . . . 54
7.1 Требования, необходимые для достижения результата . . . 54
7.2 Выходная документация . . . 54
8 Общая эксплуатация и обслуживание . . . 54
8.1 Требования, необходимые для достижения результата . . . 55
8.2 Выходная документация . . . 55
Приложение А (справочное) Основные вопросы безопасности АС . . . 56
Приложение В (справочное) Категоризация функций и классификация систем . . . 58
Приложение С (справочное) Качественное рассмотрение защиты от отказов по общей причине . . . 62
Приложение D (справочное) Связь МЭК 61508 с МЭК 61513 и стандартами атомной отрасли . . . 66
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 74
Библиография . . . 76

Введение

Настоящий стандарт устанавливает требования к системам контроля и управления и их оборудованию, которые предназначены для выполнения функций, важных для безопасности АС.

В настоящем стандарте рассматриваются взаимосвязи между:

- задачами обеспечения безопасности АС и требованиями к общей архитектуре систем контроля и управления, важных для безопасности;
- общей архитектурой систем контроля и управления и требованиями отдельных систем, важных для безопасности.

Взаимосвязь с другими стандартами

При разработке настоящего стандарта использованы международные стандарты Международной организации по стандартизации (ИСО), Международной электротехнической комиссии (МЭК), документы Международного агентства по атомной энергии (МАГАТЭ) и другие документы. Наиболее важные из них:

a) стандарты МЭК в области ядерной технологии.

Настоящий стандарт опирается на другие стандарты МЭК в области ядерной технологии, в частности на те из них, которые посвящены квалификации, проектированию щита управления, категоризации функций и классификации систем (см. 3.4 и 3.6) и мультиплексированию.

При рассмотрении компьютеризированных систем класса 1 (см. 5.1.2.1 и приложение В) настоящий стандарт следует применять совместно с МЭК 60880, МЭК 60880-2 и МЭК 60987, чтобы полностью удовлетворить требования к аппаратуре и программному обеспечению;

b) другие международные стандарты.

В настоящем стандарте принят формат изложения базовой публикации по безопасности МЭК 61508 с использованием понятий «полного жизненного цикла безопасности» и «жизненного цикла системы». В настоящем стандарте также приведена интерпретация общих требований частей 1, 2 и 4 МЭК 61508 применительно к области ядерной технологии. Соответствие требованиям настоящего стандарта будет способствовать согласованности с требованиями МЭК 61508 в тех случаях, когда они применяются в ядерной технологии.

Настоящий стандарт содержит ссылки на стандарты ИСО по вопросам, которые связаны с обеспечением качества;

c) документы МАГАТЭ серии безопасности.

Настоящий стандарт разработан в соответствии с принципами и основными направлениями Программы МАГАТЭ по безопасности атомных электростанций и руководствами по безопасности МАГАТЭ. На самом деле документы МАГАТЭ применимы ко всем стандартам ТК 45 в области контроля и управления. Термины и определения, применяемые в настоящем стандарте, согласованы с теми, которые используются МАГАТЭ (см. примечание).

Примечание — В соответствии с «Соглашением о сотрудничестве в областях, представляющих общий интерес», май 1981 г.

Настоящий стандарт содержит ссылки на МАГАТЭ 50-C-QA (Изм. 1) в разделах, связанных с обеспечением качества.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Общие требования

Nuclear power plants.
Instrumentation and control important to safety.
General requirements for systems

Дата введения — 2012 — 01— 01

1 Область применения

1.1 Общие положения

Системы контроля и управления (СКУ), важные для безопасности атомных станций, могут быть построены на традиционном оборудовании с жесткими связями, оборудовании, основанном на применении компьютерной технологии или с использованием комбинации оборудования обоих типов. Настоящий стандарт устанавливает требования и рекомендации (см. примечание) для общей архитектуры системы контроля и управления, которая может быть построена с использованием указанных технологий.

Примечание — Далее термин «требования» обозначает как собственно требования, так и рекомендации. Различие появляется на уровне особых условий, когда термин «требования» обозначает необходимость, а термин «рекомендации» — желательность.

В настоящем стандарте придается большое значение полноте и точности требований, вытекающих из целей, связанных с безопасностью атомной станции, как к исходным данным для выработки всесторонних требований к полной архитектуре системы контроля и управления в целом, так и к отдельным системам контроля и управления, важным для безопасности.

В настоящем стандарте вводится понятие «концепция жизненного цикла безопасности» для всей архитектуры системы контроля и управления в целом и каждой системы в отдельности. Жизненные циклы безопасности, представленные и рассмотренные в настоящем стандарте, не являются единственно возможными; могут применяться и другие жизненные циклы, если будут достигнуты цели, заявленные в настоящем стандарте.

1.2 Применение: новые и существующие атомные станции

Требования настоящего стандарта применимы как к системам контроля и управления на новых атомных станциях, так и к реконструируемым и модернизируемым системам на действующих АС.

Для действующих станций используется частичный набор требований, объем которых устанавливают перед началом разработки любого проекта.

1.3 Структура

Общая структура настоящего стандарта с указанием соответствующих разделов представлена на рисунке 1.

Издание официальное

Спецификация требований к функциям, системам и оборудованию контроля и управления, важным для безопасности, на основе проекта безопасности атомной станции
5.1 и 5.2

5.1 Требования, устанавливаемые на основе проекта безопасности атомной станции	5.2 Требования к выходной документации
5.1 1 Требования к функциям, характеристикам и независимости 5.1.2 Требования к категоризации 5.1.3 Ограничения	Общая спецификация требований к функциям и оборудованию систем контроля и управления, важным для безопасности

Проектирование и планирование полной архитектуры контроля и управления и назначение функций для каждой из систем контроля и управления
5.3 – 5.5

5.3 Требования к целям	5.4 Требования к общему планированию	5.5 Требования к документации
5.3.1 Проектирование архитектуры контроля и управления 5.3.2 Назначение функций отдельных систем 5.3 3 Анализ	5.4.1 Общая программа обеспечения качества 5 4.2 Общий план защищенности 5.4.3 Общий план интеграции и приемки 5 4 4 Общий план эксплуатации 5.4.5 Общий план обслуживания	5.5.1 Структурная схема архитектуры 5.5 2 Функциональная схема

6. Реализация и проектирование отдельных систем контроля и управления

6.1 Требования к целям на фазах жизненного цикла системы	6.2 Требования к планированию системы	6.3 Требования к документации
6.1 1 Спецификация требований 6.1.2 Спецификация 6.2.3 Детальный проект 6.2.4 Интеграция 6.1 5 Валидация 6.1 6 Внедрение 6.1.7 Модификация	6.2.1 Программа качества 6.2.2 План защищенности 6 2 3 План интеграции 6.2.4 План валидации 6.2.5 План внедрения 6 2.6 План эксплуатации 6 2 7 План обслуживания	6.3.1 Спецификация требований 6.3 2 Спецификации 6.3.3 Детальный проект 6.3 4 Интеграция 6.3 5 Наладка 6.3.6 Модификация

6.4 Квалификация

6.4 1, 6.4.2, 6.4.3 Требования к квалификации системы	6.4 4 Требования к квалификации документации

6.5 Перечень основных специфических требований

7 Общие интеграция и приемка

7.1 Требования к целям	7.2 Требования к выходной документации

8 Общие эксплуатация и обслуживание

8.1. Требования к целям	8.2 Требования к выходной документации

Рисунок 1 — Общая структура настоящего стандарта

- раздел 5 посвящен полной архитектуре систем контроля и управления, важных для безопасности, в том числе:

определению требований к функциям контроля и управления и соответствующим системам и оборудованию, которые устанавливаются исходя из результатов анализа безопасности АС, категоризации функций контроля и управления, а также условий размещения и эксплуатации АС,

структурированию полной архитектуры контроля и управления с разделением на ряд систем и указанием функций контроля и управления для каждой системы, а также определению критериев проектирования, включая обеспечивающие глубокоэшелонированную защиту и минимизацию вероятности отказа по общей причине,

планированию полной архитектуры систем контроля и управления;

- раздел 6 посвящен требованиям к отдельным системам контроля и управления, важным для безопасности, в частности, требованиям к системам на основе компьютеров;

- разделы 7 и 8 посвящены общей интеграции, приемке, эксплуатации и обслуживанию систем контроля и управления;

- приложение А показывает связь между требованиями МАГАТЭ и основными положениями по безопасности, используемыми в настоящем стандарте;

- приложение В содержит информацию о принципах категоризации и классификации;

- приложение С содержит примеры чувствительности систем контроля и управления к отказам по общей причине;

- приложение D содержит сопоставление МЭК 61513 с частями 1; 2 и 4 МЭК 61508. Данное приложение представляет основные требования МЭК 61508 с целью подтверждения того, что разделы, относящиеся к безопасности, отражены адекватно, в приложении D используются общие термины и разъясняются причины, по которым выбраны другие или дополнительные методы или термины.

2 Нормативные ссылки

Положения нижеследующих нормативных документов, в случае ссылки на них в данном тексте, являются положениями настоящего международного стандарта. Если в документах, на которые даны ссылки, указана дата, то никакие последующие корректировки или пересмотры этих публикаций не применимы. Однако сторонам, вступающим в соглашения на основе данного международного стандарта, рекомендуется исследовать применимость самых поздних изданий приведенных ниже нормативных документов. Если дата не указана, то применяется последнее издание нормативного документа, на который дана ссылка. Члены МЭК и ИСО составляют реестры действующих в настоящее время международных стандартов.

МЭК 60709:1981 Разделение внутри системы защиты реактора (IEC 60709:1981 Separation within the reactor protection system)

МЭК 60780:1984 Атомные станции. Электрооборудование систем безопасности. Квалификация (IEC 60780:1984 Nuclear power plants — Electrical equipment of the safety system — Qualification)

МЭК 60880:1986 Программное обеспечение компьютеров систем безопасности атомных электростанций (IEC 60880:1986 Software for the computers in the safety systems of nuclear power station)

МЭК 60880-2:2000 Программное обеспечение компьютеров в системах, важных для безопасности атомных электростанций. Часть 2: Программные аспекты защиты от отказов по общей причине, использование программных инструментов и ранее разработанного программного обеспечения (IEC 60880-2:2000 Software for computers important to safety for nuclear power plants — Part 2: Software aspects of defence against common cause failures, use of software tools and of pre-developed software)

МЭК 60964:1989 Проектирование щитов управления атомных станций (IEC 60964:1989 Design for control rooms of nuclear power plants)

МЭК 60965:1989 Дополнительные пункты управления остановкой реактора без допуска на блочный щит управления (IEC 60965:1989 Supplementary control points for reactor shutdown without access to the main control room)

МЭК 60987:1989 Программируемые цифровые компьютеры, важные для безопасности атомных станций (IEC 60987:1989 Programmed digital computers important to safety for nuclear power stations)

МЭК 61000-4-1:2000 Электромагнитная совместимость (ЭМС). Часть 4-1: Методы испытаний и измерений. Обзор серии стандартов МЭК 61000-4 (IEC 61000-4-1:2000 Electromagnetic compatibility (EMC) — Part 4-1: Testing and measurement techniques — Overview of IEC 61000-4 series)

МЭК 61000-4-2:1995 Электромагнитная совместимость (ЭМС). Часть 4: Методы испытаний и измерений. Раздел 2: Испытания на помехозащищенность при электростатическом разряде. Базовая публикация

по ЭМС (IEC 61000-4-2:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 2: Electrostatic discharge immunity test. Basic EMS Publication)

МЭК 61000-4-3:1995 Электромагнитная совместимость (ЭМС). Часть 4: Методы испытаний и измерений. Раздел 3: Помехозащищенность при воздействии радиационного, радиочастотного и электромагнитного полей (IEC 61000-4-3:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 3: Radiated, radio-frequency, electromagnetic field immunity)

МЭК 61000-4-4:1995 Электромагнитная совместимость (ЭМС). Часть 4: Методы испытаний и измерений. Раздел 4: Испытания на помехозащищенность от быстрых переходных процессов и всплесков. Базовая публикация по ЭМС (IEC 61000-4-4:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 4: Electrical fast transient/burst immunity test. Basic EMS Publication)

МЭК 61000-4-5:1995 Электромагнитная совместимость (ЭМС). Часть 4: Методы испытаний и измерений. Раздел 5: Помехозащищенность от перенапряжения (IEC 61000-4-5:1995 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 5: Surge immunity test)

МЭК 61000-4-6:1996 Электромагнитная совместимость (ЭМС). Часть 4: Методы испытаний и измерений. Раздел 6: Помехозащищенность от возмущений, вызванных воздействием радиочастотных полей (IEC 61000-4-6:1996 Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques — Section 6: Immunity to conducted disturbances, induced by radio-frequency fields)

МЭК 61069-1:1991 Измерения и управление промышленными процессами. Оценка свойств системы при ее всесторонней оценке. Часть 1: Основные подходы и методология (IEC 61069-1:1991 Industrial-process measurement and control — Evaluation of system properties for the purpose of system assessment — Part 1. General considerations and methodology)

МЭК 61226:1993 Атомные станции. Системы контроля и управления, важные для безопасности. Классификация (IEC 61226:1993 Nuclear power plants — Instrumentation and control systems important for safety — Classification)

МЭК 61500:1996 Атомные станции. Системы контроля и управления, важные для безопасности. Функциональные требования и передача мультиплексных данных (IEC 61500:1996 Nuclear power plant – Instrumentation and control systems important for safety — Functional requirement for multiplexed data transmission)

МЭК 61508-1:1998 Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 1: Общие требования (IEC 61508-1:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements)

МЭК 61508-2:2000 Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 2: Требования к электрическим/электронным/программируемым электронным системам, связанным с безопасностью (IEC 61508-2:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems)

МЭК 61508-4:1998 Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 4: Определения и сокращения (IEC 61508-4:1998 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations)

ИСО/МЭК 12207:1995 Информационная технология. Процессы жизненного цикла программного обеспечения (ISO/IEC 12207:1995 Information technology — Software life cycle processes)

ИСО 8402:1994 Управление и обеспечение качества. Словарь (ISO 8402:1994 Quality management and quality assurance — Vocabulary)

ИСО 9000-3:1997 Стандарты по управлению и обеспечению качества. Часто 3: Руководство по применению стандарта ИСО 9001 при разработке, поставке, установке и обслуживании (ISO 9000-3:1997 Quality management and quality assurance standards — Part 3: Guidelines for the application of ISO 9001 to the development, supply, installation and servicing)

ИСО 9001:1994 Системы качества. Модель обеспечения качества при проектировании, разработке, производстве, установке и обслуживании (ISO 9001:1994 Quality systems — Model for quality assurance in design, development, production, installation and servicing)

МАГАТЭ 50-С-D (Редакция 1):1988 Правила безопасности АС: Проектирование (IAEA Safety Series 50-C-D (Rev 1):1988, Code on the Safety of NPPs — Design)

МАГАТЭ 50-С-QA (Редакция 1):1988 Правила безопасности АС: Обеспечение качества (IAEA Safety Series 50-C-QA (Rev 1):1988, Code on the Safety of NPPs — Quality assurance)

МАГАТЭ 50-SG-D1:1979 Руководство по безопасности. Классификация функций и компонент безопасности для BWR, PWR и PTR (IAEA Safety Series 50-SG-D1:1979, Safety function and Component Classification for BWR, PWR and PTR — A Safety Guide)

МАГАТЭ 50-SG-D3:1980 Руководство по безопасности. Система защиты и связанные с ней элементы АС (IAEA Safety Series 50-SG-D3:1980, Protection system and related features in NPPs — A Safety Guide)

МАГАТЭ 50-SG-D8:1984 Руководство по безопасности. Системы контроля и управления для АС, связанные с безопасностью (IAEA Safety Series 50-SG-D8:1984, Safety-Related Instrumentation and Control Systems for NPPs — A Safety Guide)

МАГАТЭ 50-SG-D11:1986 Руководство по безопасности Основные принципы проектирования АС (IAEA Safety Series 50-SG-D11:1986, General Design Safety Principles for NPPs — A Safety Guide)

МАГАТЭ 75-INSAG-3:1988 Основные принципы безопасности АС (IAEA Safety Series 75-INSAG-3:1988, Basic Safety Principles for NPPs)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **прикладная функция** (application function): Функция системы контроля и управления по выполнению задачи, связанной с контролируемым процессом, а не с функционированием самой системы.

[МЭК 60880, пункт 2.1, модифицировано]

Примечание 1 — См. также «функция контроля и управления», «система контроля и управления», «прикладное программное обеспечение».

Примечание 2 — Прикладная функция является обычно одной из функций контроля и управления.

3.2 **прикладное программное обеспечение** (application software): Часть программного обеспечения системы контроля и управления, которое обеспечивает выполнение прикладных функций (см. рисунок 2).

Примечание 1 — См. также «прикладная функция», «библиотека прикладных программ», «системное программное обеспечение системы».

Примечание 2 — Прикладное программное обеспечение отличается от системного.

3.3 **библиотека прикладных программ** (application software library): Собрание программных модулей, предназначенных для выполнения типовых прикладных функций (см. рисунок 2).

Примечание — При использовании существующего оборудования такая библиотека рассматривается как часть системного программного обеспечения и квалифицируется соответствующим образом.

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

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

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

3.5 **канал** (channel): Ряд взаимосвязанных компонентов внутри системы, которые формируют один выходной сигнал. Канал теряет свою индивидуальность, если его выходные сигналы сочетаются с сигналами от другого канала, например, канала контроля или канала безопасности.

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

Примечание — См. также «категории функций, важных для безопасности», «элементы, важные для безопасности», «системы безопасности».

3.7 **отказ по общей причине (ОПП)** (common cause failure — CCF): Отказ, явившийся результатом одного или более событий, вызывающих одновременный отказ двух или более отдельных каналов многоканальной системы или многоканальных систем и приводящий к отказу системы (систем).

[МЭК 61508-4 пункт 3.6.10, модифицировано]

Примечание — В зависимости от контекста отказ по общей причине может рассматриваться на уровне системы или на уровне нескольких систем, образующих комплекс безопасности.

3.8 **сложность** (complexity). Свойство системы или компонента, имеющих устройство, исполнение или поведение, трудные для понимания или верификации.

[IEEE 610, модифицировано] [1]

3.9 **компонент** (component): Одна из частей, из которых состоит система; компонент может представлять собой часть оборудования или программного обеспечения и может сам состоять из других компонентов.

[IEEE 610] [1]

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

Примечание 2 — Термины «оборудование», «компонента» и «модуль» часто используют как взаимозаменяемые. Отношение между этими терминами пока не стандартизовано.

3.10 **компьютерная система** (computer-based system): Система контроля и управления, функции которой в большой степени зависят или полностью выполняются с использованием микропроцессоров, программируемого электронного оборудования или компьютеров (см. рисунок 2).

Примечание — См. также «система контроля и управления».

3.11 **приемка на АС** (commissioning of the NPP): Процесс, при котором собранные компоненты и системы вводятся в действие, верифицируются (подвергаются испытаниям) на соответствие техническим требованиям и характеристикам назначения; они могут включать в себя испытания как с применением радиоактивных и ядерных материалов и излучений, так и без них.

[МАГАТЭ 50-S-D]

3.12 **управление конфигурацией** (configuration management): Порядок применения технической и административной директивы и контроля с целью определения и документирования функциональных и физических характеристик сложного устройства, управления изменением таких характеристик, ведения записей и отчетов об изменении в работе и настройке, а также проверки соответствия определенным требованиям.

[IEEE 610] [1]

3.13 **данные** (data): Представление информации или сообщений в виде, подходящем для передачи, интерпретации или обработки с помощью компьютеров (см. рисунок 2).

[IEEE 610, модифицировано] [1]

3.14 **концепция глубокоэшелонированной защиты** (defence-in-depth concept): (см. А.3 приложения А).

3.15 **детерминистический метод** (deterministic method): См. А.2.2 приложения А.

3.16 **разнообразие** (diversity): 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.

[МЭК 60880-2, пункт 3.6]

Примечание 1 — См. также «функциональное разнообразие».

Примечание 2 — Это определение шире, чем использованное в МАГАТЭ 50-C-D: «существование избыточных компонентов или систем с целью выполнения определенной функции, когда такие компоненты или системы совместно несут в себе одну или более различных характеристик. Например, такие характеристики, как различные условия работы, размеры оборудования, производители, принципы функционирования и типы оборудования, использующие различные физические методы».

3.17 **оборудование** (equipment): Одна или более частей системы. Элемент оборудования — отдельная (обычно заменяемая) часть системы.

[МЭК 61226, модифицировано]

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

Примечание 2 — Оборудование может включать в себя программное обеспечение.

Примечание 3 — Термины «оборудование», «компонент» и «модуль» часто применяют как синонимы. Отношение между ними пока не стандартизованы.

3.18 **комплекс оборудования** (equipment family): Набор приборных и программных компонентов, которые могут работать совместно в одной или более определенных структурах (конфигурациях). Разработка специальной конфигурации для АС и соответствующего прикладного программного обеспечения может поддерживаться программными средствами. Комплекс оборудования обеспечивает набор стандартных операций (библиотеку прикладных функций), которые могут быть объединены, образуя специальное прикладное программное обеспечение.

Примечание 1 — См. также «функциональность», «прикладное программное обеспечение», «библиотека прикладных программ».

Примечание 2 — Линейка оборудования может быть как продуктом от определенного поставщика, так и набором изделий, соединение и адаптация которых выполнены поставщиком.

Примечание 3 — Иногда в качестве синонима термину «линейка оборудования» используют термин «приборная (аппаратная) платформа».

3.19 **погрешность** (error): Расхождение между рассчитанным, наблюдаемым или измеренным значениями величины или условиями и истинным, установленным или теоретическим значениями величины или условий (см. рисунок 3).

3.20 **оценка** (свойства системы) (evaluation of a system property): Приписывание качественного или количественного значения данному свойству системы.

[МЭК 61069-1, пункт 2.2.2]

3.21 **отказ** (failure): Отклонение реального функционирования от запланированного (см. рисунок 3).

[МЭК 60880-2, пункт 3.8]

Примечание 1 — Отказ является результатом сбоя в аппаратуре, программном обеспечении, системе или ошибки оператора или обслуживания и отражается на прохождении сигнала.

Примечание 2 — См. также «дефект», «отказ программного обеспечения».

3.22 **дефект** (fault): Дефект в аппаратуре, программном обеспечении или в компоненте системы (см. рисунок 3).

Примечание 1 — Дефекты могут быть результатом случайных отказов, которые возникают, например, из-за деградации аппаратуры в результате старения; возможны систематические дефекты, например, в результате дефектов в программном обеспечении, возникающих из-за ошибок при проектировании.

Примечание 2 — Дефект (особенно дефекты, связанные с проектированием) может оставаться незамеченным, пока сохраняются условия, при которых он не отражается на выполнении функции, т.е. пока не произойдет отказ.

Примечание 3 — См. также «дефект программного обеспечения».

3.23 **функциональное разнообразие** (functional diversity): Применение разнообразия на функциональном уровне (например, при достижении предельных значений как давления, так и температуры).

[МЭК 61069-1, пункт 2.2.2]

Примечание — См. также «разнообразие».

3.24 **функциональная валидация** (functional validation): Проверка правильности применения спецификаций прикладных функций относительно исходных требований к функциям и эксплуатационным характеристикам станции. Функциональная валидация дополняет валидацию системы и оценивает ее соответствие спецификации функций.

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

Примечание — Выполнение прикладных функций определяющим образом влияет на работу АС. Входная информация может поступать от датчиков, блоков обработки, другого оборудования или другого программного комплекса. Выходная информация может воздействовать на исполнительные механизмы, блоки обработки, другое оборудование и другое программное обеспечение (см. [4]).

3.26 **функция,** важная для безопасности (function important to safety): Особая цель, которая должна способствовать безопасности.

[МАГАТЭ 50-SG-D3 и МЭК 61226, модифицировано]

Примечание — См. также «функция контроля и управления», «подфункция контроля и управления», «прикладная функция».

3.27 **опасность** (hazard): Событие, способное причинить вред здоровью персонала АС, привести к повреждению узлов, оборудования или строительных конструкций. Опасности подразделяются на внутренние и внешние.

Примечание 1 — Внутренние опасности представляют собой, например, пожар и затопление. Внутренние опасности могут являться последствиями постулированных исходных событий.

Примечание 2 — Примером внешних опасностей может служить землетрясение или удар молнии.

3.28 **ошибка персонала** (human error or mistake): Отдельное действие персонала или процедура, которые приводят к непредвиденному результату.

3.29 **независимое оборудование** (independent equipment): Оборудование, которое обладает двумя следующими характеристиками:

a) способность выполнения функции не зависит от работы или отказа другого оборудования;

b) способность выполнения функции не зависит от воздействий, возникающих от постулированного исходного события, при котором требуется ее выполнение.

[МАГАТЭ 50-SG-D8]

Примечание — При проектировании средствами достижения независимости являются изоляция (в документах МАГАТЭ употребляется также термин «функциональная изоляция»), физическое разделение и коммуникационная независимость.

3.30 **прерывание** (interrupt): Приостановление процесса, например, выполнения компьютерной программы, вызванное внешним по отношению к данной программе событием.

[IEEE 610]

3.31 **архитектура контроля и управления** (I&C architecture): Организованная структура систем контроля и управления АС, которые являются важными для безопасности.

Примечание 1 — См. также «структура системы контроля и управления», «система контроля и управления».

Примечание 2 — Организованная структура определяет основные функции, класс и границы каждой системы, взаимосвязи и независимость систем, приоритетность и голосование между одновременно действующими сигналами и взаимодействие человек — машина.

Примечание 3 — В настоящем стандарте данный термин определяет только часть всей системы контроля и управления АС. Системы контроля и управления АС включают в себя также неклассифицированные системы и оборудование.

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

Примечание 1 — См. также «подфункции контроля и управления», «функции контроля и управления и соответствующие системы и оборудование», «прикладные функции».

Примечание 2 — Данный термин применяется разработчиками процесса при определении требований к функционированию контроля и управления. Функция контроля и управления определяется так, что она:

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

Примечание 3 — Функция контроля и управления может быть разделена на ряд подфункций (например, измерительная функция, функция управления, функция воздействия) с целью распределения по системам контроля и управления.

3.33 **подфункция контроля и управления** (I&C subfunction): Часть функции контроля и управления, заложенной в систему контроля и управления или в подсистему.

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

Примечание 2 — Вместо термина «подфункция» часто употребляется термин «функция», если в контексте не возникает двусмысленности.

3.34 **функции и соответствующие системы и оборудование** (functions, and the associated systems and equipment): Выполнение функции заключается в достижении определенной цели; соответствующие системы и оборудование представляют собой совокупность компонентов и компоненты сами по себе, которые используются для выполнения функции.

[МЭК 61226, модифицировано]

Примечание — См. также «функция контроля и управления», «система контроля и управления».

3.35 **система контроля и управления (СКУ)** (I&C system): Система, основанная на применении электрической и/или электронной и/или программируемой электронной техники, выполняющая функции контроля и управления, а также функции обслуживания и наблюдения, связанные с эксплуатацией самой системы. Термин используется как обобщающий, охватывающий все элементы системы, включая питание, датчики и другие входные устройства, линии передачи данных и другие связи, интерфейсы исполнительных устройств и других выходных устройств (см. примечания). Различные функции системы могут использовать как выделенные, так и разделенные ресурсы.

[МЭК 61508-4, пункт 3.3.2, модифицировано]

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

Примечание 2 — Элементы, входящие в состав определенной системы контроля и управления, определяют границы этой системы.

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

3.36 **архитектура системы контроля и управления** (I&C system architecture): Организованная структура системы контроля и управления.

Примечание — См. также «архитектура контроля и управления».

3.37 **элементы, важные для безопасности** (items important to safety): Элементы, которые включают в себя:

a) сооружения, системы и компоненты, неисправность или отказ которых могут привести к непредусмотренному облучению персонала АС или населения;

b) сооружения, системы и компоненты, которые препятствуют развитию возможных случаев нарушений нормальной эксплуатации при аварийной ситуации;

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

[МАГАТЭ 50-SG-D3]

Примечание 1 — См. также «система безопасности», «класс системы контроля и управления».

Примечание 2 — В данном стандарте системы контроля и управления, важные для безопасности, подразделяются на три класса: 1; 2; 3.

Примечание 3 — IAEA 50-SG-D8 подразделяет системы, важные для безопасности, на «системы безопасности» и «системы, связанные с безопасностью».

3.38 **ремонтопригодность** (maintainability): Вероятность того, что конкретная операция по обслуживанию устройства в данных условиях эксплуатации может быть выполнена в заранее определенный период времени, в заранее определенных условиях с использованием заранее определенных операций и средств.

[МЭК 60987, пункт 2.10, модифицировано]

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

[МЭК 61508-4, пункт 3.7.1, модифицировано]

3.40 **анализ безопасности АС** (plant safety analysis): См. А.2 приложения А.

3.41 **постулированное исходное событие** (postulated initiating event — PIE): Постулированные исходные события, определяющие события, которые приводят к определенным нарушениям эксплуатации или аварийным условиям с последующими отказами оборудования.

[МАГАТЭ 50-C-D]

Примечание 1 — Ожидаемые эксплуатационные происшествия: все эксплуатационные процессы, имеющие отклонения от нормальной эксплуатации, которые происходят один или несколько раз в течение времени эксплуатации АС и ввиду предусмотренных проектом мер не вызывают каких-либо значительных повреждений объектов, важных для безопасности, и не приводят к аварийным условиям.

Примечание 2 — Первичными причинами постулированных исходных событий могут быть вероятные отказы оборудования и ошибки персонала (как на самой АС, так и вне ее), события, вызванные воздействием человеческого фактора или природных явлений. Перечень постулированных исходных событий должен быть установлен надзорным органом.

3.42 **ранее разработанное программное обеспечение** (pre-developed software — PDS): Часть программного обеспечения, которая уже существует и доступна как коммерческий или запатентованный продукт.

[МЭК 60880-2, пункт 3.1]

Примечание — Ранее разработанное программное обеспечение можно разделить на: программное обеспечение общего назначения, которое не разрабатывалось для определенного оборудования, и программное обеспечение, интегрированное в компоненты оборудования, которое применяется совместно с оборудованием.

3.43 **вероятностный метод** (probabilistic method): См. А.2.2 приложения А.

3.44 **проектная организация** (project organization): Организация(и) или лица, которые в процессе прохождения всех фаз общего жизненного цикла безопасности контроля и управления и/или системы контроля и управления несут ответственность за определение и осуществление всей организационной и технической деятельности, связанной с функциями контроля и управления, системами и оборудованием, важными для безопасности.

Примечание — Этот термин введен для более четкого отличия от термина «эксплуатирующая организация».

3.45 **квалификация** (qualification): Процесс определения соответствия системы или компонентов эксплуатационным условиям. Квалификация осуществляется для установления соответствия определенного класса системы контроля и управления определенному набору квалификационных требований.

3.46 **качество** (quality): Совокупность характеристик объекта, которые придают ему способность удовлетворить установленные и реализуемые требования.

[ИСО 8402, пункт 2.1]

3.47 **обеспечение качества** (quality assurance): Совокупность планируемых и систематически проводимых мероприятий, необходимых для создания уверенности в том, что продукция или услуга будет соответствовать определенным требованиям к качеству.

[ИСО 8402, пункт 3.5, модифицировано]

3.48 **программа качества** (quality plan): Документ, регламентирующий конкретные меры в области качества, распределение ресурсов и последовательность действий, относящихся к конкретной продукции, услуге, контракту или проекту.

3.49 **резервирование** (redundancy): Способ обеспечения надежности объекта за счет использования дополнительных средств и/или возможностей, избыточных по отношению к минимально необходимым для выполнения требуемых функций.

[МАГАТЭ 50-SG-D8]

3.50 **надежность** (reliability): Вероятность того, что прибор, система или устройство будут выполнять назначенные функции удовлетворительно в течение определенного времени в определенных условиях эксплуатации.

[МАГАТЭ 50-SG-D8]

Примечание — Надежность компьютерных систем включает в себя как надежность технических средств, которая обычно выражается количественно, так и надежность программного обеспечения, которая обычно является качественной мерой, поскольку в большинстве случаев не существует критериев для установления числового значения его надежности.

3.51 **повторно используемое программное обеспечение** (reusable software): Программный модуль, который может использоваться более чем в одной компьютерной программе или программном обеспечении системы.

[IEEE 610, модифицировано] [1]

3.52 **комплекс безопасности** (safety group): Взаимосвязанный набор оборудования, спроектированный для выполнения всех операций, необходимых для того, чтобы гарантировать непревышение пределов, установленных проектом для данного постулированного исходного события.

Примечание — Функции контроля и управления в комплексе безопасности могут относиться к различным категориям.

3.53 **системы безопасности** (safety systems): Системы, обеспечивающие при требуемых условиях безопасный останов реактора и отвод тепла от активной зоны и/или ограничивающие последствия возможных эксплуатационных происшествий и аварийных условий.

[МАГАТЭ 50-SG-D8]

Примечание 1 — См. также «система, важная для безопасности», «класс систем контроля и управления».

Примечание 2 — Система безопасности по МАГАТЭ соответствует в основном классу 1 данного стандарта.

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

[ИСО/МЭК 12207, пункт 3.25, модифицировано]

3.55 **единичный отказ** (single failure): Случайный отказ, который выражается в потере способности компонента или системы выполнять предписанные функции. Отказы, возникающие как следствие единичного случайного события, рассматриваются как составляющие единичного отказа.

[МАГАТЭ 50-SG-D8, модифицировано]

Примечание 1 — См. также «критерий единичного отказа».

Примечание 2 — Единичный отказ может быть следствием как внутреннего, так и внешнего опасного воздействия.

3.56 **критерий единичного отказа** (single-failure criterion): Комплекс оборудования, отвечающий критерию единичного отказа, когда он способен функционировать в соответствии со своим предназначением, несмотря на допускаемый единичный случайный отказ, происшедший внутри комплекса. Последующие отказы, возникающие в результате допускаемого единичного отказа, рассматриваются как составляющие единичного отказа.

[МАГАТЭ 50-S-D]

Примечание 1 — См. также «единичный отказ», «отказ программного обеспечения».

Примечание 2 — Отказ из-за программного обеспечения является систематическим, а не случайным отказом.

3.57 **отказ программного обеспечения** (software failure): Отказ системы из-за проявившейся проектной ошибки в компоненте программного обеспечения

Примечание 1 — Все отказы программного обеспечения связаны с ошибками при проектировании, так как программное обеспечение в данном контексте не связано с физическими носителями, не изнашивается или не страдает от физических отказов. Так как триггеры, которые являются источниками сбоев программного обеспечения, задействуются при работе системы случайным образом, то отказы программного обеспечения имеют также случайный характер.

Примечание 2 — См. также «отказ», «сбой», «сбой программного обеспечения».

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

Примечание — См. также «дефект» (3.22).

3.59 **надежность программного обеспечения** (software reliability): Составляющая надежности системы, которая зависит от отказов программного обеспечения.

3.60 **спецификация** (specification): Документ, определяющий в полной, точной, проверяемой форме требования, дизайн, поведение или другие свойства системы либо компонента, и, зачастую, процедуры, для определения, выполняются ли эти требования.

[МЭК 60880-2, 3.21 и IEEE 610] [1]

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

[МЭК 61508-4, пункт 3.3.1, модифицировано]

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

Примечание 2 — Системы контроля и управления следует отличать от механических систем и электрических систем АС.

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

[МЭК 61508-4, пункт 3.6.6]

3.63 **жизненный цикл безопасности системы** (system safety life cycle): Необходимая деятельность в отношении системы контроля и управления, важной для безопасности, которая осуществляется в течение периода времени от стадии развития концепции с разработкой требований до последней стадии, когда система больше не может эксплуатироваться.

Примечание 1 — Жизненный цикл безопасности системы связан с общим жизненным циклом безопасности.

Примечание 2 — См. также «общий жизненный цикл безопасности контроля и управления».

3.64 **системное программное обеспечение** (system software): Программное обеспечение, спроектированное для определенной компьютерной системы или семейства компьютерных систем с целью эксплуатации и обслуживания компьютерной системы и установленных программ, например, операционные системы, ЭВМ, утилиты. Системное программное обеспечение обычно состоит из операционного системного программного обеспечения и инструментальных программ (см. рисунок 2).

[МЭК 60880-2, 3.24]

Примечание 1 — Операционное системное программное обеспечение: программы, загруженные в основной процессор в течение времени работы системы, такие как, операционная система, входные и выходные драйверы, коммуникационные программы, библиотеки прикладных программ, on-line диагностика, программы сжатия, упрощенные программы управления.

Примечание 2 — Инструментальные программы: программы, которые используют при разработке, тестировании или обслуживании других программ и систем, таких как компиляторы, генераторы кодов, графические редакторы, off-line диагностика, средства верификации и валидации.

Примечание 3 — См. также «прикладное программное обеспечение».

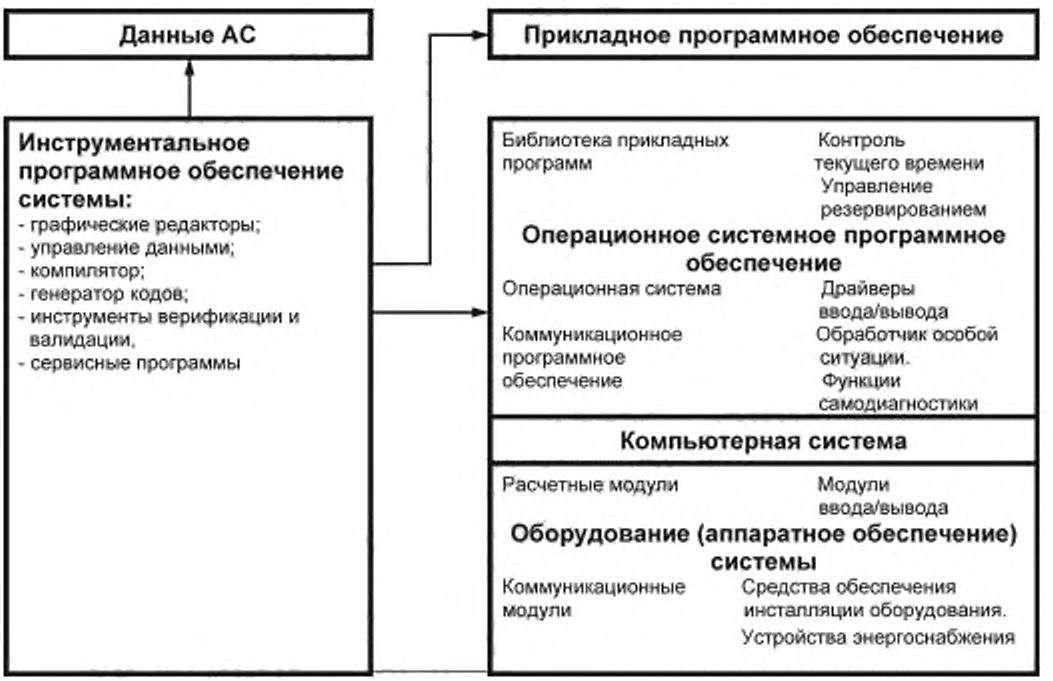


Рисунок 2 — Характерные взаимосвязи между аппаратными и программными средствами компьютерных систем



Рисунок 3 — Связь между отказом системы, случайным отказом и систематическим дефектом

4 Обозначения и сокращения

АС (NPP) — атомная станция;
ПУ (control room) — пульт управления;
ИСО (ISO) — Международная организация по стандартизации;
МАГАТЭ (IAEA) — Международное агентство по атомной энергии;
МЭК (IEC) — Международная электротехническая комиссия;
ФСО (FSE I&C) — функции, связанные с ними системы и оборудование контроля и управления;
Э/Э/ЭПС (E/E/PES) — электрические/электронные/электронные программируемые системы.

5 Полный жизненный цикл безопасности контроля и управления

Целью данного раздела является определение:

- общих требований к функциям и соответствующим системам и оборудованию контроля и управления — ФСО, важным для безопасности, исходя из проекта безопасности АС (см. разделы А.1 и А.2 приложения А);

- требований к архитектуре систем контроля и управления, важных для безопасности, исходя из общих требований к ФСО, и

- связей между требованиями архитектуры контроля и управления и требованиями к отдельным системам контроля и управления, важных для безопасности.

Для того, чтобы убедиться, что все требования безопасности, которым должны соответствовать контроль и управление, учтены, выполнены и подтверждены, требуется системный подход. Системный подход достигается путем осуществления деятельности, связанной с разработкой, вводом в эксплуатацию и проведением контроля и управления, основываясь на концепции полного жизненного цикла безопасности контроля и управления. Жизненный цикл безопасности контроля и управления связан, в свою очередь, с жизненными циклами безопасности каждой системы контроля и управления (см. раздел 6).

Фазы типового полного жизненного цикла безопасности контроля и управления охватывают:

а) рассмотрение основ проекта автоматизированной системы управления технологическим процессом (далее — АСУТП) АС, включая (см. 5.1):

- требования к функциональным и эксплуатационным характеристикам и независимости,

- категории функций,

- особенности, характерные для данной станции;

b) определение общей спецификации требований к функциям и соответствующим системам и оборудованию контроля и управления, важным для безопасности (см. 5.2);

c) разработка полной архитектуры и распределение функций контроля и управления по отдельным системам и оборудованию (см. 5.3);

d) общее планирование (см. 5.4);

e) реализация отдельных систем (см. раздел 6);

f) общая интеграция и приемка систем (см. раздел 7);

g) эксплуатация и обслуживание всей системы контроля и управления в целом (см. раздел 8).

В скобках указаны раздел и подраздел настоящего стандарта, в которых рассматривается соответствующая фаза, а в таблице 1 представлена информация о цели, входных и выходных данных, назначении каждой фазы.

Связи между рассматриваемым полным жизненным циклом и жизненными циклами безопасности каждой из систем контроля и управления показаны на рисунке 4:

a) полный жизненный цикл безопасности системы контроля и управления в целом представляет собой интерактивный процесс, при выполнении которого необходимо устанавливать совпадение результата, полученного по окончании каждой из фаз жизненного цикла безопасности системы контроля и управления, с тем, что планировалось при ее начале. Фаза может начаться до завершения предыдущей при условии проведения соответствующих проверок, которые подтвердили бы соблюдение общего содержания процесса разработки.

b) фаза только тогда считается законченной, когда все предыдущие фазы завершены.

Примечание — Ответственность за безопасность станции несет эксплуатирующая организация, и эта ответственность не может быть поделена между разработчиками, поставщиками, строителями и надзорными органами, участвовавшими в процессе на различных этапах жизненного цикла АС (см. 3.1.2 МАГАТЭ 75 INSAG-3).

Таблица 1 — Обзор общего жизненного цикла безопасности контроля и управления

Раздел или подраздел	Исходные данные	Цели деятельности	Объект	Результаты
5 Требования фаз полного жизненного цикла безопасности и их связь с жизненными циклами систем				
5.1 Определение требований к контролю и управлению на основе технического проекта АСУТП АС				
5.1.1 Обзор требований к функциональным, эксплуатационным характеристикам и независимости	Документы по проектным основам безопасности АС. Принципы работы АС	Определение: -общих требований к функциональным и эксплуатационным характеристикам ФСО, важных для безопасности; - требования к независимости, накладываемые на ФСО в соответствии с концепцией глубокоэшелонированной защиты АС; - автоматические функции и обязанности оператора	Системы АС и соответствующие ФСО, важные для безопасности	Определение исходных требований для 5.2
5.1.2 Обзор требований к установлению категорий	Категории безопасности АС	Определение ФСО. Верификация полноты охвата. Верификация выполнения всех требований	ФСО, важные для безопасности	Определение исходных требований для 5.2
5.1.3 Обзор особенностей АС	Планировочная документация АС, основные данные проекта	Определение: - границ между технологией АС и системами контроля и управления; - особенностей, вытекающих из систем обслуживания и планировки АС, условий окружающей среды; - внутренних и внешних источников потенциальной опасности; - принципов эксплуатации и обслуживания оборудования АС	Планировка АС. Системы АС. ФСО	Определение особенностей АС, влияющих на проект архитектуры (см. 5.3) и спецификацию требований к отдельным системам контроля и управления (см. 6.1)

Продолжение таблицы 1

Раздел или подраздел	Исходные данные	Цели деятельности	Объект	Результаты
5.2 Выходная документация	Результаты по 5.1	Разработка общей спецификации требований к ФСО, важным для безопасности, в терминах требований к функциональным, эксплуатационным характеристикам, независимости и категорийности	ФСО	Общая спецификация требований к ФСО для 5.3
5.3 Разработка полной архитектуры контроля и управления и распределение функций				
5.3.1 Проектирование архитектуры контроля и управления	Результаты по 5.2	Разработка проекта архитектуры систем контроля и управления, удовлетворяющего общим спецификациям требований ФСО. Принятие необходимых мер против отказов по общей причине	Функции и системы контроля и управления	Детальный проект архитектуры контроля и управления безопасности, в терминах автоматизированных систем, человеко-машинного интерфейса, а также взаимосвязей, устройств (см. 5.5.1)
5.3.2 Распределение функций	Результаты по 5.3.1 и 5.4 (с учетом результата по 6.3)	Распределение функций контроля и управления по отдельным системам и оборудованию. Формулирование требований к индивидуальным системам (границы, классификация, функциональность, надежность и др.)	Функции и системы контроля и управления	Требования к прикладным функциям систем и интерфейсу человек — машина, проекту систем контроля и управления и инструментов (см. 5.5.2)
5.3.3 Анализ	Результаты по 5. 3.1 и 5.3.2	Оценка надежности и устойчивости к отказу по общей причине. Оценка влияния человеческого фактора	Функции и системы контроля и управления	Оценка надежности и устойчивости к отказу по общей причине. Оценка влияния человеческого фактора (см. 5.3.3.2)
5.4 Общее планирование	Результаты выполнения 5.3	Разработка планов обеспечения качества, защищенности, интеграции, приемки, регламентов эксплуатации и обслуживания системы	Совместно работающие системы контроля и управления	Планы проектных стадий
6 Жизненный цикл безопасности системы	Результаты выполнения 5.5	Разработка спецификаций и создание систем контроля и управления в соответствии с архитектурой контроля и управления (см. раздел 6)	Отдельные системы контроля и управления	Результаты, описанные в таблице 3
7 Общая интеграция и приемка	Результаты выполнения 5.4.3 и 6.2.5	Проверка и приемка взаимодействующих систем в соответствии с архитектурой контроля и управления	Системы контроля и управления, входящие в архитектуру контроля и управления	Полностью интегрированные и принятые комиссией системы. Отчет об общей приемке (см. 7.2)

Окончание таблицы 1

Раздел или подраздел	Исходные данные	Цели деятельности	Объект	Результаты
8 Общая эксплуатация и обслуживание всей системы	Результаты выполнения 5.4.4, 5.4.5 и 7.1	Обслуживание при эксплуатации, ремонт систем для поддержания уровня безопасности	Системы контроля и управления, входящие в архитектуру контроля и управления	Непрерывное выполнение функций. Документирование эксплуатации и обслуживания
Примечание — Сравнение приведенных в таблице фаз с фазами по МЭК 61508-1 приведено в приложении D.				

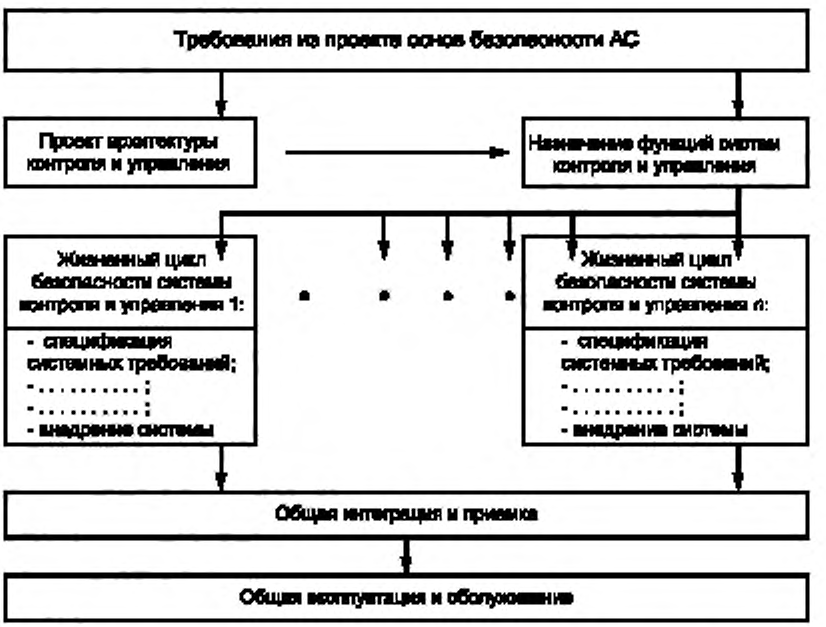


Рисунок 4 — Связь между полным жизненным циклом безопасности контроля и управления и жизненными циклами безопасности отдельных систем контроля и управления

5.1 Определение требований к контролю и управлению на основе технического проекта АСУТП АС

Настоящий раздел устанавливает исходные требования для спецификации ФСО и исходные условия для проектирования архитектуры контроля и управления, вытекающие из основ проекта безопасности и проекта АС.

В МАГАТЭ 50-C-D (Редакция 1) и МАГАТЭ 50-SG-D 11 определен ряд отдельных «принципов безопасности», которые совместно образуют «интегрированный подход к общей безопасности», обеспечивающий безопасность АС. Эти принципы должны реализовываться в проекте путем рассмотрения всех возможных «постулированных исходных событий» и создания последовательных физических барьеров, не допускающих облучения персонала, населения и радиационного воздействия на окружающую среду свыше установленных пределов (см. разделы А.1, А.2 и А.3 приложения А). В соответствии с этим подходом в проекте АС устанавливается соответствующий уровень качества для функций АС и систем, необходимых

для поддержания АС в пределах нормальных условий эксплуатации, для обеспечения правильной реакции на постулированные исходные события и осуществления долговременного управления АС после аварии.

5.1.1 Обзор требований к функциональным, эксплуатационным характеристикам и независимости функций контроля и управления

Требования к функциональным, эксплуатационным характеристикам и независимости функций контроля и управления, важных для безопасности, и принципы эксплуатации АС определяются в проекте безопасности станции и являются неотъемлемой частью всего проекта контроля и управления. Требования, касающиеся взаимодействия человек — машина, учитывают как принципы управления, так и эргономические соображения, что позволяет снизить вероятность отказов за счет человеческого фактора.

Основные положения проекта безопасности станции должны содержать следующие исходные данные:

- концепция глубокоэшелонированной защиты АС (см. раздел А.3 приложения А) и группа функций, предназначенных для подавления последствий постулированных исходных событий и выполняющих таким образом цели защиты (см. раздел А.2 приложения А).

Примечание 1 — В случаях, когда требуется высокая надежность функции, перечень требований к АС и контролю и управлению учитывает необходимость различных путей обеспечения защиты от конкретного постулированного исходного события, например, использование двух или более независимых и функционально дублирующих принципов физического воздействия и, если необходимо, второй функционально дублирующей, независимой, резервированной механической системы аварийного управления.

Примечание 2 — Барьеры глубокоэшелонированной защиты могут включать в себя функции, важные для безопасности, но могут включать также и другие функции. Требования настоящего стандарта определяют только функции, являющиеся важными для безопасности;

- требования к функциональным, эксплуатационным характеристикам функций АС, важных для безопасности, которые должны соответствовать общим требованиям безопасности (см. раздел А.3 приложения А).

Примечание 3 — Если требуется валидация правильности выполнения функции (см. 6.1.3.1), то проектом должны быть определены исходные условия, допустимые пределы и допустимая скорость изменения параметров АС, контролируемых системами контроля и управления, важными для безопасности;

- роль автоматики и регламентированных действий оператора при управлении предусматриваемыми отклонениями от нормальной эксплуатации и в условиях аварии (см. раздел А.3 приложения А);
- анализ задач в соответствии с разделом 3.2 МЭК 60964, определяющим, какие функции должны быть переданы оператору и какие — машинам;
- изменения параметров, которые должны быть представлены оператору для выполнения им действий вручную;
- принципы приоритетности между действиями, выполняемыми автоматически и вручную, с учетом категорий функций, щитов управления или местных щитов.

5.1.2 Обзор требований к установлению категорий (категоризации)

5.1.2.1 Требования настоящего стандарта к установлению категорий (категоризации) функций и классификации систем

Функции, системы и оборудование на АС классифицируют в соответствии с их важностью для безопасности (см. раздел В.1 приложения В). Настоящий стандарт устанавливает различие между установлением категорий функций контроля и управления, важных для безопасности, и классификацией систем контроля и управления. Разумность такого деления и соотношение с концепциями классификации, изложенными в документах МАГАТЭ и МЭК 61226, поясняется в приложении В.

Примечание — Термины «категоризация» и «классификация» иногда используются как синонимы. Для ясности в настоящем стандарте термин «категоризация» относят к функциям, а термин «классификация» — к системам.

Процесс установления категории соотносит каждую функцию контроля и управления с категорией, исходя из ее важности для безопасности. Эти категории характеризуются набором требований к выполнению спецификаций, проекта, внедрению, верификации и валидации функций контроля и управления, а также требованием к минимально требующемуся классу соответствующих систем и оборудования, необходимого для реализации функций. Последовательные требования применяются к целому ряду приборов,

необходимых для реализации конкретной функции, без учета того, как она распределена по другим взаимосвязанным системам контроля и управления (см. раздел А1 МАГАТЭ 50-SG-D-1).

При классификации системы контроля и управления оборудование распределяют по классам в соответствии с их важностью для безопасности. Эти классы характеризуются набором требований к свойствам и возможностям систем. Выполнение этих требований позволяет рассматривать систему как подходящую для размещения одной или более функций контроля и управления в соответствии с определенной категорией. Требования относятся к прикладным функциям, сервисным функциям и функциям, выполняемым системным программным обеспечением данной системы.

Процесс установления категорий функций контроля и управления является частью проекта основ безопасности АС и выходит за пределы области применения настоящего стандарта (см. раздел В.1 приложения В). Настоящий стандарт предусматривает, что при проектировании основ безопасности отдельные функции контроля и управления, важные для безопасности, распределяются по трем категориям А, В или С и требования основного проекта к системам и оборудованию, соответствующему этим категориям, соответствуют также требованиям к системам безопасности МАГАТЭ.

Примечание — Нормативные требования к установлению категорий в различных странах могут отличаться. По этой причине не следует ожидать единого решения при установлении категорий функций контроля и управления в соответствии с данным стандартом, который применим как к новым, так и к действующим АС. В связи с этим при установлении категорий необходимо провести специальный анализ соответствия установленных категорий функций контроля и управления требованиям к соответствующим системам и оборудованию.

Классификацию систем определяет организация, проектирующая систему контроля и управления, на фазе разработки проекта архитектуры до назначения функций контроля и управления отдельным системам (см. 5.3.1 и 5.3.2).

5.1.2.2 Требования

a) Категоризация функций контроля и управления должна содержаться в основах проекта безопасности и формировать исходные данные для выработки общей спецификации требований к функциям, системам и оборудованию контроля и управления.

b) Организация, проектирующая контроль и управление, должна проводить обзор категоризации и верифицировать ее полноту и осуществимость. В случае неосуществимости (например, при назначении слишком высокой категории для очень сложной функции) необходимо провести повторный анализ функций контроля и управления АС, пока не будет найдено осуществимое решение.

5.1.3 Обзор особенностей проекта АС

Особенности проекта АС накладывают следующие определенные ограничения на разработку архитектуры контроля и управления (см. 5.3).

a) проектная организация должна учитывать ограничения, накладываемые на оборудование контроля и управления проектом АС, условиями взаимодействия с технологическим оборудованием и событиями вне системы контроля и управления, включая:

- границы между системами и оборудованием контроля и управления и технологическими системами АС, в том числе взаимодействие с электрическими/механическими исполнительными системами и устройствами энергоснабжения,
- диапазон переходных и стационарных условий окружающей среды в нормальных условиях эксплуатации, при отклонении от нормальных условий и при аварии, при которых должны работать системы контроля и управления,
- диапазон переходных и стационарных характеристик выдаваемой и потребляемой энергии в нормальных условиях эксплуатации, при отклонении от нормальных условий и при аварии, при которых должны работать системы контроля и управления,
- основные требования к размещению и прокладке кабелей,
- особые требования к размещению и прокладке кабелей к центрам их концентрации, таким как щиты управления или кабельные коридоры,
- требования по разводке нулевой шины и электропитания,
- внешние и внутренние опасности, рассматриваемые в соответствии с принятыми предположениями об опасностях на станции, включающие в себя пожар, подтопление, обледенение, удар молнии, действие повышенного напряжения или электромагнитное воздействие, землетрясение, взрыв или химическое воздействие;

b) проектная организация должна определить ограничения, накладываемые на оборудование контроля и управления принципами эксплуатации, т.е. ограничениями со стороны:

- защищенности информации,
- эксплуатации и обслуживания (см. 2.6 МЭК 60964),
- гарантийного обслуживания систем контроля и управления.

5.2 Выходная документация

Выходная документация о выполненной работе, описанной в 5.1, представляет собой следующие общие спецификации требований к каждой ФСО, важной для безопасности.

Примечание 1 — Общие спецификации требований охватывают всю функцию контроля и управления в целом, начиная с входных устройств (датчиков, устройств обработки, другого оборудования) и заканчивая выходными (блоками управления исполнительными устройствами и др. оборудованием). Дальнейшее дробление этих спецификаций приведет к спецификациям требований к подфункциям на уровне каждой отдельной системы контроля и управления, что зависит от выбора архитектуры (см 5.3) и от того, как функции распределены по оборудованию (контрольно-измерительные приборы, процессоры, исполнительные устройства):

a) общие спецификации требований должны быть установлены для каждой ФСО. Они должны включать в себя:

1) спецификацию требований к функциональности, определяющую, каким образом функция преобразует входную информацию в выходную с целью управления или контроля работы АС,

2) спецификацию требований к рабочим характеристикам, определяющую диапазон действия, точность и динамические характеристики функции.

Примечание 2 — Сюда включают требования к своевременности выполнения функций, которые раньше для систем жесткой логики могли не учитываться;

3) категорию функции.

Примечание 3 — Категория строго определяет минимальные классификационные требования к системам контроля и управления, необходимые для выполнения функции (см. таблицу 2);

b) общая спецификация требований должна выявить некоторую зависимость между функциями, которая задает требования при распределении функций по системам контроля и управления. Эти требования касаются:

1) комбинации функций, предназначенных для управления защитными действиями,

2) комбинации функций, обеспечивающих глубокоэшелонированную защиту,

3) комбинации функций, образующих комплекс безопасности;

c) общие спецификации требований ко всем ФСО следует верифицировать с тем, чтобы убедиться в том, что установленные функции и найденные ограничения позволят распределить функции по системам и выполнить спецификации этих систем (см. 6.1).

5.3 Проект полной архитектуры и распределения функций контроля и управления

В настоящем подразделе описано:

- как ограничения, упомянутые в 5.1.3, и требования подраздела 5.2 следует применять при разработке проекта полной архитектуры систем контроля и управления, важных для безопасности АС (сокращенно «архитектуры контроля и управления»);

- как функции контроля и управления следует распределять по отдельным системам контроля и управления.

5.3.1 Проект архитектуры контроля и управления

Проект архитектуры контроля и управления определяет верхний уровень систем контроля и управления АС (см. раздел В.4 приложения В), связи между этими системами и средства обеспечения согласованного интерфейса между этими системами.

5.3.1.1 Основные требования

a) Проект архитектуры контроля и управления должен охватывать все аспекты контроля и управления с тем, чтобы выделить функции контроля и управления, важные для безопасности, приведенные в 5.2.

b) Проект должен распределять контроль и управление по достаточному числу систем и оборудования, чтобы соответствовать требованиям к:

- независимости функций в различных эшелонах защиты;

- соответствующему разделению систем по классам;

- выполнению требований к физическому разделению и электрической изоляции в соответствии с ограничениями, вытекающими из условий внешней среды и расположения АС, анализа опасностей, а также связанными с обслуживанием при эксплуатации (см. 5.3.1).

c) Проект архитектуры должен предусматривать достаточное число систем и подсистем, чтобы принцип единичного отказа выполнялся для функций категории А во всех допустимых конфигурациях систем и АС (см. 7.5 МАГАТЭ 50-SG-D3).

d) Каждая система контроля и управления должна быть классифицирована в соответствии с ее назначением в системе функций контроля и управления согласно установленной категории (см. таблицу 2).

e) Интерфейс с оборудованием АС и взаимосвязи между системами контроля и управления должны определяться в составе проекта архитектуры для того, чтобы установить:

- распределение сигналов (измерений) по различным функциям, важным для безопасности;
- выбор и приоритетность исполнительных сигналов различных систем;
- пути прохождения сигналов и оборудование, общее для выполнения автоматических функций или ручного управления на различных уровнях глубокоэшелонированной защиты.

f) Описание систем, оборудования и их взаимодействия в проекте архитектуры контроля и управления должно быть достаточно подробным, чтобы способствовать анализу вопросов безопасности контроля и управления.

Таблица 2 — Соотношение между классами систем контроля и управления и категориями ФСО

Категории функций контроля и управления, важных для безопасности			Соответствующий класс систем контроля и управления, важных для безопасности
A	(B)	(C)	1
	B	(C)	2
		C	3
Примечание — Функции категории А могут выполняться только системами класса 1; функции категории В — системами классов 1 и 2; функции категории С — системами классов 1, 2 и 3.			

5.3.1.2 Интерфейсы человек — машина

a) Проект архитектуры контроля и управления должен распределять системы с интерфейсом человек — машина по различным помещениям АС, предназначенным для управления и наблюдения, включая блочный пункт управления (далее — БПУ) и дополнительные помещения, резервный щит управления (см. МЭК 60965), местные щиты управления и пункт управления противоаварийными действиями, с необходимой степенью резервирования, с учетом ограничений, накладываемых эксплуатацией и обслуживанием оборудования АС (см. 5.1.1).

b) Проект должен опираться на принципы эксплуатации, установленные в проекте АС (см. 5.1.1), включая:

- принципы приоритетности между автоматическими сигналами и сигналами управления, вводимыми вручную;
- принципы приоритетности между различными системами взаимодействия человеко-машинных интерфейсов при нормальной эксплуатации, аварии и эксплуатации после аварии;
- принципы приоритетности между основными и резервными человеко-машинными интерфейсами;
- принципы переключения основных и резервных человеко-машинных интерфейсов.

c) Проект архитектуры должен определять, как оператор получит извещения о сбоях и отказах, регистрируемых средствами диагностики отдельных систем. Форма представления должна быть такой, чтобы оператор имел возможность:

- немедленно по индикации опознать отказ и отличать его от других индицируемых эксплуатационных данных;
- решить, не следует ли применить ручное управление для перевода АС в безопасное состояние;
- определить системы, которые следует восстановить с помощью обслуживающего персонала.

d) Проект архитектуры контроля и управления должен соответствовать основным решениям по технологии систем человеко-машинного интерфейса (например, компьютеризированная или традиционная). Для представления информации операторам должны использоваться более сложные системы, если это снижает влияние человека на возникновение отказа и это влияние можно сократить благодаря получению

более качественной информации. Уровень отказов компьютерных информационных систем вследствие отказов по общей причине следует рассматривать в сравнении с уровнем отказов вследствие влияния человеческого фактора.

e) В проекте:

- должны быть указаны функции, управляемые человеком и управляемые автоматически в соответствии с анализом задач, выполненным в проекте АС (см. 5.1.1);

- должна быть определена способность системы контроля и управления осуществлять необходимую обработку информации и завершать задачи, определенные в результате взаимодействия с оператором (см. 3.2.2 МЭК 60964);

- должно быть обеспечено соответствие информации и времени, имеющихся у оператора для выполнения управления вручную, требованиям проекта АС (см. 5.1.1).

f) Для обеспечения эффективности взаимодействия человек — машина в проекте БЩУ и других щитовых помещений АС должны использоваться технические средства, основанные на требованиях МЭК 60964 и МЭК 60965.

g) При анализе проекта должны рассматриваться задачи оператора и оптимизация требований к взаимодействию человек — машина при выполнении как важных для безопасности, так и не влияющих на безопасность задач.

5.3.1.3 Средства передачи данных

Средства передачи данных между системами, образующими архитектуру контроля и управления, включают в себя все линии, обеспечивающие прохождение одного или более сигналов или сообщений по одному или более пути с использованием различной мультиплексной техники.

a) Линии передачи данных должны соответствовать общей спецификации требований к рабочим характеристикам (см. 5.2) при всех условиях работы АС.

b) Архитектура и технология линий передачи данных должны обеспечивать соблюдение требований независимости систем. Кроме физического разделения и электрической изоляции в проекте должны быть предусмотрены меры, гарантирующие отсутствие влияния неполадок в системе передачи данных на работу средств обработки.

c) Линии передачи данных должны включать в себя средства проверки работоспособности коммуникационного оборудования и полноты передаваемых данных.

d) Для устойчивости к отказам должно быть обеспечено резервирование линий передачи данных.

e) Линии передачи данных должны быть спроектированы так, чтобы передача данных и выполнение функции более высокой категории безопасности не нарушались при передаче данных в системе более низкого класса. Например, выполнение тестов на работоспособность не должно мешать выполнению функции высшей категории.

5.3.1.4 Инструментальные средства

a) В проект архитектуры контроля и управления должны быть включены инструментальные средства, выполняемые обычно на базе компьютеров (см. 4.2 МЭК 60880-2), которые обеспечивали бы устойчивость обмена данными между системами контроля и управления, работающими совместно, и гарантировали бы сохранность базы данных АС.

Примечание — Специальные инструментальные средства для отдельных систем выбирают на стадии разработки спецификации системы (см. 6.1.3.2).

b) Инструментальные средства должны применяться на всех фазах полного жизненного цикла безопасности, за счет чего может быть достигнуто повышение качества и надежности функций, важных для безопасности, например, для поддержки:

- аспектов, связанных с проектом интерфейсов между системами контроля и управления;

- общей интеграции и приемки распределенных функций.

5.3.1.5 Защита от отказов по общей причине

Цель проекта архитектуры контроля и управления — обеспечить меры защиты от отказов по общей причине систем контроля и управления путем введения различных защитных мер против одних и тех же постулированных исходных событий (см. 5.1.1).

Эти меры защиты включают в себя:

- проектные решения по обеспечению устойчивости к опасным событиям на АС. Внешние и внутренние опасности (см. 5.1.3), влияние которых не исключено для ограниченной части архитектуры контроля и управления и которые могут привести к отказам по общей причине;

- проектные решения, направленные против отказов, которые могут быть вызваны изменениями в нагрузке АС. Включение некоторых компонентов оборудования, например, усилителей мощности и реле, или ввод компонентов программного обеспечения, например, таких как сбор входных данных, передача данных и переключение эксплуатационных режимов, могут зависеть от событий, происходящих на АС;

- проектные решения по минимизации использования общих ресурсов в архитектуре контроля и управления и взаимодействия человек – машина для различных уровней защиты. Такие общие ресурсы можно представить в виде использования одного сигнала измерения или обычной технологической операции в различных управляющих действиях;

- решения по минимизации риска систематических сбоев. В любой системе контроля и управления существует риск проектных ошибок или присутствуют ошибки, связанные с реализацией. Поэтому возможность сбоя программного обеспечения, вызывающего отказ, нельзя исключить при анализе любого отказа системы. Если используются одинаковые программные модули в сходных условиях в разных компьютерных системах, существует риск отказа по общей причине вследствие такой ошибки в программном обеспечении;

- использование разнообразия. Разнообразие обеспечивает несколько различных путей обнаружения значительных событий и реагирования на них для увеличения защиты от отказа по общей причине. К видам разнообразия относятся разнообразие персонала, разнообразие сигналов (использование разных измерительных параметров для инициирования защитных действий), функциональное разнообразие, разнообразие проектных решений и проверок, разнообразие программного обеспечения и оборудования;

- принятие стратегических решений по ограничению сложности. Использование компьютеров способствует выполнению более сложных алгоритмов и процессов, чем это возможно с помощью оборудования с жесткой логикой. При более сложных требованиях возможность ошибок и просчетов в спецификации требований и ошибок в проекте и при реализации становится значительно больше, чем в случае простых требований.

5.3.1.5.1 Устойчивость к внутренним и внешним воздействиям, которые могут привести к отказу по общей причине

Необходимо принять меры, обеспечивающие работоспособность комплекса безопасности, выполняющего функции категории А, которые требуется поддерживать на случай противодействия внутренним и внешним опасным воздействиям.

Эти меры включают в себя:

- разделение, например, размещение резервных частей системы в различных помещениях;

- независимость, например, систем подогрева, вентиляции и кондиционирования воздуха и отдельных источников энергоснабжения для каналов и систем;

- защита, например, от огня, воздействия химических веществ и вибрации;

- проектирование, например, оборудования в соответствии со стандартами МЭК по электромагнитной совместимости;

- квалификацию по воздействиям окружающей среды, например, по отношению к сейсмическим воздействиям (см. 6.4).

5.3.1.5.2 Защита от отказов по общей причине вследствие изменения потребности в энергии

a) Необходимо определить выполняющие функции категории А компоненты систем контроля и управления, работа которых зависит от нагрузки станции. Возможные виды отказов и их последствия (включающие в себя их влияние на компоненты, работа которых не зависит от режима нагрузки станции) должны быть оценены с точки зрения вероятных источников и эффектов отказа по общей причине.

b) Риск отказов по общей причине систем класса 1 должен быть минимизирован за счет использования систем контроля и управления и обеспечивающих систем, которые работают в одном и том же режиме как до, в процессе, так и после изменения нагрузки, т.е. их работа не должна зависеть от графика приложения нагрузки.

5.3.1.5.3 Защита за счет проектных решений по архитектуре систем контроля и управления и человеко-машинному интерфейсу

a) Различные рубежи защиты против постулированных исходных событий должны быть оснащены независимыми системами или подсистемами (см. примечание 1 к 5.1.1). Если используются общие ресурсы, они должны соответствовать плану обеспечения надежности комплекса безопасности.

b) Должны быть предусмотрены независимые средства контроля и управления функциями и системами, важными для безопасности АС (например, мультиплексные линии передачи данных или компьютеры), чтобы во время отказа имелась достаточная информация, необходимая для безопасной эксплуатации АС.

c) Если управление функциями категории А или В выполняется вручную как дублирующее действия автоматики, то возможность отказа по общей причине в процессе этих действий должна быть сведена к минимуму.

d) Если одна функция категории А может инициировать действие системы безопасности, а другая функция категории А, применяемая при других обстоятельствах, может вызвать противоположное действие, необходимо провести анализ с целью определения того действия, которое требуется выполнить в условиях отказа систем контроля и управления.

5.3.1.5.4 Защита от отказа по общей причине вследствие систематических сбоев

a) Планирование высокого качества, предусмотренное при разработке и создании различных систем контроля и управления комплекса безопасности, должно исключать случаи невыявленных отказов и, таким образом, свести риск отказов этих систем по общей причине к минимуму. Настоящий стандарт содержит требования, которые следует применять для обеспечения качества систем контроля и управления различных классов.

b) Систематические отказы должны выявляться средствами самоконтроля (исключая использование ручек настройки, аппаратуры самоконтроля, проверок правдоподобия), а выявляемые отказы должны переводить систему(ы) в предварительно установленное, предпочтительно безотказное состояние, при этом оператор должен получать сообщение об отказе.

c) Если требуемая надежность безотказного выполнения функции безопасности больше, чем надежность, полученная в результате оценки безотказного состояния данной системы, то проект данной системы следует переработать.

Примечание 1 — Требуемая степень защиты от отказов зависит от категории выполняемых функций.

Примечание 2 — Цель настоящего подраздела — дать общие сведения. Детальные требования к защите от отказов по общей причине вследствие ошибок в программном обеспечении для функций категории А приведены в 4.1 МЭК 60880-2.

5.3.1.5.5 Защита за счет разнообразия

a) В случае, если требуется высокая надежность комплекса безопасности, при проектировании архитектуры контроля и управления следует опираться на принцип разнообразия, особенно если имеются неопределенности в выполненных в проекте оценках.

b) Необходимо рассмотреть методы функционального разнообразия и разнообразия сигнала. Эти методы являются эффективными для снижения вероятности отказа по общей причине, возникшего вследствие ошибок в спецификациях требований или в спецификации и установке прикладного программного обеспечения.

c) Разнообразие оборудования может быть эффективным против отказа по общей причине компонентов аппаратного обеспечения и может обеспечить защиту против сбоев программного обеспечения системы. В частности, ее следует рассматривать при создании сложных систем, если опыт эксплуатации подобных систем ограничен.

d) Следует использовать разнообразие процедур или методов верификации и валидации (например, разнообразие оборудования для электромагнитных испытаний, испытания на взаимную совместимость с использованием эмулятора и пр.), что дополнительно поможет избежать отказов по общей причине без усложнения системы защиты.

e) Если для защиты против отказа по общей причине используется защита за счет разнообразия, то в проект следует включить анализ ее эффективности. Как положительный, так и отрицательный результат следует зафиксировать и отразить в документации (см. 5.3.3).

5.3.1.5.6 Стратегические решения по ограничению сложности

Для того, чтобы снизить до минимума вероятность отказа по общей причине из-за сложности систем, проектирование архитектуры контроля и управления должно включать в себя анализ, показывающий, что степень применения компьютеров вместо систем, построенных на жесткой логике и степень участия человека приемлемы с точки зрения обеспечения безопасности.

Примечание — Такой подход может зависеть от национального опыта, позиции регулирующего органа и надежности компьютерных технологий.

5.3.2 Распределение функций

При задании функций контроля и управления все требования к ФСО, важные для безопасности, указанные в 5.2, распределяются по отдельным системам полной архитектуры контроля и управления. Если необходимо, одна функция может быть представлена в виде нескольких подфункций, распределен-

ных по ряду систем. Все функции или подфункции являются прикладными функциями систем контроля и управления (см. 6.1.1.1).

a) Спецификации функциональных требований и требований к характеристикам прикладных функций должны учитываться в общих требованиях к ФСО. Если функция распределена по более чем одной системе, то взаимосвязанные системы должны быть выстроены так, чтобы они соответствовали требованиям, определенным в 5.2.

b) Спецификации функциональных требований и требований к характеристикам прикладных функций должны включать в себя все вспомогательные функции валидации, блокировки и контроля, которые были определены при проектировании архитектуры контроля и управления, например состояние и режим работы взаимосвязанных систем, валидация сигналов, получаемых от других систем.

c) Распределение прикладных функций по системам должно соответствовать принципам, связанным с классом системы и категорией функции, представленным в таблице 2.

d) Функции категории А назначаются системам, которые соответствуют критерию единичного отказа.

e) При отнесении функций категории А одного и того же комплекса безопасности к системам следует принимать во внимание меры защиты от отказов по общей причине по 5.3.1.5. Примеры распределения функций различных категорий приведены на рисунке С.1 приложения С.

f) По результатам распределения прикладных функций по системам необходимо пытаться минимизировать сложность систем класса 1.

Примечание — Это особенно справедливо для новых АС. В случае замены систем жесткой логики на компьютерные к последним в отношении прикладных функций обычно предъявляются те же требования, что и к системам жесткой логики.

g) Требуемая надежность каждой прикладной функции, введенной в системы, должна быть на уровне достижимых пределов, включая отказ по общей причине.

5.3.3 Анализ

С целью верификации проекта архитектуры контроля и управления и распределения функций по системам необходимо проводить анализ. Такой анализ является итеративным процессом и осуществляется при выполнении проектных работ (см. раздел 6).

5.3.3.1 Оценка надежности и защиты от отказа по общей причине

a) Должен быть выполнен расчет надежности функций комплекса безопасности категории А, который должен учитывать зависимость от источников снабжения энергией (например, электрической и энергией сжатого воздуха) и устройств вентиляции и теплоснабжения.

b) Первоначально расчет может опираться на оценку надежности, достижимой для функций различных систем, и должен уточняться впоследствии при проектировании, основываясь на оценках надежности отдельных систем (см. 6.1.3.1.2).

c) Должна быть проведена оценка эффективности мер, направленных на снижение чувствительности комплекса безопасности, включающего в себя функции категории А, к отказам по общей причине,

d) Проектную документацию на систему (см. 6.3.3) следует проанализировать с целью найти общие или идентичные компоненты программного обеспечения или оборудования, которые поддерживают различные функции комплекса безопасности, включающего в себя функции категории А. Если такие узлы будут найдены в различных эшелонах защиты, необходимо привести подтверждение того, что при этом достигается низкая вероятность отказа по общей причине.

e) Не существует общепринятого метода количественной оценки вероятности отказа по общей причине, поэтому используют методы, обеспечивающие только качественные оценки (см. приложение С). Применяемые методы, например метод β-фактора для оборудования, должны быть определены в начале проектирования.

Примечание 1 — Цель указанных рекомендаций — избежать внесения изменений в планирование и проект системы при изменении требований, которые могут привести к возникновению отказов по общей причине вследствие ошибок из-за этих изменений.

Примечание 2 — Глубина анализа отказов по общей причине может зависеть от категории функций, поддерживаемых системами, и должна быть обоснована.

Примечание 3 — Требования к анализу отказов по общей причине вследствие ошибок в программном обеспечении приведены в 4.1.3 МЭК 60880-2.

Примечание 4 — Точность оценки вероятности отказа по общей причине можно улучшить, если системы контроля и управления имеют модульную структуру, так что при объединении компонентов и систем можно выполнить качественную оценку с помощью пошаговой верификации и, дополнительно, по возможности количественную.

5.3.3.2 Оценка человеческого фактора

Верификация архитектурного проекта должна включать в себя анализ требований, связанных с влиянием человеческого фактора, чтобы оптимизировать проект систем человеко-машинного интерфейса.

5.4 Общее планирование

В настоящем подразделе приведены требования к разработке общих планов, обеспечивающих соблюдение требований к функциям контроля и управления, важным для безопасности, распределенным по системам, в течение жизненного цикла систем.

Требования настоящего подраздела согласуются и дополняют планы, рассмотренные в 6.2 для отдельных систем контроля и управления.

Примечание — Приведенные ниже требования к планам не препятствуют тому, чтобы планы оформлялись в виде различного числа документов.

Общие планы должны быть разработаны, прежде чем начнутся предусмотренные в них работы.

5.4.1 Общая программа обеспечения качества

Настоящий стандарт предполагает, что программа обеспечения качества, соответствующая требованиям МАГАТЭ 50-С-QA (Редакция 1), существует как неотъемлемая часть проекта АС и в соответствии с ней осуществляется контроль соответствующей деятельности.

a) Программа обеспечения качества должна разрабатываться и осуществляться по каждому направлению деятельности, связанному с жизненным циклом безопасности контроля и управления [см. раздел 2 МАГАТЭ 50-С-QA (Редакция 1)].

b) Программа обеспечения качества должна охватывать все направления деятельности, необходимые для достижения качества, а также действия, направленные на проверку достижения требуемого качества [см. раздел 102 МАГАТЭ 50-С-QA (Редакция 1)].

c) Деятельность по проверке должна быть определена в планах верификации. Планы верификации включают в себя средства, процесс и результаты на каждой стадии безопасного жизненного цикла контроля и управления и определяют:

- процедуры и способы верификации деятельности;
- записи, которые должны храниться и проверяться;
- подлежащие проверке виды деятельности, связанные с безопасностью;
- процедуры, направленные на выявление ошибок и несоответствий;
- критерии, определяющие полное завершение фазы;
- завершающие отчеты, в которых подтверждается соответствие результатов фазы исходным требованиям и выявляются отклонения.

d) Программы обеспечения качества должны планироваться и включаться в общую программу обеспечения качества при проектировании АС, а входящие в них виды деятельности — учитываться в общем плане действий по проектированию АС.

5.4.2 Общий план защищенности

Для защиты информации, обрабатываемой системами, важными для безопасности, от несанкционированного изменения (сохранность), нарушения доступа (доступность) и несанкционированного вскрытия (конфиденциальность) требуются определенные меры безопасности.

Примечание 1 — В системах контроля и управления АС требования сохранности и доступности превалируют над требованием конфиденциальности.

Программное обеспечение (тексты программ, а также параметры и данные) может быть особенно уязвимым при конструировании и наладке. Угрозы опасного воздействия, которые необходимо рассмотреть, включают в себя умышленные преднамеренные изменения, которые приводят как к полностью ошибочной работе программного обеспечения или сбоям, возникающим в определенное время, так и к искажению данных.

Примечание 2 — Угрозы, возникающие в связи с непреднамеренными изменениями, рассматриваются в перечне системных требований (см. 6.1.1.4).

Общий план обеспечения защищенности содержит следующие организационные и технические меры защиты архитектуры систем контроля и управления от преднамеренных, спланированных действий, которые могут дезорганизовать выполнение функций, важных для безопасности:

a) требования к защищенности функций и систем, важных для безопасности, должны быть отражены в плане защищенности системы (см. 6.2.2);

b) риск от несанкционированного доступа и вмешательства должен систематически отслеживаться на всех фазах жизненного цикла от начала до снятия с эксплуатации;

c) меры по обеспечению защищенности системы не должны заметно отражаться на надежности или эксплуатационных свойствах;

d) жесткость требований по защищенности отдельной системы и соответствующего оборудования должна определяться выполняемыми системой функциями. Компьютерные системы, выполняющие функции категории А, требуют более высокой степени защищенности, чем системы, выполняющие функции категории В или С;

e) для поддержания постоянно высокого уровня защищенности систем на АС должна проводиться специальная политика обеспечения защищенности, учитывающая специфику отдельных рабочих мест. Она должна включать в себя процедуры, устанавливающие связь между административной и технической защищенностью, допуска к системам, защищенности при работе с данными, модернизации и обслуживании, проверки защищенности и отчетности, а также процедуры тренингов по обеспечению защищенности;

f) системы, выполняющие функции, важные для безопасности, должны быть физически защищены от несанкционированного доступа. Контроль доступа должен включать в себя строгую идентификацию и порядок удостоверения для персонала систем, выполняющих функции категории А, и надежную идентификацию персонала для систем, выполняющих функции категорий В и С (см. 7.12 МАГАТЭ 50-SG-D3);

g) необходимо исключить устройства удаленного доступа (внешнего по отношению к АС) к системам, выполняющим функции категории А. Если предусматривается использование устройств удаленного доступа, размещенных в пределах АС, следует изучить и показать, что их использование не приведет к дополнительному риску как от несанкционированного доступа, так и от возникновения дополнительных источников возможных отказов системы;

h) доступ к системе должен регистрироваться путем записи персонала, типа доступа, времени и выполненных действий;

i) указанные записи, касающиеся защищенности систем, выполняющих функции категории А, должны просматриваться через четко определенные промежутки времени, а для систем, выполняющих функции категории В и С, — периодически.

5.4.3 Планы общей интеграции и приемки

Общая интеграция представляет собой совокупность всех технических и административных действий, проводимых непосредственно на АС и направленных на монтаж систем контроля и управления, выполнение соединений, проверку, калибровку и установление готовности к эксплуатации.

Общая приемка представляет собой совокупность всех проводимых непосредственно на АС технических и административных действий, которые до начала эксплуатации энергоблока должны подтвердить, что установленные системы и энергоблок готовы к работе.

Примечание — Общая приемка систем контроля и управления является частью приемки энергоблока (см. 4.4 МАГАТЭ I75-INSAG-3).

Общая интеграция и приемка включают в себя наладку и пуск отдельных систем (см. 6.1.5 и 6.1.6).

a) Вслед за интеграцией систем контроля и управления на АС должно быть подтверждено выполнение всех спецификаций функциональных и параметрических требований к функциям контроля и управления, важных для безопасности во всех заранее определенных режимах работы энергоблока.

b) Объем работы по интеграции и приемке систем может быть сокращен, если комплексное тестирование уже проводилось на предприятии-изготовителе или площадке АС или если это была уже не первая поставка систем на АС. Эти сокращения объема общей верификации и валидации следует обосновать и задокументировать.

5.4.3.1 Общий план интеграции

Общий план интеграции систем контроля и управления должен разрабатываться в рамках программы обеспечения качества. В дополнение к общим требованиям 5.4.1 по обеспечению качества и верификации применяют следующие требования:

a) испытания взаимосвязанных систем должны проводиться для подтверждения того, что:

- все интерфейсы взаимосвязанных систем работают правильно,

- выявление отказов, корректирующие действия и представление соответствующих данных осуществляются в соответствии с спецификациями требований к функциям контроля и управления;

b) испытания взаимосвязанных систем на устойчивость к воздействию электромагнитных возмущений должны проводиться в соответствии с требованиями МЭК 61000-4-1 — МЭК 61000-4-6;

c) должна быть проверена правильность выполнения заземления и эквипотенциальных соединений всего оборудования и экранов кабелей;

d) необходимо провести испытание систем на влияние отключения внешнего электропитания для того, чтобы проверить их функционирование и устойчивость к прерыванию и последующему восстановлению питания;

e) должно быть проверено соответствие условий окружающей среды по месту размещения систем контроля и управления специфицированным условиям эксплуатации;

f) необходимо проверить аналоговые и логические сигналы обмена между системами, чтобы показать, что при выполнении различных функций, важных для безопасности, обеспечиваются заданные значения сигналов и логических состояний. В случае, если функции представления информации, аварийной сигнализации, записи и выполнения расчетов выполняются системой, не влияющей на безопасность, то эти испытания следует проводить совместно с такой системой, если нельзя предложить более простой способ проверки правильности передачи данных;

g) функции замкнутого логического управления должны проверяться от входа до выхода, включая исполнительные устройства и интерфейсы оператора;

h) испытания должны подтверждать, что правильная информация поступает в каждую систему в случае отказа резервированного оборудования, информационных линий связи, датчиков или управляющих устройств. Испытания должны подтверждать правильность включения и времени действия режима управления;

i) необходимо провести испытания мультиплексных систем управления на приемлемое время реакции и правильность передачи данных от исходных команд до получения подтверждения правильности индикации состояния устройства управления. Испытания должны проводиться при нормальных условиях эксплуатации, имитации аварийных, наихудших условий и отказов аппаратного обеспечения.

5.4.3.2 Общий план приемки

Общий план окончательной валидации ФСО должен разрабатываться в рамках программы приемки систем АС (см. 4.4.200 МАГАТЭ 75-INSAG-3) при соблюдении следующих требований:

a) для подтверждения соответствия функциональности систем и их характеристик всем ранее определенным общим спецификациям требований в процессе приемочных испытаний должна проверяться и корректироваться установка режимов, порогов, параметров и значений величин для калибровки приборов;

b) во время приемки на АС следует проверить и уточнить эксплуатационные режимы систем контроля и управления.

5.4.4 Общий план эксплуатации

Общее планирование эксплуатации относится к эксплуатации взаимосвязанных систем контроля и управления. Общий план включает в себя планы эксплуатации отдельных систем (см. 6.2.6).

Общий план эксплуатации разрабатывается в рамках программы обеспечения качества. В дополнение к общим требованиям 5.4.1 к обеспечению качества и верификации предъявляются следующие требования:

a) общий план должен описывать:

- средства пуска, начальной загрузки и поддержания взаимосвязанных систем в рабочем состоянии,
- средства верификации готовности систем к выполнению функций, важных для безопасности,
- регламентные операции, например, периодическое тестирование, которое необходимо выполнять в течение эксплуатации энергоблока для поддержания требуемой надежности функций, важных для безопасности;

b) общий план должен определять условия, при которых должна проводиться модификация параметров или управляющих воздействий системы и влияние такой модификации на работу систем и на безопасную эксплуатацию энергоблока. Общий план должен также устанавливать, что модификации могут проводиться:

- под административным контролем,
- под административным контролем и после согласования с разработчиком при соответствующих испытаниях и верификации.

Примечание — Технология модификации и контролирующие органы, которые дают разрешение на модификацию, могут зависеть от организации, выполняющей работу, и национальных регулирующих актов;

c) общий план должен охватывать все режимы эксплуатации взаимосвязанных систем и определять, как системы должны работать в каждом из рассматриваемых случаев, включая:

- необходимые действия и требования к работе взаимосвязанных систем и энергоблока в случае отказа системы или опасности внешнего воздействия,

- требования к работе систем и энергоблока при проведении периодических испытаний, обслуживании и/или при введении корректировок (модификации),

- отказ от упомянутых выше требований — в этом случае должно быть осуществлено и подтверждено восстановление нормального режима эксплуатации АС.

5.4.5 Общий план обслуживания

Общий план обслуживания относится к обслуживанию на уровне взаимосвязанных систем контроля и управления. Он включает в себя и координирует планы обслуживания отдельных систем контроля и управления (см. 6.2.7).

Общий план обслуживания разрабатывается в рамках программы обеспечения качества. В дополнение к общим требованиям обеспечения качества и верификации по 5.4.1 к отдельным системам контроля и управления предъявляются следующие требования:

a) следует накладывать ограничения на операции по обслуживанию отдельных систем контроля и управления так, чтобы любая из них не отражалась на безопасности энергоблока. В частности, если требуется (см. 6.1.1.2.5), чтобы в процессе обслуживания системы контроля и управления продолжали соответствовать критерию единичного отказа, общий план должен определять, какое оборудование может быть выведено из работы, последствия его вывода, а также средства по вводу в действие и подтверждению его правильной работы;

b) должен предусматриваться системный подход к проверке и замене частей системы, чтобы сделать маловероятными отказы по общей причине в тех частях архитектуры контроля и управления, которые в случае аварии подвергаются воздействию изменяющихся условий окружающей среды. Такой подход должен обеспечить, чтобы те части системы, которые подвергаются воздействию облучения и связанными с ним ускоренному старению или изменению физических свойств (кабели, детекторы) или состояние которых изменяется в соответствии с воздействующим сигналом (например, включение усилителей мощности, реле), не могли привести к невыявленным отказам.

Примечание — Интервалы замены оборудования могут определяться фактором ускоренного старения;

c) если операции по обслуживанию включают в себя адаптацию конфигурации или калибровочных данных, их следует контролировать при помощи документирования, которое позволит обеспечить:

- выполнение регулировок в установленных пределах (такие пределы могут устанавливаться проектами системы или энергоблока, тогда нет необходимости накладывать ограничения на действия обслуживающего персонала),

- если такие регулировки выполняются, когда система находится в работе, применяют требования 5.4.4,

- записи обо всех выполненных регулировках должны сохраняться.

5.5 Выходная документация

Выходная документация по проекту архитектуры контроля и управления и распределению функций является источником необходимых исходных данных для спецификации технических требований на отдельные системы из архитектуры контроля и управления (см. 6.1.1).

5.5.1 Документация по проекту архитектуры

a) Выходная документация должна определять для каждой системы контроля и управления:

- ограничения на проект, возникшие из-за особенностей АС (см. 5.1.3);

- ограничения, связанные с проектом архитектуры (см. 5.3.1);

- физическое и функциональное разграничения между системами.

b) Документация на используемый инжиниринговый инструментарий должна содержать информацию, из которой должно быть видно:

- каким образом проектирование как фаза жизненного цикла системы опирается на данные инструментальные средства;

- как должно использоваться каждое инструментальное средство;

- как должна верифицироваться выходная информация каждого инструментального средства.

Примечание — Требования к инжиниринговым методам и инструментальным средствам создания программного обеспечения для систем класса 1 приведены в 4.2 и 4.3 МЭК 60880-2.

5.5.2 Документация по распределению функций

a) Выходная документация должна определять функциональные требования, требования к характеристикам и надежности выполнения прикладных функций (см. 5.3.2), назначенных каждой системе. Требования могут быть оформлены в виде текстовой документации, блок-схем, матриц, структурных схем и пр., обеспечивающих ясное представление о функциях.

b) Спецификация требований к прикладным функциям компьютерных систем не должна зависеть от характеристик применяемой технологии, т.е. от компьютеров, реле.

c) Для разработки документов с требованиями, которые легко воспринимались бы как разработчиками технических требований к системе, так и операторами АС, должны использоваться инжиниринговые методы и инструментальные средства разработки систем и программного обеспечения.

6 Жизненный цикл безопасности системы

В проекте архитектуры контроля и управления выделяют отдельные системы контроля и управления, которые выполняют функции, важные для безопасности (см. 5.3.1). Настоящий раздел устанавливает цели систем и требования к таким системам. Требования раздела относятся также к компьютерным системам.

Примечание — Бóльшая часть требований может применяться и к системам контроля и управления, выполненным по традиционным технологиям.

Для того, чтобы быть уверенным в том, что все связанные с безопасностью требования, которым должна соответствовать система, учтены, удовлетворены и реализованы, необходимо выполнять работу на основе системного подхода. Системный подход достигается за счет организации деятельности, связанной с разработкой, построением и эксплуатацией системы в рамках жизненного цикла безопасности системы. Этот жизненный цикл, в свою очередь, охватывается деятельностью, осуществляемой в рамках общего жизненного цикла безопасности контроля и управления (см. раздел 5 и рисунок 4).

Фазы типичного жизненного цикла безопасности системы включают в себя:

- спецификацию требований к системе;
- спецификацию на систему;
- детальное проектирование и реализацию системы;
- интеграцию системы;
- валидацию системы;
- внедрение системы;
- модификацию проекта системы (при необходимости).

Квалификацию системы рассматривают отдельно, поскольку ее можно выполнить частично вне рамок жизненного цикла безопасности системы. Этот подход учитывает имеющийся опыт, который все больше основывается на применении уже существующего оборудования.

Типичный жизненный цикл безопасности системы и связи с жизненными циклами программного обеспечения и оборудования в соответствии с требованиями МЭК 60880 и МЭК 60987 приведены на рисунке 5.

Обзор целей, исходных данных и результатов деятельности на различных фазах типичного жизненного цикла системы и ссылки на соответствующие подразделы приведены в таблице 3.

Настоящий раздел включает в себя:

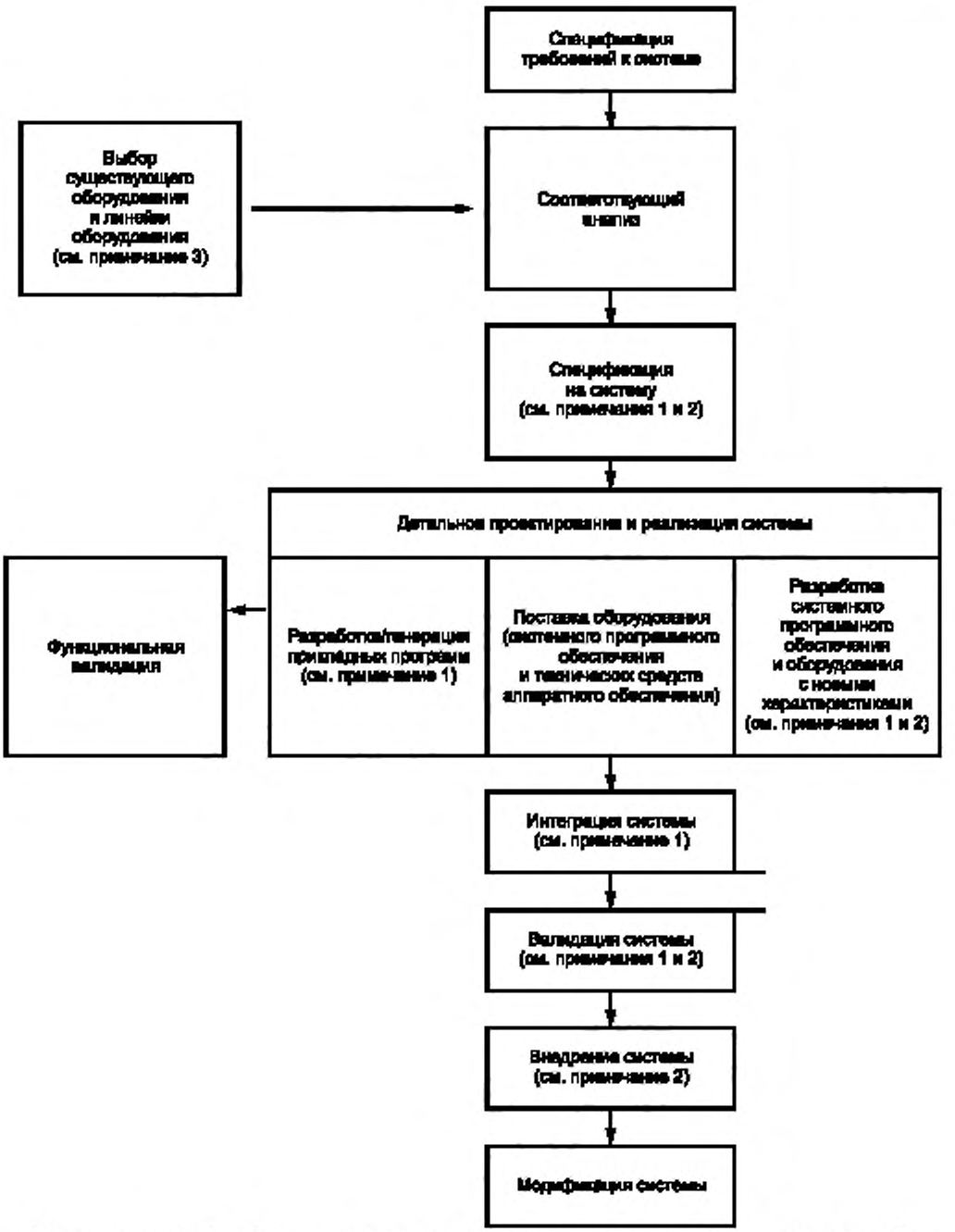
- требования, предъявляемые ко всем системам, важным для безопасности;
- требования, предъявляемые (в дополнение к предыдущим) к определенным классам систем или категориям функций. Специальные требования приведены в таблице 4.

Жизненный цикл системы является итеративным процессом; фаза может начинаться, прежде чем деятельность в рамках предыдущей фазы завершится; однако фазу можно считать законченной только если предыдущие фазы завершены, а результаты их выполнения соответствуют исходным данным.

Примечание — Эти требования отличаются от требований 6.1 МЭК 60880. Для программного обеспечения желательно, но в качестве необходимого требования не рассматривается, завершать каждую фазу разработки до начала следующей фазы, выполняемой в соответствии с указанными выше требованиями.

Таблица 3 — Обзор жизненного цикла безопасности системы

Раздел или подраздел	Исходные данные	Цель деятельности	Результат деятельности
6 Требования к жизненному циклу системы и его связь с полным жизненным циклом безопасности			
6.1.1 Спецификация требований к системе	Результаты по 5.5; 5.4	Разработка спецификации требований к: - функциям; - проектным ограничениям; - разграничению и интерфейсам с другими системами и устройствами; - интерфейсам взаимодействия с человеком; - условиям окружающей среды	Спецификация требований к системе. Требования к прикладным функциям
6.1.2 Спецификация системы	Результат по 6.1.1. Документация на существующее оборудование, которое может использоваться. Результаты по 6.2.1, 6.2.2	Оценка пригодности существующего оборудования для применения в проекте системы. Разработка проекта архитектуры системы, реализующего спецификации требований к системе. Распределение прикладных функций по подсистемам	Документация на спецификацию системы (см. 6.3.2), включающая в себя: - перечень выбранного оборудования и соответствующий анализ; - архитектуру системы; - спецификацию программного обеспечения
6.1.3 Проектирование и реализация системы	Результат по 6.1.2 Результат по 5.1.1 Результат по 6.2.1, 6.2.2	Расширение и уточнение проекта архитектуры. Разработка аппаратного и программного обеспечения (системного и прикладного). Проверка требований к прикладным функциям	Детальная проектная документация на систему (см. 6.3.3). Функциональная валидация и расчет надежности (см. 6.1.3.1). Оборудование и программное обеспечение подсистем и компонентов
6.1.4 Интеграция системы	Результат по 6.1.3 Результаты по 6.2.1, 6.2.2, 6.2.3	Сборка отдельных компонентов аппаратного и программного обеспечения, образующих систему	Отчет об интеграции. Интегрированная система
6.1.5 Валидация системы	Результаты по 6.1.2 и 6.1.4 Результаты по 6.2.1, 6.2.2, 6.2.4	Валидация спецификации на систему	Отчет о валидации системы
6.1.6 Внедрение системы	Результаты по 6.1.5 Результаты по 6.2.1, 6.2.2, 6.2.5	Установка, монтаж и испытание системы	Отчет о внедрении. Установленная и испытанная на объекте система
6.1.7 Модификации проекта системы	Решение о модификации (если требуется) Результаты по 6.2.1, 6.2.2, 6.2.7	Выполнение корректировок, улучшений или переделок системы	Отчеты о внесении изменений в систему. Модифицированная система
6.2 Планирование системы	Результаты по 5.4, 6.1	Разработка плана верификации, плана внедрения, эксплуатации и планов обслуживания и защиты	Планы системы
6.4 Квалификация системы	Результаты по 6.2.1, 6.2.2	Разработка плана квалификации	Квалификационная документация
Примечание — Сравнение приведенного в таблице определения фаз с предложенным МЭК 61508-2 см. в приложении D.			



Примечание 1 — Для систем класса 1 требования к программному обеспечению на данной стадии определены в МЭК 60880.

Примечание 2 — Для систем класса 1 требования к оборудованию на данной стадии определены в МЭК 60987.

Примечание 3 — Для систем класса 1 требования к существующему программному обеспечению на данной стадии определены в МЭК 60880-2.

Рисунок 5 — Жизненный цикл безопасности системы

6.1 Требования

Настоящий подраздел определяет требования к жизненному циклу безопасности системы.

Данные требования охватывают свойства, относящиеся к:

- конкретным функциям, назначенным системе в процессе распределения функций,
- основным характеристикам, которые в соответствии с системой классификации делают систему пригодной для выполнения функций, важных для безопасности, определенных категорий.

Примечание — Раздел 8 МЭК 61226 содержит основные требования к ФСО и особые требования к различным категориям ФСО. Эти требования соответствующим образом учтены в настоящем стандарте, когда формируются требования к системам и функциям.

6.1.1 Спецификация требований к системе

Целью данной фазы является выполнение основополагающего описания требований к системе, не связанного с возможным использованием конкретных технических решений.

Выходная документация, описывающая архитектуру контроля и управления и распределение функций (см. 5.5), является исходной для создания спецификации требований к системе.

На выходе этой фазы должен быть создан базовый документ, используемый для установления связи между документами, описывающими постановку задачи, и документами, которые представляют собой техническое решение.

Спецификация требований к системе должна определять:

- функции системы;
- ограничения на проектные решения;
- границы и связи с другими системами;
- интерфейсы пользователей;
- условия окружающей среды;
- требуемую квалификацию.

6.1.1.1 Функции

Должны быть рассмотрены требования к каждой прикладной функции и сервисным функциям системы. Предъявляются следующие требования:

6.1.1.1.1 Прикладные функции

Спецификации требований к прикладным функциям, важным для безопасности, определяются при распределении функций (см. 5.5.2).

a) Спецификация требования к каждой прикладной функции должна устанавливать:

1) функциональность, включая диапазоны входных и выходных величин и уставки. Для пороговых функций спецификация определяет границы между уставками и допустимыми значениями (т.е. значениями величины, включающими в себя неопределенности вследствие калибровки или дрейфов приборов);

2) характеристики, включающие в себя точность и время отклика. Если необходимо, требования к характеристикам определяют для различных исходных условий на АС и постулированных исходных событий.

Примечание — МЭК 61069-2 (6) может быть использован при идентификации и определении характеристик.

b) Спецификация требований к каждой прикладной функции должна устанавливать ее категорию и ограничения со стороны других функций комплекса безопасности (если они существуют). Эти требования неявно, в качественном виде, определяют требуемую надежность функции.

При процедуре распределения функций для каждой категории функций определяется минимальный класс системы контроля и управления. Вместе с требованиями к независимости функций одного и того же комплекса безопасности (критерий единичного отказа, проектная защита от отказа по общей причине) такие факторы позволяют проводить качественную оценку надежности функции или ряда функций комплекса безопасности.

Количественная оценка надежности прикладных функций может потребоваться при верификации проекта системы и общего проекта энергоблока (см. МЭК 60880). Эту оценку обычно проводят при проектировании оборудования системы, т.к. уже имеется накопленный опыт, однако метода, пригодного для количественной оценки надежности программного обеспечения, не существует (см. 6.1.3.1.2).

6.1.1.1.2 Сервисные функции

Сервисные функции, в отличие от прикладных, напрямую не связаны с выполнением действий, связанных с процессом, но относятся к специальным действиям, включающим в себя функции, необходимые

для конфигурирования, валидации, квалификации, внедрения, приемки, эксплуатации, периодических испытаний, обслуживания, введения модификаций проекта и обеспечения защищенности системы.

Спецификации требований к сервисным функциям определяются разработчиком системы. Точность требований к этим функциям определяют в разные периоды проектирования системы. В некоторых случаях они могут быть окончательно сформулированы в спецификациях на систему и на фазе разработки проекта архитектуры после выбора подходящего технического решения в отношении оборудования и программного обеспечения.

Требования к сервисным функциям должны принимать во внимание взаимодействия и ограничения, которые могут возникать при планировании системы (см. 6.2).

Примечание — Например, управление изменением параметров должно соответствовать результатам, определенным планом защищенности (см 6.2.2), планом эксплуатации системы (см. 6.2.6) и планом обслуживания (см. 6.2.7).

6.1.1.1.3 Функции системного программного обеспечения

Спецификация требований к системе обычно не полностью описывает функции системного программного обеспечения. Фактически эти функции, относящиеся к работе и самоконтролю собственно системы, характерны для существующего оборудования, используемого при построении системы (см. 6.1.2.1), и могут быть более точно определены на фазе спецификации системы. Однако требования к системному программному обеспечению безусловно определяются требованиями к функциональности прикладных функций и требованиями проектного ограничения на систему (см. 6.1.1.2.1).

Требования к функциям должны быть полностью определены как для вновь разрабатываемого, так и для поставляемого системного программного обеспечения.

6.1.1.2 Проектные ограничения

Следующие требования определяют проектные ограничения, которые сужают выбор решений при проектировании системы и задании функций. Ограничения зависят от класса системы и категории функции и должны учитываться при разработке спецификации системы и проекта архитектуры для того, чтобы:

- выполнять требования, обусловленные категоризацией прикладных функций;
- обеспечивать функционирование системы в соответствии с проектом;
- дать возможность или облегчить демонстрацию правильности работы системы.

6.1.1.2.1 Архитектура системы

Архитектура системы определяется категорией функций, которые должны выполняться системой (см. 5.3.2), и концепцией глубокоэшелонированной защиты (см. 5.2 и 7.8.1 МАГАТЭ 50-SG-D3).

a) Система может содержать функции высшей категории, соответствующей ее классу (см. 5.3.2), и функции более низкой категории. Система может включать в себя подсистемы более низкого класса, обеспечивающие выполнение следующих требований:

1) проектные требования к каждой подсистеме не должны быть ниже, чем требования к функциям наивысшей категории, выполняемым подсистемой;

2) проект системы должен обеспечивать выполнение требований к подсистемам или оборудованию более высоких классов в случае отказа оборудования более низкого класса.

b) Проект системы должен предусматривать резервирование и другие свойства, необходимые для обеспечения устойчивости к отказу (см. 6.1.2.2.3) и поддержания прикладных функций, важных для безопасности (см. 6.1.2.4).

Примечание — Система может также включать в себя резервирование для выполнения ряда других требований. Необходимость в таком резервировании определяется на стадии проектирования системы.

c) Проект системы должен соответствовать каким-либо требованиям независимости (см. 6.1.2.2.2) с целью:

- предохранить систему от влияния отказов систем с меньшим уровнем влияния на безопасность;
- предохранить систему от взаимного влияния отказов резервированных ветвей оборудования, поддерживающих функции категории А.

d) Проект систем 1-го класса должен предусматривать достаточное резервирование, чтобы удовлетворить критерию единичного отказа для функций категории А как при эксплуатации, так и при обслуживании системы (см. перечисление e) 6.1.2.4).

Примечание — Отказы из-за программного обеспечения являются систематическими, а не случайными. Поэтому критерий единичного отказа не может применяться при разработке программного обеспечения системы в том виде, в каком это делается при проектировании оборудования. На уровне каждой системы и архитектуры

контроля и управления следует рассматривать возможные воздействия отказа по общей причине из-за программного обеспечения на каждом уровне защиты или между резервированными уровнями.

6.1.1.2.2 Внутреннее поведение системы

a) Проект компьютерной системы должен обеспечивать детерминированное поведение, согласующееся с требованиями к характеристикам назначенных функций.

Примечание 1 — Если временная задержка между воздействием и откликом имеет гарантированные минимум и максимум при всех требуемых условиях, то можно сказать, что компьютерная система обладает детерминированным поведением (определение по [4]).

b) Коммуникационная технология должна быть выбрана и нормирована для того, чтобы удовлетворить требованиям к характеристикам при всех загрузках данных, генерируемых ожидаемыми переходными процессами на АС (включая лавинообразные изменения состояния в случае полной потери источников питания).

c) Чтобы обеспечить высокую степень гарантии в детерминированном поведении, системы класса 1 должны разрабатываться с использованием технологий в соответствии приложением В МЭК 60880 (особенно B2.d относительно времени реакции и B2.e — относительно прерываний). Технология, использующая статическую диспетчеризацию операций (см. примечание 2), предпочтительнее технологии с использованием прерываний.

Примечание 2 — Слово «статическая» означает принадлежность событию или процессу, который происходит без управления компьютерной программой (IEEE 610). Таким образом, при статической диспетчеризации планирование команд не зависит от работы компьютера, хотя возможно конечное число различных планов, зависящих от маршрута выполнения.

Примечание 3 — См. раздел 1 МЭК 60880 относительно роли приложений к стандарту и о том, что требуется, если практика отличается от того, что приведено в приложении.

d) Системы класса 2 могут разрабатываться с применением технологий, отличающихся от приведенных в перечислении в). В этих случаях проект системы должен гарантировать, что система будет работать необходимым образом при всех требуемых условиях АС.

e) С целью усиления способности систем классов 1 и 2 выдерживать непредусмотренные условия должны быть:

- обеспечены достаточные проектные области использования ресурсов (таких как бесперебойное питание, память, полоса пропускания каналов связи, ресурсы операционной системы) и внутренняя синхронизация;

- предусмотрены устройства слежения за любыми отклонениями от детерминированного поведения и восстановления нормального режима АС в случае временной потери входной информации, (например, таймер), циклическое обновление, выполняемое для изменения состояния, запускающего регистрацию событий на АС.

6.1.1.2.3 Самотестирование и устойчивость к отказам

a) Системы должны проектироваться так, чтобы ошибки и отказы регистрировались как можно раньше с целью поддержания требуемой работоспособности системы. Выявление отказов с помощью устройств самодиагностики не должно осуществляться за счет применения слишком сложных устройств. Насколько это возможно для каждой системы следует соблюдать требования 4.8 и А.2.8 приложения А МЭК 60880 к самодиагностике.

b) Чтобы оператор АС мог выполнить соответствующие корректирующие действия, ему должна представляться достаточная, своевременная и привлекающая внимание информация об отказах.

c) Проектом системы должно быть предусмотрено восстановление прежнего режима работы при выявлении отказов (частичная деградация).

d) Для систем класса 1 средства самодиагностики должны соответствовать МЭК 60880 и МЭК 60987.

6.1.1.2.4 Способность к тестированию

a) Системы должны быть оборудованы устройствами тестирования, которые позволяли бы верифицировать их способность выполнять функции, важные для безопасности.

Примечание 1 — В соответствии с МАГАТЭ (см. 4.12 МАГАТЭ 50-SG-D8), тестирование предпочтительнее полной проверки от датчиков до исполнительных устройств, однако более приемлемыми являются комплексные проверки. Тесты включают в себя в основном:

a) изменение состояния или величины сигнала на входе и определение изменения на устройствах сбора информации;

b) прерывание передачи и подтверждение того, что устройство сбора данных определит отказ и выполнит корректирующую операцию;

c) тестирование и калибровку датчиков (см. 7.10.2 МАГАТЭ 50-SG-D3);

d) тестирование исполнительных устройств (см. 7.10.3 МАГАТЭ 50-SG-D3).

b) Межповерочные интервалы должны определяться планами эксплуатации и обслуживания системы (см 6.2), при разработке которых руководствуются требуемой надежностью функций (см. 4.5 МАГАТЭ 50-SG-D8), надежностью оборудования и ожидаемой скоростью дрейфа калибровочных характеристик.

c) Если межповерочные интервалы таковы, что требуется периодическое тестирование системы при эксплуатации, проект системы должен включать в себя устройства тестирования и калибровки, способные выполнять проверку в процессе эксплуатации.

Примечание 2 — Использование автоматического оборудования облегчает проведение периодического тестирования. Это оборудование может вводить имитированные входные сигналы, записывать результирующие состояния на выходе и сравнивать полученные выходные сигналы с ожидаемыми.

d) Проект систем класса 1 и их проверочного оборудования должен обеспечить безопасность АС в процессе тестирования и сводить к минимуму ложное выполнение любого защитного действия или иного опасного влияния тестов на работу АС. Способ тестирования должен также сводить к минимуму время, в течение которого цепь защиты выводится из обслуживания.

6.1.1.2.5 Ремонтопригодность

a) Система должна быть спроектирована так, чтобы была обеспечена возможность удобного обслуживания и (в случае отказа) простой диагностики, безопасного ремонта или замены и перекалибровки (см. 4.5 МАГАТЭ 50-SG-D8).

b) Для того, чтобы свести к минимуму риск и нагрузку на персонал при выполнении обслуживания, необходимо учитывать возможности человека и ограничения, связанные с факторами окружающей среды.

c) Система должна быть спроектирована так, чтобы была возможность отражать правильность выполненных действий по ремонту и перекалибровке.

Подлежат проверке:

- правильность восстановления соединений в цепи;
- правильность калибровки аналоговых измерений и всех соответствующих аварийных уставок;
- способность системы выполнять предусмотренные функции, важные для безопасности.

Примечание — Требования по обслуживанию и тестированию раздела 10 МЭК 60987 применяют к системам, важным для безопасности. Требования разделов МАГАТЭ 50-SG-D3 — 7.10 (способность к тестированию), 7.11 (резервирование при эксплуатации), 7.12 (контроль доступа) применяют к компьютерным системам класса 1, а разделов 4.5 (способность к тестированию) и 4.6 (ремонтопригодность) МАГАТЭ 50-SG-D8 — к компьютерным системам класса 2.

6.1.1.3 Границы и интерфейсы с другими системами и техническими средствами

Для того, чтобы обеспечить интеграцию системы в архитектуру контроля и управления в соответствии с требованиями раздела 5, необходима следующая информация:

- намечаемое помещение для размещения и физические ограничения, связанные с размещением системы на АС (см. 5.1.3);
- физические и функциональные интерфейсы системы с обслуживающими системами и оборудованием (см. 5.1.3);
- физические и функциональные интерфейсы системы с вспомогательными системами и оборудованием, с которыми она обменивается информацией (см. 5.3.1.3);
- интерфейсы с программными инструментальными средствами, используемыми для обеспечения обмена данными между системами и верификации состояния этих данных (см. 5.3.1.4).

6.1.1.4 Интерфейсы пользователей

Требования к человеко-машинному интерфейсу должны обеспечивать минимальный риск ошибки персонала, например, непредумышленной ошибки, недосмотра, пропуска информации при пуске, эксплуатации, тестировании и обслуживании системы или в процессе проведения модификаций проекта.

Примечание — Защита от злонамеренных изменений рассматривается в плане защищенности (см. 6.2.2).

6.1.1.5 Условия окружающей среды

В соответствии с ограничениями, накладываемыми со стороны проекта АС, следует определить диапазоны нормальных и аварийных условий внешней среды, которые система должна выдерживать (см. 5.1.3). Перечень учитываемых условий среды должен содержать:

- окружающие условия, включая температуру, влажность, давление, уровень радиации и электромагнитных помех при нормальной эксплуатации и в условиях аварий.

Примечание 1 — Внешние условия, связанные с электромагнитными помехами, определяются в соответствии с МЭК 61000 (от МЭК 61000-4-1 — МЭК 61000-4-1);

- окружающие условия, выражающие возможные опасные воздействия, внешние по отношению к системе, выключая сейсмические условия;
- условия энергоснабжения и отвода тепла.

Примечание 2 — Требования к электропитанию систем контроля и управления, важных для безопасности, определяют в соответствии с МЭК 61225.

6.1.1.6 Квалификация

Системы классов 1 и 2 должны быть квалифицированы. Для компьютерных систем такой квалификации подвергается оборудование, системное и прикладное программное обеспечение, установленное в оборудовании (см. 6.4).

6.1.2 Спецификация системы

Цель этой фазы разработки системы — дать высококачественное описание оборудования и структуры программного обеспечения, чтобы определить оборудование, которое должно быть использовано или разработано при создании системы, и назначение прикладных функций.

Спецификация требований к системе и документация на существующее оборудование, которое может использоваться на АС, являются исходными данными для спецификации системы.

Подготовленная в этой фазе (см. 6.3.2) документация является исходной для деятельности, связанной с объединением аппаратного (оборудования) и программного обеспечения системы на последующих фазах жизненного цикла системы.

В соответствии с разделом А.1 приложения А МЭК 60880 на этой фазе определяются требования к программному обеспечению, оборудованию и требования по интеграции системы.

Спецификация системы должна включать в себя:

- используемое оборудование;
- архитектуру системы;
- требования к программному обеспечению;
- распределение прикладных функций по подсистемам.

6.1.2.1 Выбор существующего оборудования

Это наиболее общие существующие компоненты (отдельные компоненты оборудования и программного обеспечения или отдельные компоненты семейства оборудования), используемые для создания части или «новой» системы в целом.

Примечание 1 — Существующие компоненты могут быть покупными или продуктом собственного изготовления производителя.

Примечание 2 — Подраздел 4.3 МЭК 60880-2 посвящен критериям принятия существующего программного обеспечения функций категории А для повторного использования.

a) Пригодность компонентов, которые могли бы использоваться, должна оцениваться и рассчитываться, чтобы показать, что их характеристики соответствуют требованиям к системе.

b) Необходимые оценки и расчеты должны основываться на сравнении информации, полученной из документации двух видов: спецификации требований к системе и документации на существующие компоненты. Последние включают в себя спецификации на изделия и (если доступны) отчеты о квалификации систем.

c) Применяются следующие требования:

- документация должна полностью определять функциональность и свойства всех компонентов.

Примечание — Документация должна включать в себя время загрузки и объем памяти, требующийся для компонентов программного обеспечения, частоту отказов компонентов, рабочие условия внешней среды для системы данной конфигурации, требования к монтажу в шкафах, к кабелям и электропитанию, расходу энергии, устройствам обслуживания;

- свойства, которые установлены недостаточно точно, должны быть уточнены на основе анализа или испытаний;

- в документации должны содержаться показатели надежности и рабочие характеристики, которые определены для прикладных функций при планируемой конфигурации компонентов;

- документация должна определять функциональность и свойства инжиниринговых методов и инструментальных средств программирования;

- должны быть определены избыточные функции (т.е. функции, которые введены в оборудование, но не будут использованы); следует продемонстрировать, что эти функции не приведут к нарушению выполнения требуемых функций.

d) Если обнаружатся расхождения между спецификацией требований к системе и спецификацией семейства оборудования, которые выявят несоответствие оборудования предполагаемому классу системы, то оборудование должно быть отвергнуто. Оценка пригодности должна установить соответствие характеристик рассматриваемого оборудования его назначению согласно спецификации требований к системе (см. 6.3.2.2).

e) Для систем классов 1 и 2 должна проверяться возможность квалификации в соответствии с 6.4.

f) Если квалификация была выполнена ранее, то свойства, вошедшие в данную квалификацию, должны быть точно идентифицированы. Необходимо также установить, какие должны быть выполнены работы по дополнительной квалификации, связанной со спецификой АС.

6.1.2.2 Архитектура системы

Архитектура системы предполагает разделение на ряд взаимосвязанных подсистем и компонентов, которое обеспечивает резервирование и возможность изменения конфигурации. Целью разделения системы является достижение оптимально упрощенного построения оборудования и программного обеспечения, которые отвечают функциональным требованиям, требованиям к эксплуатационным характеристикам и соответствуют требованиям надежности и ремонтопригодности.

Структура подсистем системы должна:

- соответствовать проектным требованиям в соответствии с 6.1.1.2;

- предоставлять возможность выполнить требования к распределению прикладных функций (см. 6.1.2.4);

- соответствовать требованиям к надежности прикладных функций, важных для безопасности (см. 6.1.1.1.1).

6.1.2.2.1 Распределение подсистем по помещениям АС (централизация/децентрализация)

a) При определении мест размещения подсистем на АС и трассировании связей между ними следует учитывать:

- необходимость разделения резервированных каналов оборудования, построенного по мажоритарному принципу с тем, чтобы снизить влияние локальных воздействий (таких как пожар) и обеспечить соответствие критерию единичного отказа (см. 6.1.1.2.1);

- необходимость с целью выполнения требования по контролю за несанкционированным доступом централизации функций, важных для безопасности;

- возможность централизации сложного оборудования для облегчения эксплуатации, периодического тестирования, обслуживания и контроля условий окружающей среды;

- возможность уменьшения сложности кабельного хозяйства при использовании мультиплексной передачи данных.

b) Для систем класса 1 следует использовать средства резервирования передачи информации от мест, к которым при нормальной эксплуатации доступ невозможен (например, из контеймента реактора).

Требования к мультиплексным передачам приведены в МЭК 61500.

6.1.2.2.2 Независимость

Независимость включает в себя условия предотвращения нежелательного взаимного воздействия подсистем данной системы или взаимодействия с другими системами, которые могут возникнуть из-за отклонений от нормальной работы или отказа какой-либо составной части системы или подсистемы. Нежелательное взаимовлияние может возникнуть в результате таких событий, как электромагнитные наводки, короткое замыкание, обрыв заземления, пожар, химический взрыв, падение самолета и распространение искаженной информации.

a) Если требуется независимость (см. 6.1.1.2.1), то она должна достигаться за счет использования:

- электрической изоляции, которая может обеспечиваться посредством применения волоконной оптики, оптических изоляторов, экранирования кабельных линий;
- физического разделения, которое достигается посредством дистанцирования, сооружения барьеров или комбинации двух этих способов;
- независимости коммуникаций компьютерных систем, которая достигается выбором подходящих архитектур передачи данных и протоколов обмена (см. 5.3.1.3).

Примечание 1 — Требования по электрической изоляции и физическому разделению приведены в 4.3 МАГАТЭ 50-SG-D8 и 7.8 МАГАТЭ 50-SG-D3.

b) В системах класса 1 физическое разделение и электрическая изоляция между подсистемами различных групп безопасности должны соответствовать требованиям МЭК 60709.

c) Разделение и изоляция между системами класса 1 и системами и оборудованием, не влияющим на безопасность, должны соответствовать требованиям МЭК 60709.

Примечание 2 — Предпочтительным способом физического разделения и защиты кабелей систем безопасности (как электрических, так и оптических) является использование выделенных кабельных проходок или каналов, обеспечивающих полную защиту от опасных воздействий.

6.1.2.2.3 Защита от развития отказов и их побочных эффектов

Кроме развития отказов, которое можно предотвратить за счет обеспечения независимости, следует рассматривать другие типы развития последствий отказов в компьютерных системах, например:

- непреднамеренное прерывание разделяемых ресурсов (вычислительная мощность, полоса пропускания коммуникаций, память, ресурсы операционной системы и т.д.);
- отказ разблокировки прерванных ресурсов;
- разрушение синхронизации в пределах системы или в пределах архитектуры контроля и управления.

Кроме того, сбой в программе, который препятствует выполнению определенной функции, может привести к отказу других программ, обслуживающих другие функции этой же системы (побочные эффекты). Отказ может произойти вследствие ошибок в данных программах или оборудовании, используемом для выполнения различных функций, например, отказ процессора может привести к отказу других функций вследствие исключения или зависания одной из функций.

Архитектура системы должна минимизировать риск и последствия от развития отказа и побочных эффектов, связанных с отказами. Можно рассматривать следующие технологии:

- внутренняя изоляция, когда отказ не может развиться из-за отсутствия соответствующих путей развития и вследствие разделения ресурсов;
- система мониторинга с помощью внутренних (например, самодиагностика) или внешних (например, другие системы или операторы) средств системы, способных обеспечить раннее выявление искаженных данных и/или отказавших ресурсов;
- защитные интерфейсы, позволяющие системе или ее подсистемам выявлять искаженные входные данные и/или неправильные взаимодействия;
- встроенная валидация резервированных входных сигналов, используемых для последующей обработки;
- строго определенные режимы поведения, используемые для выявления отказа и позволяющие системе снизить вероятность развития отказа и/или его воздействие.

Примечание — Детальные требования, позволяющие избежать склонности программных комплексов к ошибкам, и требования к верификации и испытаниям программных модулей приведены в МЭК 60880 и МЭК 60880-2.

6.1.2.3 Спецификация программного обеспечения

Спецификация программного обеспечения включает в себя:

- спецификацию прикладных функций (характеристики прикладных программ);
- спецификацию архитектуры программного обеспечения.

Примечание 1 — Архитектура программного обеспечения определяет основные компоненты и программное обеспечение подсистем, их взаимосвязь и как требуемые свойства будут достигнуты. Требования к архитектуре программного обеспечения не входят в область применения настоящего стандарта (для систем класса 1 см. МЭК 60880 и МЭК 60880-2);

- спецификацию сервисных функций и функций системного программного обеспечения.

Примечание 2 — Если используется существующее оборудование, то спецификации системного программного обеспечения являются в основном частью документации на оборудование.

a) Для того, чтобы облегчить выполнение спецификации, верификацию и валидацию прикладных функций, архитектура программного обеспечения должна предусматривать четкое разделение между прикладным и системным программным обеспечением (см. B.2a МЭК 60880). В этом случае верификация и валидация прикладного программного обеспечения могут выполняться независимо.

b) Спецификация прикладного программного обеспечения должна основываться на спецификации требований к прикладным функциям (см. 6.1.1.1). При необходимости в нее следует включать связи с функциями контроля и мониторинга системы.

c) Для того, чтобы избежать ошибок при спецификации и верификации, программное обеспечение каждой прикладной функции должно быть по возможности уточнено за счет введения в структуру компонентов со стандартными рабочими характеристиками.

Примечание 3 — Существует покупное оборудование, которое может включать в себя описание разработанного прикладного программного обеспечения с соответствующими средствами, использующими подходящие существующие компоненты библиотеки прикладных программ.

d) Для того, чтобы реализовать поддерживающие режимы работы и свести к минимуму вероятность ошибочных действий, должны быть описаны соответствующие средства отбора и верификации сигналов, а также блокировки.

6.1.2.4 Распределение прикладных функций в системе

Рассматривается распределение:

- входных сигналов запуска или окончания функций по определенным процессорным устройствам;
- процедур голосования, управления по приоритетам, функций защиты оборудования;
- связей выходных управляющих действий с исполнительными устройствами.

a) Распределение функций, важных для безопасности, по системам и подсистемам должно соответствовать спецификациям функциональных требований, требований к рабочим характеристикам и к категоризации функций (см. 6.1.1.1.1).

b) При распределении следует учитывать содержание отказов.

c) Резервированные функции и сигналы, важные для безопасности, не должны обрабатываться в одной и той же подсистеме, чтобы при отказе или при случаях локальных опасных воздействий, возникших в одном канале, система могла бы выполнять свои функции.

d) Функции различных категорий, приданные одной системе или подсистеме, должны рассматриваться как функции наивысшей из их числа категории безопасности, исключая случаи, когда можно показать, что более низкая категория данных и функций не может нарушить работу функций более высокой категории. Это может привести к разделению функций в различных подсистемах или к решению о размещении функций более низкой категории в других системах [итерационный процесс при общем распределении (см. 5.3)].

e) Для функций категории А резервированная обработка не должна выполняться ресурсами той же подсистемы, а резервированные сигналы — направляться по одному и тому же маршруту передачи данных.

f) Функции категории А должны отвечать критерию единичного отказа как при работе, так и в случае, когда одна из резервированных линий защиты заблокирована для проведения операций обслуживания.

6.1.3 Детальное проектирование и реализация системы

Цель данной фазы жизненного цикла безопасности системы состоит в:

- разработке/получении подробного проекта оборудования системы,
- разработке (проектировании и программировании)/получении компьютерных программ, которые составляют операционное и инструментальное программное обеспечение системы.

Примечание 1 — Нормально (см. 6.1.2.2), если выполняются только ограниченное количество новых разработок, например, интерфейсов с другими системами;

- разработке (проектировании и программировании)/генерировании прикладного программного обеспечения системы.

Примечание 2 — Если используется существующее оборудование, то прикладные программы генерируются автоматически теми средствами, которые входят в спецификацию прикладного программного обеспечения (см. 6.1.2.3).

Документация по спецификации системы и план интеграции являются основными исходными данными для фазы детального проектирования и реализации системы.

Результатами данной фазы являются:

- подсистемы и компоненты оборудования и программного обеспечения для последующей фазы интеграции системы;
- компьютерные программы для работы в системе.

Разработка/приобретение оборудования и программного обеспечения являются частью их жизненных циклов и в настоящем стандарте не рассматриваются.

Для систем класса 1 требования к разработке программного обеспечения установлены в МЭК 60880 и МЭК 60880-2, а требования к оборудованию — МЭК 60987.

6.1.3.1 Анализ

6.1.3.1.1 Функциональная валидация спецификации требований к прикладным функциям

Функциональную валидацию проводят с целью выявления ошибок и пропусков в описании прикладных функций, которые могут быть не обнаружены при валидации системы (см. 6.1.5). Функциональная валидация включает в себя моделирование работы АС и оборудования:

a) Для функций категории А должна быть проверена правильность спецификации прикладных функций в сравнении с функциональными и характеристическими требованиями функций АС (см. 5.1.1).

b) Для валидации должны использоваться окончательная версия прикладного программного обеспечения, созданного при детальном проектировании, и соответствующее аппаратное обеспечение.

6.1.3.1.2 Оценка надежности

a) Следует установить, что надежность прикладных функций, выполняемых системой, достаточна. Строгость приводимых обоснований должна быть выше в случае функций высшей категории:

- обоснование должно основываться на разумном сочетании детерминистических критериев и количественного анализа надежности;
- оценивание влияния возможных отказов оборудования на надежность выполнения функции должно проводиться с помощью вероятностного количественного анализа, основанного на интенсивности отказов компонентов. Анализ охватывает архитектуру системы и компонентов и должен учитывать как систематические, так и случайные отказы;
- оценивание влияния возможных ошибок при проектировании программного обеспечения на надежность функций должно основываться на качественном анализе, принимая во внимание сложность проекта, качество разработки, и учитывать опыт эксплуатации подобных объектов. Оценка, основанная на ранее согласованных методиках, должна продемонстрировать то, что качество программного обеспечения соответствует необходимой надежности.

Примечание — Результаты анализа и имитационных испытаний могли бы быть использованы для количественной оценки, но такой методики не существует. Системы жесткой логики обычно не имеют количественной оценки отказов, возникающих из-за ошибок при проектировании.

b) Анализ возможности нежелательного воздействия сервисных функций системы на прикладные функции следует провести с тщательностью, соответствующей важности прикладных функций для безопасности.

c) Если выполняемая системой функция входит в состав комплекса безопасности и существуют требования к надежности, предъявляемые структурой контроля и управления к этому комплексу (см. 5.3.3.1), то анализ надежности следует проводить с учетом последствий единичных отказов, отказов по общей причине и развития отказов для всех систем, входящих в данный комплекс безопасности.

d) Для систем класса 1 при анализе надежности следует также оценивать соответствие оборудования для испытаний системы требованиям 6.1.1.2.4.

6.1.4 Интеграция системы

Цель данной фазы — соединение узлов оборудования и модулей программного обеспечения и проверка совместимости загруженного в оборудование программного обеспечения (см. раздел 7 МЭК 60880).

Подсистемы и компоненты системы, детальная документация по разработке, план интегрирования системы являются составными частями фазы интеграции системы.

Результатом выполнения этой фазы является интегрированная система.

a) Интеграция должна проводиться в соответствии с планом, определенным в 6.2.3.

b) После того, как все прикладные программы (как созданные с помощью инструментальных средств семейства оборудования, так и специально разработанных) загружены в систему, необходимо проверить соответствие требованиям к рабочим характеристикам.

c) На фазе интеграции должно быть проведено тестирование, которое показало бы, что каждая выбранная прикладная функция выполняет поставленную задачу.

Примечание — В зависимости от технологии проектирования, используемой для обеспечения детерминированного поведения системы (см 6.1.1.2.2), может оказаться необходимым проведение испытаний, использующих как случайные данные при большой скорости их изменения, так и входные сигналы других функций внутри той же компьютерной системы.

6.1.5 Валидация системы

Цель этой фазы — проверка интегрированной системы на соответствие спецификациям функций, характеристик и интерфейсов (см. раздел 8 МЭК 60880).

Интегрированная система, документация спецификации системы и план валидации системы являются основными исходными данными на этой фазе.

a) Валидация системы должна проводиться в соответствии с планом, определенным в 6.2.4.

b) При валидации функций категории А следует применять требования раздела 8 МЭК 60880.

c) При валидации функций категорий В и С следует применять требования раздела 8 МЭК 60880 со следующими дополнениями.

- уровень детализации испытаний должен быть таким же, но объем испытаний может быть уменьшен в соответствии с целями функций, важных для безопасности;

- не требуется, чтобы группа, ответственная за валидацию системы, была независимой от разработчиков.

6.1.6 Внедрение системы

Цель этой фазы — установка системы, выполнение межсоединений и испытание ее на площадке АС.

Последующие действия, связанные общей интеграцией системы с другими системами и общей приемкой, являются частью полного жизненного цикла безопасности контроля и управления (см. раздел 7).

a) Внедрение системы должно проводиться в соответствии с планом, определенным в 6.2.5.

b) Подходящие средства, например, этикетки или цветная маркировка, должны использоваться для идентификации компонентов, кабелей и оборудования, составляющего систему для снижения вероятности ошибок при монтаже, эксплуатации и обслуживании.

6.1.7 Модификация проекта системы

Может потребоваться внесение изменений в проект системы вследствие возникновения новых требований или обнаружения дефектов проекта при оценке эксплуатационных записей и отчетов.

a) Реализация модификации должна проводиться в соответствии с заранее определенными процедурами (см. 6.3.6).

b) После проведения модификации необходимо проверить работу системы.

c) Не допускается внесение изменений в оборудование и программное обеспечение, кроме тех, которые определены условиями проведения операций обслуживания.

d) Если потребуется замена оборудования, необходимо показать/подтвердить, что замена соответствует первоначальной спецификации на оборудование.

e) Для систем класса 1 процесс модификации программного обеспечения должен соответствовать требованиям раздела 9 МЭК 60880, а процесс модификации оборудования — разделу 11 МЭК 60987.

6.2 Планирование системы

Цель настоящего подраздела — разработка планов, обеспечивающих условия, при которых системой выполняются и будут поддерживаться требования к назначенным ей функциям контроля и управления, важным для безопасности.

Требования 5.4 относятся к соответствующим общим планам для данных функций, распределенных по взаимосвязанным системам.

Примечание — Требования к планированию не означают, что планы могут быть реализованы в ряде различных документов.

Планы системы должны разрабатываться на ранней стадии жизненного цикла системы до начала любой деятельности по реализации системы.

6.2.1 Программа обеспечения качества системы

a) Программа обеспечения качества должна охватывать каждый вид деятельности в жизненном цикле безопасности системы. Требования к плану обеспечения качества системы взяты из МАГАТЭ 50-С-QA (Редакция1) и ИСО 9001.

b) Программа обеспечения качества системы должна включать в себя направления деятельности, которые необходимы для достижения необходимого качества системы, для проверки достижения требуемого качества и получения соответствующих подтверждений этого [см. раздел 102 МАГАТЭ 50-С-QA (Редакция 1)]. Требования к деятельности по проверке установлены верификационным планом системы (см. 6.2.1.1).

c) Программа обеспечения качества системы посвящена качеству системы и аспектам, связанным с качеством интеграции оборудования и программного обеспечения. Планы обеспечения качества собственно оборудования и программного обеспечения находятся вне области применения настоящего стандарта.

Примечание — Требования к программе обеспечения качества систем безопасности определены в разделе 3 МЭК 60880.

d) Программа обеспечения качества системы должна содержать:

- указания на национальные стандарты и методики, используемые при проектировании (в соответствии с 4.2.2 ИСО 9001);
- определение фаз жизненного цикла системы, основные задачи и ожидаемый результат выполнения каждой фазы (в соответствии с 4.4.2 ИСО 9001);
- описание отношений между различными задачами и их взаимодействий (в соответствии с 4.4.3 ИСО 9001);
- описание организационной структуры (в соответствии с 4.1.2 ИСО 9001);
- перечень покупных компонентов внешних поставщиков (в соответствии с 4.6. и 4.7 ИСО 9001);
- идентификация изделий и маркировка (в соответствии с 4.8 ИСО 9001-3). Соответствующие требования установлены в плане управления конфигурацией (см. 6.2.1.2);
- определение всех инспекционных процедур и проверок (в соответствии с 4.10 ИСО 9001);
- определение видов деятельности и задач обеспечения качества;
- определение персональной/организационной ответственности за деятельность и задачи по обеспечению качества, включая обеспечение независимости [в соответствии с МАГАТЭ 50-С-QA (Редакция 1)];
- процедуры отчетности о несоответствиях требованиям, стандартам и методикам. Процедуры должны включать в себя рассмотрение влияния на безопасность АС и обеспечивать определение всех видов воздействий, возникающих в ходе несоответствия требованиям, например, на взаимозаменяемость, обслуживание, запасное оборудование, инструкции по эксплуатации и т.д. (в соответствии с 4.13 ИСО 9001).

e) Программа обеспечения качества должна создаваться на ранней стадии жизненного цикла системы и входить в общую программу деятельности в рамках жизненного цикла безопасности контроля и управления. Программа может быть частью спецификации на систему или быть отдельным документом (см. 3.2 ИСО 60880).

6.2.1.1 Верификационный план системы

a) Верификационный план системы должен описывать:

- процесс верификации на всех фазах жизненного цикла безопасности системы;
- соответствующую организацию и ответственность.

b) Результаты, полученные на каждой фазе жизненного цикла безопасности системы, должны быть сверены с запланированными перед ее началом.

c) Каждый шаг верификации должен завершаться отчетом о проделанном анализе и выводами относительно достигнутого результата. После завершения фазы должен быть подготовлен завершающий отчет, показывающий соответствие результатов первоначальным требованиям и заключение относительно отклонений.

d) Верификация должна проводиться лицом, компетентным в вопросах безопасности системы, хорошо разбирающимся в исходных требованиях, по отношению к которым проводится верификация.

e) Основательность верификационного плана должна быть соразмерна классу безопасности системы. В верификационном плане должно уделяться большое внимание вопросам, связанным с безопасностью, требующим верификации, при этом следует учитывать, что вероятность ошибки или пропуска в сложном узле гораздо больше, чем в простом.

f) Документы, подлежащие пересмотру, должны определяться в плане обеспечения качества системы.

g) Документы, относящиеся к деятельности по верификации, например, исходные требования и результаты деятельности, верификационные отчеты и, возможно, средства, использованные для достижения результата, должны быть учтены в планах управления конфигурацией.

h) Для систем класса 1 верификация должна проводиться лицом, независимым от разработчиков системы (в соответствии с 6.2.1 МЭК 60880).

6.2.1.2 План управления конфигурацией системы

Примечание — Часть требований к плану управления конфигурацией системы (см. ниже) заимствована из IEEE 828 [3].

a) Идентификация конфигурации:

- должны быть определены основное направление (критический путь) с контрольными точками в пределах жизненного цикла системы, а также объекты, подлежащие контролю. Контролируемые объекты могут быть промежуточными или окончательными (например, оборудование, программное обеспечение, документация по верификации, инструкции пользователя), а также элементами инструментальной среды (например, компиляторы, инструментальные средства, испытательные стенды);

- все объекты, подлежащие контролю, должны быть идентифицированы; каждый отдельный объект должен иметь собственный адрес, а также должны быть однозначно определены различные варианты конфигурации;

- связи между устройствами, находящимися на критическом пути, и устройствами, из которых они были собраны, должны быть установлены и зарегистрированы;

- управление конфигурацией системы должно обеспечивать изменение конфигурации всех критических путей системы;

- должны быть предусмотрены поисковые средства, с помощью которых можно легко определить связи и многократное применение объектов.

b) Контроль конфигурации:

- для контроля конфигурации должны быть предусмотрены средства приостановки проекта; необходимо определить процедуры и обоснование для любой корректировки проекта после его приостановки;

- необходимо отслеживать статус каждого контролируемого объекта, что подразумевает получение сведений о первоначальной согласованной версии, статусе предлагаемых изменений, а также внедрении согласованных изменений.

c) План управления конфигурацией должен разрабатываться в начале проектирования и поддерживаться в течение всего жизненного цикла системы.

6.2.2 План защищенности системы

План защищенности системы разрабатывается в соответствии с общим планом защищенности (см. 5.4.2):

a) В процессе разработки спецификации на систему и при проектировании требований к техническим контрмерам, определенным для системы в общем плане защищенности (см. 5.4.2), должны трансформироваться в требования технического проекта и быть документально оформлены.

b) Для проверки правильного применения контрмер, определенных при проведении анализа защиты системы, должна быть проведена оценка проектной документации.

c) При верификации и валидации системы путем испытаний в ее окончательной конфигурации должна быть продемонстрирована эффективность функций защищенности.

6.2.3 План интеграции системы

План интеграции системы определяет технические и организационные меры по объединению подсистем в систему и интеграции оборудования и программного обеспечения. План охватывает следующие действия, описанные в 7.4 МЭК 60880:

a) в плане интеграции системы должны быть описаны типы необходимых испытаний, проверка воздействий окружающей среды и критерии приемки;

b) испытания интеграции должны проводиться в соответствии с концепцией поэтапной интеграции;

c) необходимо различать испытания, связанные с самой системой (функции аппаратного и программного обеспечения системы), и испытания, относящиеся к функционированию АС (прикладные функции).

Примечание — Для того, чтобы избежать проведения идентичных испытаний или необязательных проверок, могут быть использованы результаты испытаний модулей (оборудование, программное обеспечение, комбинированные модули), проведенных в процессе типовых испытаний или предыдущих проектов.

6.2.4 План валидации системы

План валидации системы охватывает технические и организационные меры, осуществляемые с целью демонстрации соответствия спецификации системы и спецификации технических требований на систему. Валидацию требований к прикладным функциям рассматривают на фазе функциональной валидации (см. 6.1.3.1.1).

a) План валидации системы должен содержать описание конфигурации(й) системы, подлежащей проверке, сведения об испытаниях, аналитических оценках и отчетах, которые необходимо выполнять:

1) соответствующая документация должна определять конфигурацию системы, подлежащую валидации, входные данные, используемые методики, устройства и средства калибровки, а также подходящие критерии приемки. Если критерии являются подходящими, то должны оцениваться точность и влияние средств измерения на характеристики системы;

2) документы по анализу валидации должны определять, что анализ должен показать ожидаемые результаты и подходящие критерии приемки.

b) Для функций категории А план валидации системы должен разрабатываться и выполняться группой специалистов, не зависящих от разработчиков системы, лиц, участвовавших в реализации системы, и/или тех, кто занимается модификацией системы (см. раздел 8 МЭК 60880).

Примечание — Независимость лиц, привлеченных к выполнению плана валидации и подготовке отчета по ее итогам, не требуется.

c) Для функций категории В за разработку плана валидации системы должны отвечать лица, не участвовавшие в проектировании, реализации и/или модификации системы.

d) Для функций категорий А и В план валидации должен обеспечивать связь между спецификацией и соответствующими испытаниями и верификациями.

e) Рекомендуется, чтобы для функций категории С план валидации обеспечивал связь между спецификацией и соответствующими испытаниями и верификациями.

6.2.5 План внедрения системы

План внедрения системы охватывает организационные и технические меры по установке системы на АС и проверке, необходимой для подтверждения готовности системы к эксплуатации. План дополняется общими планами интеграции и приемки (см. 5.4.3).

a) План внедрения системы должен описывать необходимые действия для подтверждения того, что конфигурация системы и любой из настраиваемых параметров верна, система укомплектована, правильно установлена, смонтирована, соединена и может работать в соответствии с разработанными специфицированными требованиями.

b) Для систем класса 1 план внедрения должен соответствовать требованиям раздела 9 МЭК 60987 и 10.1.1 МЭК 60880.

c) Для функций категории А необходимо продемонстрировать, что каждый канал безопасности работает на месте установки правильно.

6.2.6 План эксплуатации системы

План эксплуатации содержит порядок, в соответствии с которым эксплуатируется система, и требования, действующие в течение эксплуатации системы.

a) План эксплуатации системы должен определять, как система должна эксплуатироваться во всех режимах работы. План должен соответствовать плану обслуживания (см. 6.2.7) и общим планам эксплуатации и обслуживания (см. 5.4.4 и 5.4.5).

b) План эксплуатации должен определять условия, которым система должна соответствовать прежде чем она будет запущена в эксплуатацию. В частности:

- система должна быть полностью установлена, интегрирована и принята (см. 5.4.3);
- в наличии должны быть план обслуживания (см. 6.2.7) и эксплуатационные документы пользователя.

c) Если требуются периодические испытания (см. 6.1.1.2.4), то план эксплуатации должен определять:

- частоту и продолжительность каждого испытания, условия, которые следует выполнять, прежде чем приступить к испытаниям, и воздействия, при их наличии, на эксплуатацию системы и энергоблока;
- необходимые этапы проведения каждого испытания, приборы и средства калибровки, анализ правильности результатов;

- верификацию полного восстановления нормального состояния, если требуются временные изменения в системе.

Примечание — Периодические испытания проводятся совместно подразделениями АС, занимающимися эксплуатацией и обслуживанием. Это направление деятельности может рассматриваться как часть регламентного обслуживания (см. 6.2.7).

d) План эксплуатации должен определять порядок ведения записей, которые должны выполняться в течение эксплуатации. Записи должны включать в себя детальное описание отказов, отметки о проведенных тестах системы и записи запросов системы.

e) План эксплуатации должен рассматриваться с точки зрения его воздействия на безопасность станции.

f) Для систем классов 1 и 2 план должен содержать требования периодического тестирования системы в соответствии с требованиями вероятностного анализа.

g) Для систем класса 3 план должен определять проведение периодического тестирования системы через конкретные интервалы времени, если условия непрерывной эксплуатации не гарантируют выявления отказов.

6.2.7 План обслуживания системы

Обслуживание системы включает в себя организационные и технические меры, необходимые для поддержания работоспособности находящейся в эксплуатации системы. План обслуживания системы разрабатывают в соответствии с планом эксплуатации системы и общими планами эксплуатации и обслуживания (см. 5.4.4 и 5.4.5).

a) План обслуживания системы должен определять:

- регламентные действия и операции, которые следует применять для выявления неявных отказов системы, поддержания проектных режимов работы и надежности системы (профилактическое обслуживание);

- действия и операции, которые необходимо проводить, чтобы содержать систему в полностью работоспособном состоянии (корректирующее обслуживание).

b) Объем профилактического обслуживания должен определяться на основе метода системного анализа, такого, например, как анализ характера отказа и его влияния на работу системы, или на основе применения модели обслуживания, основанной на характеристиках надежности, или изучения деревьев отказов функций системы.

c) Процедуры замены компонентов должны гарантировать, что:

- установленные компоненты функционально идентичны замененным и соответствуют требованиям качества;

- если замена проводится без прерывания работы системы, то ее воздействие на работоспособность системы оценивается и документально оформляется до проведения операции;

- ведутся записи о всех заменах, позволяющие выполнить все требования по наблюдению и учету.

d) Процедуры по перекалибровке должны гарантировать, что:

- новая калибровка выполняется в определенных пределах (если такие пределы установлены системой, то нет необходимости предъявлять требования к действию обслуживающего персонала);

- если перекалибровка проводится без прерывания работы системы, то ее воздействие на работоспособность системы оценивается и документально оформляется до проведения операции;

- ведутся записи всех операций перекалибровки, позволяющие выполнить все требования по наблюдению и учету.

6.3 Выходная документация

Настоящий подраздел определяет выходную документацию на фазах жизненного цикла системы: содержание, характерные черты и основные разделы, которые необходимо верифицировать.

Выходная документация должна представлять собой ряд взаимосогласованных документов, которые подтверждают соответствие окончательного проекта исходным требованиям.

6.3.1 Документация на спецификацию требований к системе

6.3.1.1 Содержание

Спецификация требований к системе должна быть полной, содержать всю информацию, необходимую для последующей деятельности в течение жизненного цикла безопасности системы и квалификации системы.

6.3.1.2 Характерные черты

Характерные черты документа, содержащего спецификацию требований к системе:

a) требования должны быть верифицируемыми.

Примечание 1 — Подраздел 4.3 IEEE 830 [2] содержит правила по проверке верифицируемости требований;

b) требования должны быть ясными и точными с тем, чтобы они были недвусмысленно понятны всем заинтересованным лицам, включая рецензентов и лиц, отвечающих за спецификацию системы и функциональную валидацию.

Примечание 2 — Например, в противоположность документу, приводящему обширные объяснения и дополнительную информацию, документ с точным и исчерпывающим изложением требований способствует ограничению риска неправильной интерпретации. Наиболее подходящим путем достижения этих целей является написание требований в соответствии с руководящими документами, такими как IEEE 830 [2] и EWICS № 6 [5];

c) требования к прикладным функциям следует излагать в терминах, связанных с функционированием, а не с компьютерной технологией, чтобы сделать доступной работу по верификации для инженеров-технологов и оперативного персонала, занимающихся контролем и управлением, которые могут иметь ограниченные познания в области компьютерной технологии;

d) требования должны разрабатываться с использованием документированных инжиниринговых методов, инструментальных средств и руководств системы.

Примечание 3 — Детальные требования к программным инструментам для систем класса 1 приведены в 4.2 МЭК 60880-2;

e) для того, чтобы облегчить выполнение оценки соответствия спецификации на систему и обеспечить связь с планом квалификации системы, требования рекомендуется излагать в письменном структурированном виде.

6.3.1.3 Верификация

Должны быть верифицированы следующие пункты спецификации требований:

a) требования должны быть прослеживаемыми и должны соответствовать требованиям к системе, установленным при разработке проекта архитектуры и распределении функций (см. 5.5);

b) требования к интерфейсам должны согласовываться с требованиями на взаимосвязанные системы и оборудование;

c) необходимо выявить требования, которые необоснованно увеличивают сложность системы (сложность может привести к увеличению риска ошибок в требованиях на систему и/или в самой системе).

6.3.2 Документация по спецификации системы

6.3.2.1 Содержание

a) Документация по спецификации системы должна быть полной и представлять всю информацию, необходимую для последующей деятельности в течение безопасного жизненного цикла системы, особенно в фазах проектирования и валидации системы.

b) Документация по спецификации системы должна определять, будет ли использоваться покупное оборудование или должно разрабатываться новое. Следует подтвердить, что выбранное оборудование пригодно для создания системы.

c) Документация по спецификации системы должна описывать следующую архитектуру системы:

- декомпозицию системы на подсистемы и/или на компоненты оборудования и программного обеспечения;
- внутреннее поведение системы (см. 6.1.1.2.2), включая описание основных внутренних для системы событий и ее защиту от этих событий (см. 6.1.2.2.3);
- границы, условия окружающей среды, ожидаемую надежность оборудования, поведение, функции, характеристики и интерфейсы каждой подсистемы;
- классификацию каждой подсистемы; следует представить обоснование, если подсистема окажется более низкого класса, чем система или подсистема, в которую она входит;
- условия эксплуатации и связь подсистем с системой.

Примечание — Описание подсистем может выполняться в соответствии с иерархией так, чтобы облегчить восприятие от общей схемы вниз до элементарных подсистем (т.е. подсистем, которые не могут далее дробиться в проектной документации). Может быть также полезна информация, показывающая «горизонтальные» связи.

d) Документация по спецификации системы должна включать в себя спецификацию программного обеспечения (см. 6.1.2.3).

e) В системах классов 1 и 2 должно быть определено распределение функций по подсистемам, т.е. спецификация системы должна определять, какие подсистемы участвуют и/или являются необходимыми для выполнения конкретной функции.

6.3.2.2 Характерные черты

Характерные черты документации по спецификации системы:

a) документация должна быть ясной и четкой, чтобы ее недвусмысленно могли понять все заинтересованные читатели, особенно рецензенты, а также изготовители системы и лица, выполняющие работы по интеграции и валидации;

b) спецификация прикладных функций должна быть выполнена так, чтобы облегчить верификацию и понимание со стороны инженерного и оперативного персонала АС, связанного с системами контроля и управления;

c) спецификация системы должна разрабатываться с использованием документированных инженерных методов, инструментальных средств и руководств системы. Эти методы, средства и руководства должны минимально отличаться от методов, средств и руководств, используемых при спецификации требований к системе.

Примечание — Методы и средства разработки программного обеспечения могут улучшить качество проектной спецификации на систему даже в сравнении с проектной спецификацией на систему с жесткой логикой;

d) спецификация на систему должна быть написана и упорядочена с тем, чтобы облегчить выполнение оценки соответствия требованиям к системе и обеспечить основу для проведения проверки системы, т.е. она должна облегчить полную идентификацию спецификаций (вместо объяснений и привлечения дополнительной информации).

6.3.2.3 Верификация

a) Верификацию спецификации системы на соответствие спецификации требованиям к системе следует проводить до завершения разработки детального проекта. Должна быть возможность для внесения поправок до установки на месте и сборки системы.

b) Должна быть установлена эффективная связь между ответственными за спецификацию системы и поставщиками оборудования для определения порядка верификации.

c) Верификация должна документально подтвердить соответствие и зарегистрировать любое несоответствие спецификации системы спецификации требований к системе.

d) Необходимо верифицировать правильность передачи из спецификации требований к прикладным функциям в спецификацию прикладного программного обеспечения.

e) Для систем классов 1 и 2 любое несоответствие должно быть устранено или обосновано с точки зрения безопасности за счет введения возможных компенсирующих мер.

f) Для систем классов 1 и 2 компоненты, увеличивающие сложность системы, но не обусловленные требованиями к ней, должны быть выявлены, а их наличие обосновано с точки зрения безопасности.

Примечание — Наличие особенностей, не предусмотренных спецификацией требований к системе, может значительно увеличить сложность системы, что ведет к снижению уверенности в ее правильной работе.

6.3.3 Документация детального проекта системы

Проект может осуществляться в несколько стадий. Требования настоящего пункта относятся к окончательному варианту документации на систему, которая должна быть в наличии после завершения проектных работ, интеграции и валидации, когда система готова к поставке и внедрению на АС.

Документация детального проекта системы обычно может быть разделена на четыре группы:

- документация проекта системы;
- необходимый анализ (см. 6.1.3.1);
- документация на прикладное программное обеспечение;
- документация на компоненты оборудования и системное программное обеспечение.

Примечание 1 — Если система выполнена с применением существующих технических устройств, то проектная документация на оборудование системы и программное обеспечение является частью документации на существующее оборудование.

Рассматриваются только первые две группы, поскольку проекты программного обеспечения и оборудования не входят в область применения настоящего стандарта (см. 6.1.3).

Примечание 2 — Для систем класса 1 требования к документации на программное обеспечение установлены в МЭК 60880, МЭК 60880-2, а требования к документации на оборудование — МЭК 60987.

6.3.3.1 Содержание

a) Документация проекта системы должна быть полной, представлять всю информацию, необходимую для дальнейшей деятельности по обеспечению жизненного цикла безопасности системы, включая интеграцию, валидацию, внедрение, эксплуатацию и обслуживание.

b) Документация проекта системы развивает содержание документации спецификации и должна представлять детальное описание внутренней структуры и внутреннего поведения системы. Уровень детализации описания может быть соотнесен с классом безопасности системы.

c) Документация проекта системы должна включать в себя описание внедрения оборудования на АС и проведения испытаний.

d) Документация проекта системы должна включать в себя описание функциональности и рабочих характеристик системы, которые должны подвергаться валидации, в частности, ожидаемое время отклика при различных условиях на АС, номинальная настройка уставок и алгоритмы управления, а также диапазоны безопасного регулирования.

6.3.3.2 Характерные черты проектной документации

Характерные черты проектной документации на систему:

a) документация должна быть ясной и четкой, так чтобы каждая часть была однозначно понятной заинтересованным специалистам, включая разработчиков и рецензентов плана интеграции, плана квалификации системы, плана внедрения и приемки и плана обслуживания системы, обслуживающему персоналу, разработчикам и рецензентам модификаций проекта.

b) должно быть обеспечено внесение изменений в документацию детального проекта системы в течение его разработки, чтобы гарантировать возможность применения окончательной версии документации для реализации системы.

6.3.3.3 Верификация

a) Верификация детального проекта системы и его документации должна проводиться до реализации нового оборудования и программного обеспечения; должно быть предусмотрено время для внесения поправок, необходимость которых выявлена при верификации.

b) Требования к надежности прикладных функций системы (см. 6.1.3.1.1) должны верифицироваться на возможность их выполнения на ранней стадии детального проекта.

Примечание — Анализ надежности системы может потребовать внесения поправок в детальный проект, архитектуру системы, например, изменить степень резервирования и даже решения по выбору полной архитектуры контроля и управления.

c) Основываясь на оценке влияния прикладных функций на безопасность, следует провести строгий анализ возможности их искажения при выполнении сервисных функций.

d) Допущения, внесенные при верификации детального проекта, должны быть сформулированы и представлены в виде документа.

6.3.4 Документация по интеграции системы

6.3.4.1 Содержание

Документация по интеграции системы должна включать в себя план интеграции, отчет о проведенных при интеграции испытаниях и всю информацию, необходимую для последующей фазы валидации.

6.3.4.2 Характерные черты

a) Отчет о проведенных при интеграции испытаниях должен содержать:

- варианты модулей оборудования и программ, спецификацию проведенных испытаний, использованные инструментальные средства и оборудование, а также любые данные, относящиеся к калибровке;
- результаты каждого испытания с перечнем всех несоответствий между ожидаемым и действительным результатами, и для каждого несоответствия — описание проведенного анализа и принятых решений о продолжении испытания либо о внесении изменения.

b) Для систем класса 1 применяют требования 7.7 МЭК 60880.

6.3.4.3 Верификация

a) Верификация отчета об интеграции системы на соответствие плану интеграции должна проводиться до проведения валидации.

b) Для систем классов 1 и 2 с целью обеспечения возможности оценки результатов испытаний и анализа их достаточности должна быть установлена четкая прослеживаемость связи документации детального проекта с соответствующими компонентами, интеграционными испытаниями и анализом.

6.3.5 Документация по валидации

6.3.5.1 Содержание

Документация по валидации должна включать в себя план валидации и отчет о проведении валидации, а также всю информацию, необходимую для квалификации системы.

6.3.5.2 Особенности

Для систем класса 1 применяют требования 8.1 МЭК 60880.

6.3.5.3 Верификация

Результаты валидации и их анализ должны документироваться и сравниваться с требованиями, представленными в плане валидации системы с тем, чтобы подтвердить, что режим функционирования системы соответствует этим требованиям.

Примечание — Рассматриваемая документация вместе с документацией по функциональной валидации (см. 6.3.3.1) должна отражать соответствие системы как спецификации на систему, так и спецификации требований к ней.

6.3.6 Документация по модификации системы

6.3.6.1 Содержание

a) Заявка на модернизацию

Эта документация должна содержать:

- обоснование изменений и влияние (если оно ожидается) на безопасность АС;
- функциональное описание изменения (с выполненными чертежами, диаграммами потоков, структурными схемами и пр.) и предполагаемые технические средства для реализации изменения;
- связь данного изменения с любыми другими изменениями на АС.

b) Комплект документации на внесение изменений.

По окончании внесения изменения в проект, т.е. в программное обеспечение, компоненты оборудования и документацию, отражающую изменение проекта, должна быть подготовлена документация на внесение изменений в работающую систему. Комплект документации должен описывать узлы оборудования, программные модули и средства для введения изменения, т.е. какое оборудование должно быть введено, какая операция должна быть выполнена для загрузки нового программного обеспечения, а если используется известная процедура, то следует дать на нее ссылку.

6.3.6.2 Характерные черты

Заявка на модификацию должна быть однозначно идентифицирована и рассмотрена компетентными специалистами. Результат рассмотрения (принять или не принять) должен быть оформлен документально.

6.3.6.3 Верификация

a) Для систем класса 1 весь комплекс документов на внесение изменения должен быть оценен на полноту и правильность технического решения специалистами, не принимавшими непосредственного участия в разработке проекта внесения изменения, но компетентными для оценки предлагаемого технического решения.

b) Комплекс документации не может быть использован без оценки вносимого изменения.

6.4 Квалификация системы

Настоящий подраздел устанавливает требования к процессу квалификации систем контроля и управления классов 1 и 2 (см. 6.1.1.6). Этот процесс дает уверенность в том, что система контроля и управления способна длительное время соответствовать проектным требованиям, необходимым для обеспечения выполнения функций, важных для безопасности, в оговоренных условиях эксплуатации.

6.4.1 План квалификации

Должен быть разработан план квалификации, который бы определил все аспекты, подлежащие оценке, для достижения и поддержания квалификации системы и функций, важных для безопасности, которые она выполняет.

6.4.1.1 Квалификация оборудования

Примечание — Квалификацию оборудования называют также «квалификацией по выполняемым функциям и условиям окружающей среды».

Для квалификации оборудования системы может использоваться несколько методик. Они включают в себя типовые, функциональные испытания, теоретические оценки, а также накопленный в этой области опыт. Предпочтительным является метод, основанный на проведении типовых испытаний (см. МЭК 60780).

a) Систему следует квалифицировать по условиям окружающей среды в соответствии с требованиями МЭК 60780 и МЭК 60987. Условия окружающей среды должны включать в себя те из них, которые указаны в 6.1.1.5.

b) Должна быть определена подходящая последовательность испытаний компонентов или комплексов компонентов или системы в целом, с тем чтобы:

- проверить функциональные характеристики при нормальных внешних условиях и при всех заданных предельных условиях эксплуатации;
- подтвердить устойчивость к сейсмическим воздействиям.

6.4.1.2 Квалификация программного обеспечения

Примечание 1 — Квалификацию программного обеспечения называют также «определением (качества, пригодности) и оценкой программного обеспечения» («software evaluation and assessment»).

Квалификация программного обеспечения учитывает, насколько строго соблюдался процесс разработки программного обеспечения, а также объем испытаний и валидации, проводимых на интегрированной системе. Для ранее разработанного программного обеспечения опыт его эксплуатации может при определенных условиях компенсировать недостаток информации о процессе разработки.

Программное обеспечение компьютерных систем, подлежащее квалификации, должно включать в себя:

- системное программное обеспечение, которое может быть ранее разработанным и даже не для АС;
- прикладное программное обеспечение, интегрированное в систему, которое разработано специально для АС.

a) Для того, чтобы быть уверенным, что качество программного обеспечения достаточно для достижения требуемой надежности функций, выполняемых системой, квалификация должна быть выполнена как для системного, так и для прикладного программного обеспечения.

b) Для систем класса 1 вновь разработанное программное обеспечение следует квалифицировать в соответствии с требованиями МЭК 60880.

c) Программное обеспечение уже использовавшегося ранее оборудования, выбранного для систем класса 1, должно было разработано в соответствии с известными правилами и стандартами, обеспечивающими высокое качество, требуемое для функций категории А (см. 8.1.2 МЭК 61226). В частности, должны быть удовлетворены требования МЭК 60880-2 к ранее разработанному программному обеспечению и программным инструментам и требования МЭК 60987.

Примечание 2 — МЭК 60880-2 определяет критерии применения и ограничения на использование в процессе квалификации документированных данных прошлого опыта эксплуатации.

d) Программное обеспечение уже использовавшегося ранее оборудования, выбранного для систем класса 2, должно было разработано и выполнено в соответствии с известными правилами и стандартами. Может также использоваться программное обеспечение квалифицированного покупного оборудования с известной из документации историей удовлетворительной работы в подобных применениях (см. 8.1.2 МЭК 61226).

Примечание 3 — Критерии применения программного обеспечения покупного оборудования класса 2 с известным опытом эксплуатации являются предметом разработки будущего стандарта МЭК по программному обеспечению систем класса 2.

6.4.1.3 Аспекты квалификации, связанные с семейством оборудования и спецификой АС

Как показано на рисунке 6, квалификация системы включает в себя аспекты, связанные:

- с изделиями, которые могут быть выполнены не специально для АС, и применение которых могло быть предварительно оценено;

- со спецификой системы, которая оценивается в течение ее жизненного цикла применения на АС.

a) При квалификации оборудования и программного обеспечения системы, построенной путем конфигурирования семейства оборудования (см. 6.1.2.1), можно исходить из ранее проведенной квалификации отдельных и конфигураций взаимосвязанных компонентов. В таком случае необходимо провести анализ, который показал бы, что процесс квалификации охватывает окончательную конфигурацию системы для применения на АС, включая монтаж, загрузку и распределение температуры внутри шкафов.

b) Основанный на предыдущем анализе план квалификации должен идентифицировать в проекте системы все новые узлы и определить, должны ли быть проведены дополнительные квалификационные испытания и оценки.

6.4.2 Дополнительная квалификация взаимодействующих систем

a) Может потребоваться разработка плана дополнительных испытаний на уровне взаимодействующих систем контроля и управления в дополнение к их индивидуальной квалификации, например, испытания на электромагнитную совместимость отдельных линий связи и заземления.

b) Возможность проведения и содержание дополнительных испытаний должны быть проверены при верификации проекта архитектуры контроля и управления.

6.4.3 Поддержание квалификации

a) Должен быть установлен дополнительный план поддержания квалификации в процессе эксплуатации и обслуживания системы, когда проводится замена некоторых частей системы на другие, которые не являются идентичными, а также в случае функциональных модификаций.

b) Дополнительный план должен содержать идентификацию модулей, которые выполняют функции категорий А и В соответственно, чтобы обеспечить соответствие принятым версиям, подтвержденным в процессе валидации.

6.4.4 Документация

a) Должен быть подготовлен перечень информации, которая должна представляться лицензирующему органу.

b) В перечне должно быть сделано различие между информацией, необходимой до внедрения системы, и информацией, которую следует предоставлять лицензирующему органу в процессе внедрения и приемки системы, например, отчеты об испытаниях. Может потребоваться следующая информация:

- описания (подробные изложения фактов);
- разъяснения (изложение фактов с аргументацией);
- демонстрации;
- подтверждения;
- доказательства (последовательные доводы, которые доказывают утверждения).

c) Документация может быть сгруппирована в соответствии с назначением, но она должна содержать:

- отчет о предварительном анализе безопасности и обобщающие документы для оценки концепции и основ проекта системы;
- подробные описания всей системы или ее частей, позволяющие провести независимую верификацию и валидацию. Эта документация может содержать подробную информацию о типовых испытаниях компонентов;
- подробные или краткие разъяснения, демонстрации или доказательства, необходимые для подтверждения проектных решений и упрощения процессов независимых верификации и валидации;
- информацию, касающуюся внедрения, интеграции, приемки, приемочных испытаний на заводе поставщика и на АС, для того чтобы обеспечить верификацию на тех этапах жизненного цикла безопасности, которые находятся между фазами проектирования и эксплуатации;
- информацию, необходимую для работы системы, чтобы верифицировать процедуры поддержания качества системы в течение длительного времени.

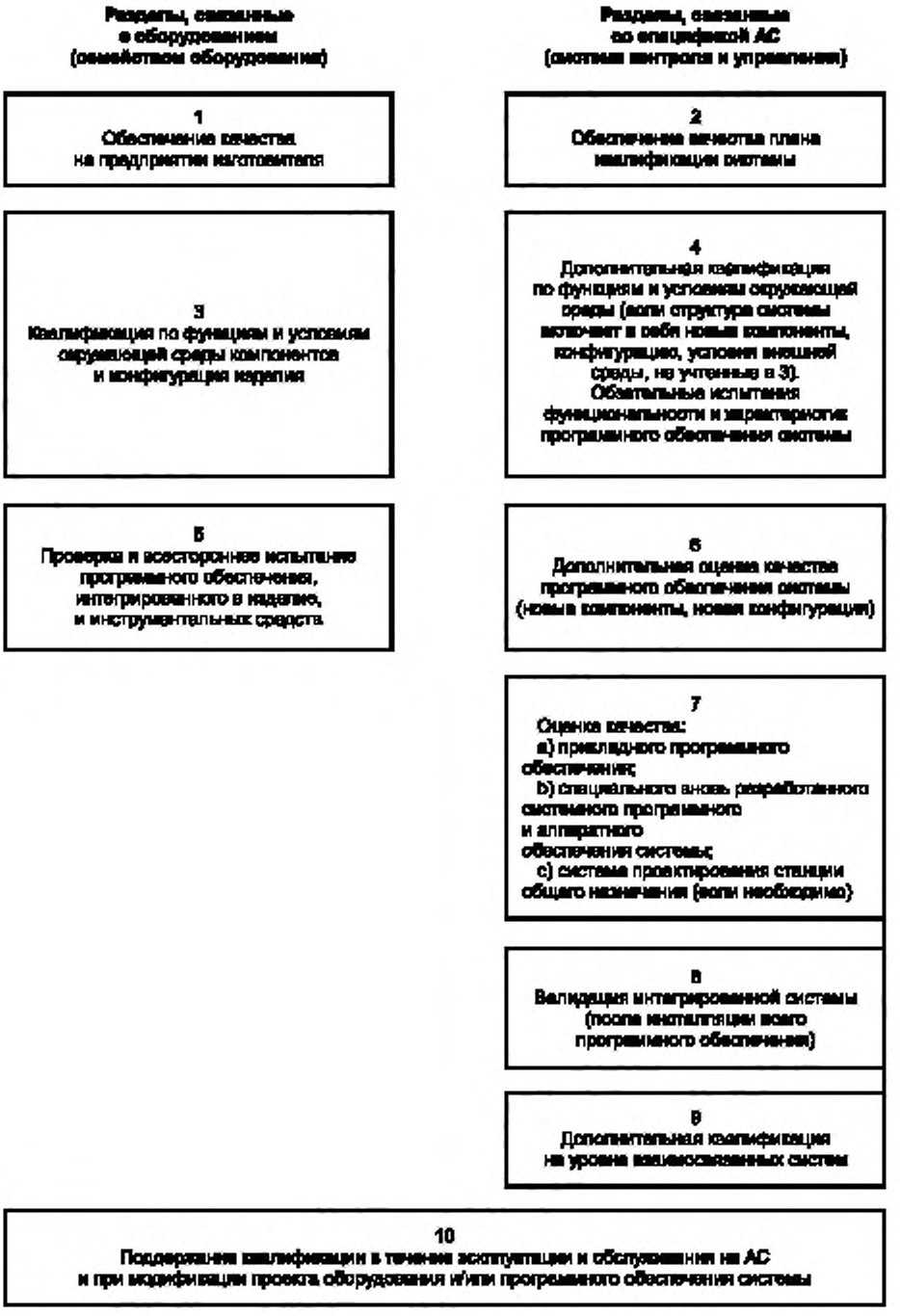


Рисунок 6 — Разделы плана квалификации системы

6.5 Сводка наиболее важных специальных требований к различным классам и категориям

Таблица 4 — Требования к проектированию и квалификации систем контроля и управления и оборудованию

Класс 1	Класс 2	Класс 3
Типовое оборудование		
Разработанное в соответствии со стандартами МЭК атомной отрасли (см. 6.1.2.1)	Отобранное квалифицированное готовое покупное оборудование	Отобранное готовое покупное оборудование
Требования к характеристикам оборудования/семейства оборудования		
Должно допускаться разделение резервированных узлов с целью обеспечения соответствия критерию единичного отказа (см. 6.1.1.2.1)		
Детерминированное поведение при стационарных условиях (см. 6.1.1.2.2)	Также детерминированное поведение с использованием методологии сортировки (см. 6.1.1.2.2)	
Минимальная зависимость работы системы от загрузки АС (см. 5.3.1.5.3)		
Устройства самопроверки: МЭК 60880 и МЭК 60987 (см. 6.1.2.3)		
Способность к тестированию (см. 6.1.1.2.4; 6.1.3.1.2)		
Способность обеспечить независимость: МЭК 60709 (см. 6.1.2.2.2)		
Квалификационные требования (см. 6.4)		
Оборудование: МЭК 60780. Программное обеспечение: МЭК 60880 и МЭК 60880-2	Оборудование: МЭК 60780. Программное обеспечение	

Таблица 5 — Требования к спецификации и реализации ФСО

Категория А	Категория В	Категория С
Независимые подсистемы для резервированных функций (см. 6.1.2.4). Критерий единичного отказа при эксплуатации и обслуживании (см. 6.1.2.4)		
Независимость от резервных ручных средств управления (см. 5.3.1.5)		
Функциональная валидация (см. 6.1.3.1.1)		
Анализ надежности (см. 6.1.3.1.2) (в прямой зависимости от категории)	Анализ надежности (см. 6.1.3.1.1) (в прямой зависимости от категории)	Анализ надежности (см. 6.1.3.1.1) (в прямой зависимости от категории)
Валидация по МЭК 60880 (см. 6.2.4)	Валидация по МЭК 60880 (см. 6.2.4) с возможными изъятиями	Валидация по МЭК 60880 с возможными изъятиями (см. 6.2.4)

Окончание таблицы 5

Категория А	Категория В	Категория С
Верификация каждого канала безопасности в условиях АС (см. 6.2.5)		
Корректировка проекта по МЭК 60880 и МЭК 60987 (см. 6.1.7)		
Планирование системы		
План верификации независимой группой экспертов (см. 6.2.1.1). План валидации независимой группой экспертов (см. 6.2.4)	План валидации с привлечением независимых экспертов (см. 6.2.4)	План валидации с привлечением независимых экспертов (см. 6.2.4)
Документирование и верификация		
Необходим охват интеграционных испытаний (см. 6.3.4.3)	Рекомендуется охват интеграционных испытаний (см. 6.3.4.3)	

7 Общая интеграция и приемка

Цель этой фазы — провести интеграцию систем контроля и управления непосредственно на АС и убедиться, что в течение приемочных испытаний на АС все функции контроля и управления, важные для безопасности, выполнялись, как ожидалось. План приемки систем контроля и управления включают в программу приемки систем АС (см. 4.4 МАГАТЭ 75-INSAG-3).

7.1 Требования, необходимые для достижения результата

a) Необходимы систематичные действия в соответствии с разработанными планами внедрения системы, общей интеграции и приемки и обеспечения защищенности, определенными в 5.4. и 6.2.

b) Деятельность по общей интеграции должна охватывать все установленные и отдельно испытанные системы, имеющие отношение к контролю и управлению (см. 6.1.6).

c) Базы данных должны быть загружены и величины, подлежащие хранению, проверены.

d) Оборудование и программное обеспечение компьютерных систем должны находиться под управлением конфигурацией.

e) Для новых АС верификация и валидация всех функций, важных для безопасности, должны быть выполнены до загрузки топлива в реактор.

7.2 Выходная документация

a) Выходная документация на интеграцию системы контроля и управления с отчетами о хронологии верификации и валидации должна быть представлена до начала эксплуатации.

b) Отчет о приемке должен подтвердить, что система соответствует всем требованиям по ее использованию, а функции, важные для безопасности, соответствуют всем заранее установленным требованиям (см. 5.2).

c) Обнаруженные отклонения от проекта должны быть оценены, скорректированы и доведены до эксплуатирующей организации, чтобы любое влияние на работу АС не было оставлено без внимания (см. 4.4.2 МАГАТЭ 75-INSAG-3).

Примечание — Точные требования к документации будут зависеть от конкретной эксплуатирующей организации.

8 Общая эксплуатация и обслуживание

Системы контроля и управления могут быть приняты в эксплуатацию, если рассмотрение отчетов о приемке покажет, что вся работа выполнена удовлетворительно. Эксплуатация может продолжаться до тех пор, пока из записей, выполняемых при обслуживании, не станет ясно, что системы нуждаются в ремонте или модификации. Эксплуатация может быть продолжена в результате успешного завершения ремонта или модификации после рассмотрения и оценки соответствующих отчетов.

Условия начала эксплуатации должны быть оговорены до передачи систем после общей приемки эксплуатирующей организации. Независимо от этого соглашения должны быть удовлетворены следующие требования:

- должны быть завершены достаточные испытания систем, подтверждающие, что системы функционируют в соответствии со спецификацией. Если при испытаниях выявляются дефекты, то их следует описать в документации и, если возможно, исправить перед передачей системы в эксплуатацию;
- должны быть подготовлены документация пользователя и регламент обслуживания.

8.1 Требования, необходимые для достижения результата

Эксплуатация и обслуживание систем контроля и управления АС направлены на удовлетворение требований к функциям контроля и управления, важным для безопасности.

a) Должны быть введены регламенты эксплуатации, обслуживания и обеспечения защищенности, упомянутые в 5.4 и 6.2.

b) Инструкции, которым должны следовать оперативный и обслуживающий персонал, должны находиться в помещении блочного щита управления или в ближайшем помещении. Их форма и содержание должны соответствовать международным или национальным правилам.

c) В соответствии с МЭК 60880 для систем класса 1 должны быть введены инструкции по эксплуатации и обслуживанию программного обеспечения.

8.2 Выходная документация

При эксплуатации, ремонте и обслуживании должна вестись документация (в хронологическом порядке). Для выявления необходимости проведения обслуживания и модернизации в процессе эксплуатации с определенной периодичностью должны выполняться записи и составляться отчеты, содержащие соответствующие оценки.

Примечание — Подробные требования к выходной документации устанавливаются конкретной эксплуатирующей организацией.

Приложение А
(справочное)

Основные вопросы безопасности АС

В настоящем приложении представлены основные положения концепции безопасности, которые применены в настоящем стандарте к проекту систем контроля и управления на АС.

А.1 Цели безопасности АС

Любая промышленная деятельность, которая влечет за собой риски для рабочих, населения и окружающей среды, требует от оператора принятия всех мер, необходимых для того, чтобы эти риски находились на разумно достижимом низком уровне. Одним из характерных рисков ядерной энергетики является потенциальная опасность ионизирующего излучения (см. раздел 201 МАГАТЭ 50-C-D).

Основная цель радиационной безопасности — защитить людей, общество и окружающую среду посредством установления и поддержания эффективной защиты от радиационного воздействия АС (см. 2.1 75-INSAG-3 и раздел 2 МАГАТЭ 50-C-D).

Безопасность современных АС определяется вероятностью тяжелого повреждения активной зоны менее 10^{-4} событий в год. Применение всех принципов безопасности для будущих АС должно привести к достижению уровня этой вероятности не более 10^{-5} событий в год. Строгое применение мер по управлению в аварийных условиях и мер по ликвидации последствий должно привести к уменьшению вероятности повышенного выброса с АС, требующего контроля за ее пределами, по крайней мере, в 10 раз (см. 2.3 МАГАТЭ 75-INSAG-3).

А.2 Анализ безопасности АС

Анализ безопасности в проекте АС выполняют, чтобы установить и подтвердить основы проектирования узлов, важных для безопасности, и гарантировать, чтобы проект АС в целом был способен обеспечить соблюдение пределов и контрольных уровней доз облучения, а также выбросов и сбросов, установленных регулирующим органом, при всех режимах работы АС (см. 2.3 МАГАТЭ 75-INSAG-3).

Анализ безопасности может включать в себя:

- подтверждение того, что пределы эксплуатации и условия соответствуют требованиям нормальной эксплуатации АС;
- описание постулированных исходных событий, характерных для проекта АС, и места их возникновения;
- анализ и оценку последовательностей событий, возникающих вследствие исходного постулированного события;
- сравнение результатов анализов с принятыми радиационными критериями и проектными пределами;
- установление и подтверждение основ проектирования;
- подтверждение того, что возможно управление при отклонениях от нормальной эксплуатации и авариях с помощью средств автоматических систем безопасности в комбинации с предписанными действиями оператора.

Такой анализ безопасности проводится в виде итеративного процесса, начиная с концептуальных основ проекта вплоть до окончательной оценки безопасности АС, и должен учитывать все детали структуры АС, которые могут отразиться на безопасности. При анализе безопасности рассматриваются вероятные ошибки персонала в процессе эксплуатации и условиях аварии.

Анализ должен показать, что действия, выполнение которых обеспечивается системами управления и операторами, влияют на состояние АС, поддерживая дозы облучения персонала и населения ниже установленных пределов как при нормальной эксплуатации и отклонениях от нормальной эксплуатации, так и в аварийных условиях.

А.2.1 Анализ последующих событий

Целью анализа является последовательное детальное выявление возможных последствий постулированного исходного события, включая те из них, которые возникают из-за отказов вспомогательных и обеспечивающих систем и из-за ошибки оператора. Результаты такого анализа последующих событий могут затем использоваться для определения соответствия требованиям безопасности АС, правилам проектирования, установленным МАГАТЭ (см. приложение к МАГАТЭ 50-C-D).

При анализе для определения возможных состояний АС после постулированного исходного события полезными инструментами являются анализ дерева событий (качественный анализ) и дерева отказов (количественный анализ).

Отмечается, что невозможно и нет необходимости включать в анализ безопасности каждое последующее событие, которое может произойти. Однако в анализе безопасности следует выявить и рассмотреть в деталях те постулированные исходные события и их последствия, которые соответствуют граничным случаям проекта безопасности.

Даже ограничиваясь рассмотрением последствий событий, приводящих к граничным состояниям, указанным выше, использование методологии дерева событий во многих практических случаях приводит для каждого постулированного исходного события к выявлению большого числа состояний АС, которые действительно могут

быть рассмотрены детально. Поэтому допустимо ограничиваться при детальном анализе рядом типичных последствий события.

А.2.2 Оценка основ проектирования: детерминистический или вероятностный методы

Для оценки степени достижения целей безопасности разработаны соответствующие методики (см. 3.3.4 МАГАТЭ 75-INSAG-3).

При использовании детерминистического подхода проектные события выбирают так, чтобы ограничить круг связанных вероятных исходных событий, которые могли бы повлиять на безопасность АС.

Вероятностный метод используют для оценки вероятности любого отдельного случая и его последствий. При проведении оценки допустимо принимать в расчет меры по смягчению последствий как на самой АС, так и за ее пределами.

Сравнение детерминистического и вероятностного методов:

отсутствие достаточных данных о поведении компонентов или систем контроля и управления или невозможность определить подходящую модель могут препятствовать строгой количественной вероятностной оценке. Однако частичный вероятностный метод может дополняться качественным инженерным рассмотрением. С другой стороны, детерминистический метод требует такого инженерного рассмотрения, которое, безусловно, содержит некоторые качественные вероятностные оценки.

В сущности, текущая практика состоит в использовании детерминистического метода при проектировании систем контроля и управления и вероятностного — для оптимизации отдельных частей проекта и оценки общей безопасности АС.

А.3 Глубокоэшелонированная защита

Основой философии безопасности является концепция глубокоэшелонированной защиты. Эта концепция должна применяться ко всем аспектам деятельности, связанной с безопасностью, для гарантии обеспечения частичного перекрытия мер безопасности, чтобы в случае, когда отказ произошел, он компенсировался или исправлялся дополнительными мерами (см. раздел 2 МАГАТЭ 50-C-D; 3.2 и приложение к МАГАТЭ 75-INSAG-3; 3.3 МАГАТЭ 50-SG-D8 и МАГАТЭ 50-SG-D11).

Первое применение концепции глубокоэшелонированной защиты заключается в создании в процессе проектирования набора независимых, но дополняющих друг друга устройств и процессов для предотвращения аварии или обеспечения соответствующей защиты в случае, если отказ все-таки имел место. Примеры многоуровневой защиты:

- создание многократно резервированных средств, обеспечивающих выполнение каждой основной функции безопасности, т.е. управление реактивностью, отвод тепла и удержание радиоактивности;
- использование надежных защитных устройств в дополнение к внутренним свойствам безопасности;
- организация управления АС с помощью автоматики и действий оператора;
- создание оборудования и процессов, обеспечивающих уменьшение последствий аварии.

В общем, все линии защиты должны применяться в течение всего времени действия различных эксплуатационных режимов:

Цель первой линии защиты — предотвратить отклонение эксплуатации АС от нормальной. Для этого необходимо, чтобы станция была надежно, с определенной степенью консервативности спроектирована, построена и эксплуатировалась при соответствующем уровне качества и инженерного опыта.

Цель второй линии защиты — выявить и предупредить отклонения от условий нормальной эксплуатации, чтобы предотвратить переход предусмотренных проектом эксплуатационных событий в аварийную ситуацию.

Для третьей линии защиты предполагается, что (хотя это крайне нежелательно) развитие предусмотренных событий не могло быть предотвращено предыдущими линиями защиты, и поэтому для управления последствиями возникающих аварийных условий предусматривается дополнительное оборудование и процессы.

После третьей линии защиты дополнительная защита населения обеспечивается за счет неосновных вспомогательных свойств АС (которые не представляются важными для безопасности) и планов аварийной готовности, которые, по большей части, не зависят от типа реакторной установки.

Второе применение концепции глубокоэшелонированной защиты состоит в сооружении и эксплуатации АС так, чтобы радиоактивные материалы удерживались рядом физических барьеров. Эти физические барьеры являются пассивными и чаще всего включают в себя топливо, оболочку топливного элемента, границу контура охлаждения реактора и контейнмент. Проект должен обеспечить необходимую эффективность и защитные свойства каждого из указанных выше физических барьеров.

Еще одно применение концепции глубокоэшелонированной защиты заключается в осуществлении однократного или многократного резервирования систем контроля и управления. Для того, чтобы уменьшить масштаб нарушения и достичь глубокоэшелонированной защиты, допускается использование более одной системы контроля и управления, которые срабатывают по мере того, как контролируемая переменная отклоняется от нормального значения. В первую очередь, если переменная отклоняется от значений, соответствующих нормальным условиям, отрабатывают неклассифицированные системы. После действий этих систем управления может включаться один или несколько уровней дополнительных систем управления, важных для безопасности, прежде чем будут задействованы защитные системы, в случае если событие превращается из незначительного отклонения от нормальной эксплуатации в постепенно нарастающий переходный процесс. Целью каждой линии защиты является приостановление развития события и возврат системы к нормальной эксплуатации при небольших отклонениях и безопасный останов при событиях, которые могут превратиться в более серьезные.

Приложение В
(справочное)

Категоризация функций и классификация систем

В.1 Обоснование схемы категоризации/классификации

МАГАТЭ 50-SG-D1 устанавливает перечень функций безопасности, учет которых при проектировании АС позволяет соответствовать основным требованиям безопасности: от способов безопасного останова реактора до отвода остаточного тепла от активной зоны и снижения вероятности выброса радиоактивных веществ. Данный документ устанавливает принцип классификации компонентов содержащего жидкости оборудования, необходимых для выполнения функций безопасности, в соответствии с их важностью для безопасности. Данный документ вводит методологию классификации функций безопасности и задания требований к проекту, основанную на учете последствий отказа функции безопасности, вероятности того, что может потребоваться выполнение функции, и вероятности того, что функция может при необходимости не выполняться.

МАГАТЭ 50-SG-D8 распространяет принцип классификации на системы контроля и управления. Данный документ подразделяет системы контроля и управления на «системы, важные для безопасности», и «системы, не влияющие на безопасность». Далее «системы, важные для безопасности» подразделяют на «системы безопасности» и «системы, относящиеся к безопасности» (см. рисунок 1 и «определения» в МАГАТЭ 50-SG-D8). МАГАТЭ 50-SG-D3 и МАГАТЭ 50-SG-D8 определяют требования к проектированию систем защиты и систем, относящихся к безопасности соответственно. МЭК 60880 и МЭК 60987 опираются на эту классификацию МАГАТЭ.

МЭК 61226 подразделяет функции и соответствующие системы и оборудование, важные для безопасности, на три категории: А, В и С. Данный документ устанавливает критерии отнесения функций контроля и управления к конкретным категориям и требованиям к проектированию соответствующих систем и оборудования (см. раздел 8 МЭК 61226).

Число классов, установленных МАГАТЭ, отличается от установленных в МЭК 61226 (системы защиты и системы, относящиеся к безопасности, в отличии от категорий А, В и С). Более того, МАГАТЭ и МЭК не всегда используют одни те же определения и концепции (система классификации МАГАТЭ и классификация ФСО в МЭК), и эти расхождения могут быть источником различных интерпретаций.

Настоящий стандарт следует требованиям МЭК 61226 в отношении деления на три класса, данный подход типичен для различных уровней обеспечения требуемого исполнения и надежности при использовании существующих в настоящее время технических средств контроля и управления и изделий (например, разработанные в соответствии со стандартами атомной отрасли, отобранные и классифицированные покупные изделия, отобранные покупные изделия). Однако во избежание неоднозначной трактовки требований стандарта выработана специальная схема градации функций и соответствующих систем и оборудования.

Ниже изложены основные требования настоящего стандарта к категоризации и классификации.

В.2 Обоснование принципов категоризации и классификации, принятых в настоящем стандарте

Функции, системы и оборудование АС можно рассматривать с двух точек зрения (см. рисунок В.1):

- функциональная точка зрения.

В этом случае рассматриваются только выполняемые системами и оборудованием функции. Несмотря на то, что известно, что для выполнения функции безопасности необходимы датчики, устройства обработки, обмена информацией и пр., функциональный подход не учитывает, что эти устройства могут входить в состав более крупной сборки оборудования, которая выполняет также и другие функции (см. «системная точка зрения»). Технические средства для выполнения функции называются системами и оборудованием, связанным с данной функцией:

системная точка зрения.

В этом случае системы АС рассматриваются как организованный набор аппаратуры, который выполняет множество функций/подфункций, например, система защиты, система автоматизации и управления, система взаимодействия человек — машина. Отдельные функции, выполняемые системой, могут относиться к различным категориям.

В.2.1 Фаза проектирования АС

Разработчики технологии АС анализируют станцию и соответствующие системы с функциональной точки зрения. Определяются постулированные исходные события, которые могут происходить на реакторной установке и АС, и функции, важные для безопасности, необходимые для обеспечения управления этими исходными событиями с целью предотвращения их развития в аварийные ситуации. Для управления каждым постулированным исходным событием в соответствии с принципом глубокоэшелонированной защиты может потребоваться несколько независимых функций (или подфункций). Функции (или подфункции) относят к категориям А, В или С в зависимости от того, какую роль они играют в обеспечении безопасности АС — принципиально важную, дополнительную, вспомогательную или непосредственную.

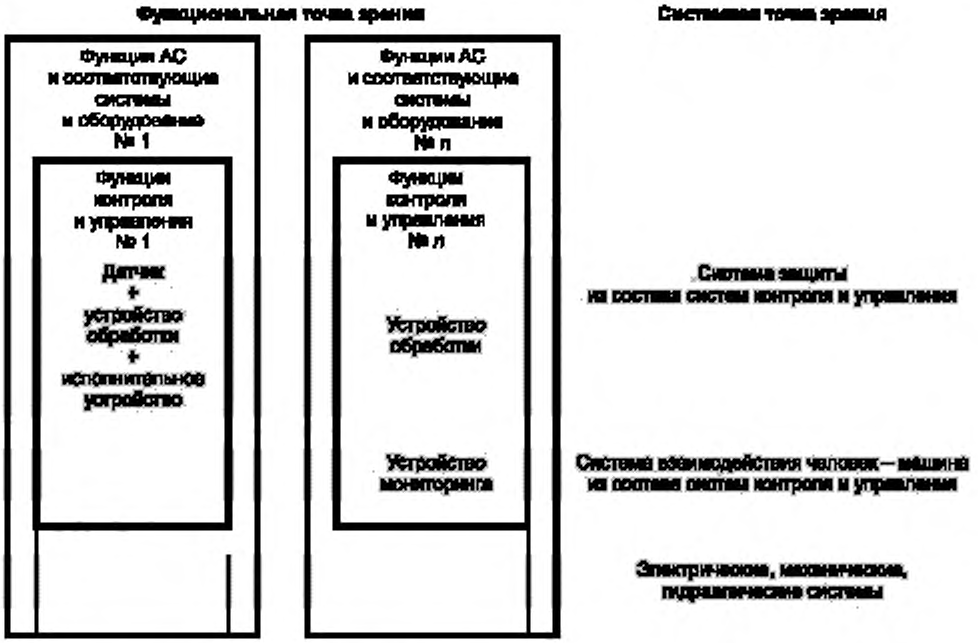


Рисунок В.1 — Отношения между функциями и системами контроля и управления АС

Способы категоризации обычно основываются на детерминистическом, вероятностном рассмотрении и рассмотрении с позиции снижения риска. Они принимают во внимание различные факторы, такие как вероятность и возможная тяжесть последствий постулированного исходного события при сбоях в системе контроля и управления, времени, в течение которого инициируется требуемое однократное выполнение функции, временные границы и надежность, с которыми могут быть выполнены альтернативные действия или исправлен любой отказ в системе контроля и управления.

Процесс присвоения категории допускает, чтобы функции контроля и управления комплекса безопасности были распределены по различным категориям, например, может потребоваться другая реакторная уставка для функционирования только при маловероятных условиях предусмотренного переходного процесса, сопровождающегося отказом основной защитной функции. В этом случае функции контроля и управления должна быть присвоена скорее не категория А (предполагающая размещение в системе класса 1), а категория В или С.

Категории определяют уровень требований к проекту, а также минимальный требуемый класс соответствующей системы и оборудования, необходимых для выполнения функции.

Функции системы безопасности АС



В.2.2 Фаза проектирования контроля и управления

При проектировании контроля и управления АС анализируют функции контроля и управления и соответствующие системы и оборудование, используя системный подход. Задача состоит в определении ряда систем контроля и управления для осуществления функций контроля и управления с уровнем качества и независимости, требуемым для разработчиков технологического процесса. Системы, распределяются по классам в зависимости от достижимого уровня качества.



Процесс классификации и назначения функций для компьютерной системы отличается от подхода, используемого для технологии, основанной на жесткой логике, поскольку:

- при жесткой логике функции обычно вводятся однажды в ряд отдельных электронных компонентов или реле, а компьютерные системы с использованием одних и тех же компонентов оборудования позволяют выполнять несколько функций;
- компьютерная система включает в себя ряд вспомогательных функций, например, функции самоконтроля и диагностики, которым не присваивается категория при проектировании АС;
- выбор архитектуры системы может быть ограничен с точки зрения сложности для упрощения выполнения функций высшей категории безопасности;
- для проектанта имеется возможность формировать требования к архитектуре системы, например, разделение по функциям, внутренний режим работы, сложность, защита от отказов по общей причине, которые связаны не с отдельными функциями, а с системами контроля и управления и характеристиками применяемого оборудования и классификацией этих систем.

Процесс классификации и назначения функций приводит к осознанию необходимости устанавливать классификацию систем контроля и управления по функции, обладающей высшей категорией из выполняемых системой функций.

В.3 Присвоение категорий функциям контроля и управления, важным для безопасности

В настоящем стандарте предполагается, что проект безопасности АС, разрабатываемый технологами, распределяет отдельные функции контроля и управления, важные для безопасности, по трем категориям А, В, С. Требования к категориям, по сути, определяют качество оборудования, применяемого для выполнения конкретных функций.

Процесс присвоения категорий функциям контроля и управления заканчивается на уровне подфункций (см. примечание), так что для инженеров, занимающихся контролем и управлением, дополнительный анализ проводить не требуется.

Примечание — Одна и та же функция, важная для безопасности, может выполняться с использованием ряда подфункций или единственной функцией, включающей в себя все подфункции. Это может привести к неопределенности при разработке требований к категориям, поскольку подфункции могут иметь разное отношение к безопасности и, как следствие, различные категории.

В дополнение к требованиям по категоризации функций проект безопасности АС определяет требования к независимости и разнообразию отдельных функций для обеспечения глубокоэшелонированной защиты. Необходима независимость функций, поддерживающих различные линии защиты в одном и том же комплексе безопасности, функций снижения риска.

Требования к независимости и разнообразию являются исходными при назначении функций систем контроля и управления. «Системы и оборудование», связанные с функцией, могут быть распределены по различным системам контроля и управлениям так, чтобы они имели одну и ту же классификацию безопасности (см. В.2).

В.4 Классификация систем контроля и управления

Системы контроля и управления образуют полную архитектуру контроля и управления, обычно объединяя ряд функций или подфункций, которые выполняют схожие задачи. Системы можно характеризовать функциями, которые они выполняют. Некоторые системы контроля и управления и их функционирование зависят от типа АС. Характерные примеры систем контроля и управления, важных для безопасности, приведены ниже.

а) Системы автоматического и ручного управления

Системы контролируют параметры энергоблока или оборудования для:

- поддержания технологического процесса в пределах, принятых в результате анализа безопасности АС;
- поддержания безопасной эксплуатации систем АС и оборудования, важного для безопасности;
- снижения до минимума размеров и скорости возможных нарушений;
- снижения до минимума частоты возникновения событий, которые требуют срабатывания систем защиты, что может достигаться за счет обеспечения высокого качества, избыточного резервирования систем автоматического и ручного управления или обеспечения более чем одного уровня действия. Например, комбинацией автоматического и ручного управления (если имеется достаточное время для правильной реакции) или комбинацией двух и более из указанных выше мер.

Системы автоматического и ручного управления могут влиять на безопасность, так как их функционирование, надежность, а также последствия отказа составляют часть исходных данных для проектирования системы защиты (см. 3.3 МАГАТЭ 50-SG-D3). Такие системы могут быть также основным средством выполнения функций, важных для безопасности, например, если есть достаточно длительный период времени для осуществления корректирующих действий.

Типичная работа этих систем состоит в регулировании процессов по открытой петле, замкнутой петле, а также в управлении вручную.

b) Системы человеко-машинного интерфейса.

Системы представляют информацию оператору и другим о состоянии энергоблока и его систем, важных для безопасности. Они также используются для поддержки принятия решения оператором и выполнения вручную действий по поддержанию безопасности энергоблока.

Типичная работа таких систем заключается в:

- преобразовании информации от датчиков или сигналов других систем в информацию, пригодную для представления на дисплее или с помощью индикаторов, электронно-лучевых трубок, принтеров и т.д. Система предоставляет такую информацию, как обзор, обработку аварийной сигнализации, а также руководство по эксплуатации;
- отображении аварийных и предупредительных сигналов и другой информации;
- обеспечении интерфейса с системами ручного управления.

c) Системы защиты и обеспечения безопасности.

Эти системы способствуют тому, что определенные проектом для предусмотренных эксплуатационных событий пределы не превышаются и последствия аварий находятся в рассмотренных проектом пределах.

Свод правил МАГАТЭ по безопасности (см. МАГАТЭ 50-SG-D3) определяет типовую функциональность этих систем:

- определение аварийных условий и автоматическое включение соответствующих систем, в том числе останов реактора;
- обеспечение приоритетности выполнения функций различных категорий (например, прерывание работы системы управления).

d) Система аварийного энергоснабжения.

Типовая функциональность:

- снижение нагрузки;
- упорядочение нагрузки дизель-генераторов и других источников энергоснабжения.

Системы контроля и управления, выполняющие функции, важные для безопасности, относятся к одному из трех классов, соответствующих определенным требованиям к проекту, изготовлению и качеству, которые позволяют этим системам выполнять функции, относящиеся к одной или более категорий: A, B или C, или неклассифицированные функции (см. B.2). Пример типовой классификации систем контроля и управления приведен в таблице B.1.

Таблица B.1 — Типовая классификация систем контроля и управления

	Класс 1	Класс 2	Класс 3	Неклассифицированные
Системы автоматического и ручного управления АС		X	X	X
Системы человеко-машинного интерфейса		X	X	X
Системы защиты и обеспечения безопасности	X			
Система аварийного энергоснабжения	X			

Требования к функции самой высокой категории безопасности определяют класс системы.

Приложение С
(справочное)

Качественное рассмотрение защиты от отказов по общей причине

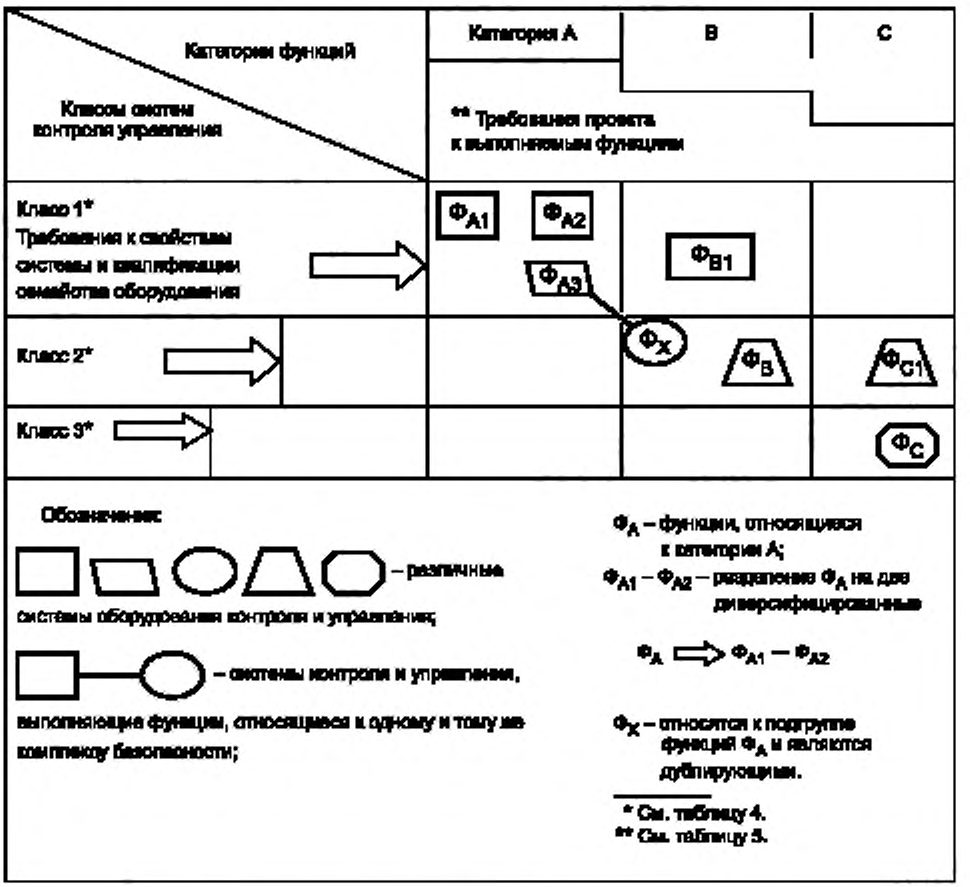


Рисунок С.1 — Примеры распределения функций систем контроля и управления комплекса безопасности

С.1 Пример распределения функций комплекса безопасности между системами

Рисунок С.1 приведен в соответствии с таблицами 4 и 5 подраздела 6.5 и показывает связь с соответствующими разделами настоящего стандарта. Таблица 4 отражает требования к характеристикам и квалификации комплекса оборудования, предназначенного для построения систем контроля и управления различных классов. Таблица 5 содержит требования к системам контроля и управления, которые предназначены для выполнения функций, классифицированных по категориям в соответствии с настоящим стандартом. Требования к характеристикам оборудования, такие, например, как требования по устойчивости к воздействию окружающей среды, надежности программного обеспечения, могут быть удовлетворены за счет выбора подходящего семейства технических средств. Требования к системам в первую очередь относятся к таким проектным характеристикам, как, например, устойчивость архитектуры системы к отказам и адекватность проектных методов верификации и валидации, принятым для подтверждения правильности функционирования.

Примеры распределения функций комплекса безопасности по системам контроля и управления, отражающие различные проектные подходы, соответствующие требованиям к надежности, представлены на рисунке С.1. Выбранные подходы основаны на анализе эффективности различных мер обеспечения устойчивости к отказам по общей причине (см. 5.3.3.1).

$Ф_{A1}$ - - - $Ф_{A2}$: комплекс безопасности должен выполнять две разные функции категории А — $Ф_{A1}$ и $Ф_{A2}$.

Проведение анализа на устойчивость к отказам по общей причине необходимо для того, чтобы показать, что в данном случае использование функционального разнообразия (см. 5.3.1.5.5, перечисление b) способствует эффективной защите от отказов по общей причине. Затем обе функции вводятся в независимые системы класса 1, выполненные на том же самом типе оборудовании.

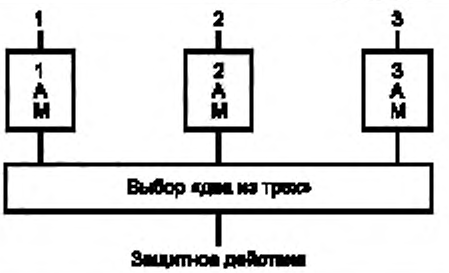
$Ф_A$ - - - $Ф_X$: комплекс безопасности должен выполнять основную функцию $Ф_A$ категории А и дополнительную функцию категории В или С, $Ф_X$ как средство дублирования. Анализ устойчивости к отказам по общей причине должен в этом случае показать, что применение разнообразия технических средств (см. 5.3.1.5.5) обеспечивает достаточную защиту от отказа системы по общей причине. Функция $Ф_A$ назначается одной системе класса 1, а функция $Ф_X$ передается системе класса 2, выполненной на другом семействе технических средств с тем, чтобы обеспечить разнообразие аппаратуры.

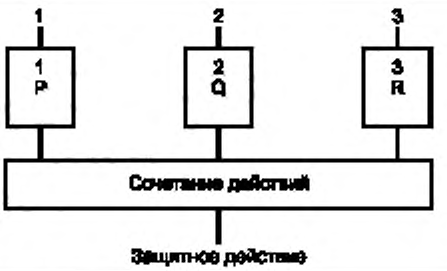
$Ф_{B1}$ - - - $Ф_B$: комплекс безопасности должен выполнять две разные функции категории В — $Ф_{B1}$ и $Ф_B$. Анализ устойчивости к отказу по общей причине должен показать, что применение разнообразия оборудования и функционального разнообразия обеспечивает достаточную защиту от отказа по общей причине. Функцию $Ф_{B1}$ назначают одной системе класса 1, а функцию $Ф_B$ размещают в системе класса 2, выполненной на других технических средствах для того, чтобы обеспечить дублирование по аппаратуре.

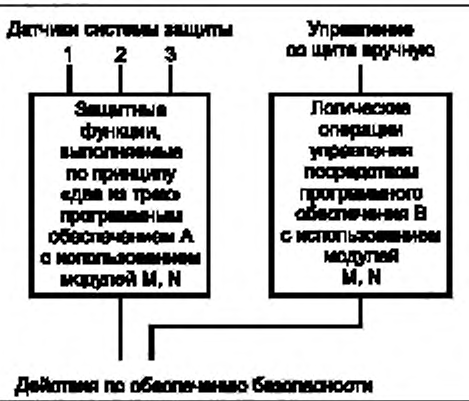
Случай с функциями $Ф_C$ и $Ф_{C1}$ аналогичен предыдущему случаю.

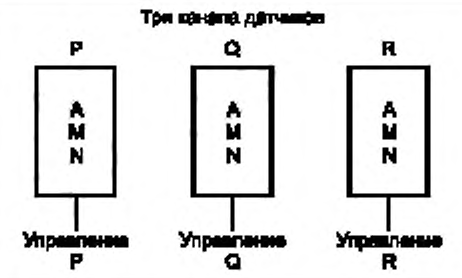
С.2 Примеры чувствительности к отказам по общей причине в комплексе безопасности

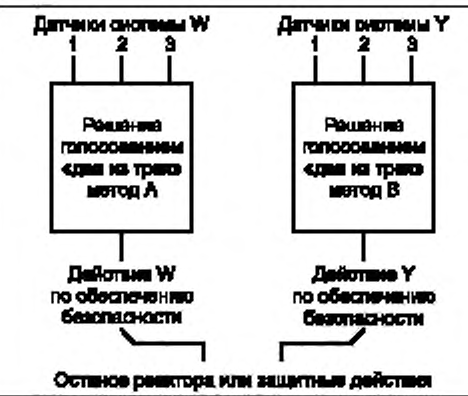
Могут возникнуть следующие типичные ситуации.

Пример 1 Комплекс безопасности, содержащий систему с тремя идентичными резервированными каналами, выполняющими единственную защитную функцию А	
Возможный случай отказа по общей причине Вероятность: (Н) = высокая; (М) = средняя; (L) = низкая	**Возможная защита** Эффективность: (Н) = высокая; (М) = средняя; (L) = низкая
Ошибка при спецификации требований к прикладной функции А (Н)	Независимая верификация спецификации (М)
Дефект в спецификации или при разработке прикладного программного обеспечения или дефект в модуле системного программного обеспечения (М). Отказ может возникнуть как следствие прохождения одинаковых сигналов по трем каналам [(L) — для систем класса А)]	Разработка системы, соответствующей классу 1 (Н)
Одновременный отказ технических средств трех каналов вследствие опасного воздействия	Физическая и электрическая независимость (Н)
Отказ при голосовании двух из трех (или при других действиях каналов)	Разработка системы класса 1 (Н). Применение надежных проверенных на практике решений (стандартный модуль) (Н)

Пример 2 Группа безопасности, содержащая систему с резервированными каналами, выполняющими одиночную функцию защиты А и отвечающими общим требованиям, но использующим разное программное обеспечение для обработки информации (устройства обработки P, Q, R)	
Возможный случай отказа по общей причине Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка при спецификации требований к прикладной функции А (H)	То же, что в примере 1
Дефект в спецификации или при разработке прикладного обеспечения или дефект в модуле системного программного обеспечения (M). Отказ может произойти вследствие особенности прохождения одинаковых сигналов в каждом из трех каналов (L)	Разработка системы класса 1 (H). Меры противодействия: резервирование программного обеспечения
Одновременный отказ оборудования трех каналов вследствие опасного воздействия	То же, что в примере 1
Отказ при голосовании двух из трех каналов (или при других действиях каналов)	То же, что в примере 1

Пример 3 Комплекс безопасности, содержащий систему с двумя каналами, выполняющими независимо одну и ту же защитную операцию* ——— * Предполагается, что оператор имеет достаточное время и информацию для реагирования	
Возможный случай отказа по общей причине Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Дефект в спецификации или при разработке прикладных программ или дефект в общесистемных программных модулях M, N [(L) при асинхронной работе]	Разработка системы класса 1 (H)
Ошибка при спецификации требования к обеим функциям (L)	Защита обеспечивается функциональным разнообразием (автоматически; вручную) (H)
Одновременный отказ оборудования каналов системы вследствие опасного воздействия	То же, что в примере 1
Ошибка при голосовании «два из трех» (или при других действиях каналов)	Ручное управляющее действие по направлению основного трафика голосования (H)

Пример 4 Комплекс безопасности, содержащий распределенные дублированные функции P, Q, R, использующие различные датчики и исполнительные устройства и одинаковое оборудование в каждом канале управления	
Возможный случай отказа по общей причине Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка в спецификации требований к трем функциям	Защита обеспечивается функциональным разнообразием (P, Q, R) (H)
Дефект при определении требований или при разработке прикладного программного обеспечения или дефект в общесистемных программных модулях M, N [(L) при асинхронной работе]. Различные траектории сигнала	Полностью независимое оборудование Система класса 1 (H)
Одновременный отказ оборудования каналов системы вследствие опасного воздействия	То же, что в примере 1
Отказ в двух из трех каналов (или другие события в каналах)	Ручное управляющее действие по направлению основного трафика голосования (H)

Пример 5 Комплекс безопасности, содержащий дублированные защитные функции W и Y, распределенные в двух различных системах (разнообразие оборудования и системного программного обеспечения при возможном сходстве, например, алгоритмов, синхронизации операций, документации и общим персоналом)	
Возможный случай отказа по общей причине Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка при спецификации требований к обеим функциям (L)	Защита обеспечивается за счет функционального разнообразия (W и Y) (H)
Дефект спецификации требований или при разработке прикладных программ или дефект в общесистемных программных модулях M, N [(L) при асинхронной работе]. Различные траектории сигнала (L). Вероятность некоторого подобия траекторий сигнала	Полностью независимое оборудование. Разработка системы класса 1
Ошибка в обоих исполнительных действиях по обеспечению безопасности (L)	Различные (дублированные) системы исполнительных устройств (H)

Приложение D
(справочное)

Связь МЭК 61508 с МЭК 61513 и стандартами атомной отрасли

В настоящем приложении сравниваются положения МЭК 61508 (части 1, 2 и 4) и МЭК 61513.

Части 3, 5, 6 и 7 МЭК 61508 не рассматриваются, т. к. они не входят в область применения настоящего стандарта. Например, область применения части 3 МЭК 61508 относительно программного обеспечения частично охватывается МЭК 60880.

Настоящее приложение состоит из четырех разделов:

- в разделе D.1 рассматриваются основные отличия в областях действия и концептуальных основах двух стандартов;
- в разделе D.2 МЭК 61513 сравнивается с МЭК 61508-1 (основные требования);
- в разделе D.3 МЭК 61513 сравнивается с МЭК 61508-2 (системные вопросы);
- в разделе D.4 МЭК 61513 сравнивается с МЭК 61508-4 (определения).

D.1 Область действия и концептуальные основы

При сопоставлении прежде всего рассматриваются некоторые важные отличия областей применения двух стандартов.

Рассматриваемые в МЭК 61508 системы могут быть любыми — электрическими, электронными или основываться на применении технологии программируемой электроники, и, хотя настоящий стандарт содержит основные требования к архитектуре для всех этих технологий, его основная направленность — компьютерные системы.

МЭК 61508 относится к «системам, связанным с безопасностью», тогда как настоящий стандарт следует положениям МАГАТЭ и распространяется на «системы, важные для безопасности».

a) Границы полного жизненного цикла безопасности.

Полный жизненный цикл по МЭК 61508 включает в себя все системы, предусмотренные проектом безопасности оборудования, находящегося под контролем, включая системы контроля и управления — электрические, электронные, выполненные с применением программируемой электроники или на основе других технологий, а также устройства, снижающие риск внешнего воздействия.

Настоящий стандарт специально не рассматривает ни анализ безопасности АС, ни средства оценки соответствия требованиям к характеристикам и надежности, возникающие при анализе. В проекте безопасности АС, который выполняют в соответствии с определенными принципами МАГАТЭ, в правилах МЭК и требованиях национальных регулирующих органов, используется опыт, накопленный в области атомной техники, который в настоящем стандарте не рассматривается. Проектные основы АС определяют постулированные исходные события, их последствия, концепцию глубокоэшелонированной защиты АС, категории функций, необходимых для обеспечения защиты. Однако настоящий стандарт определяет исходную информацию, требуемую для формирования основ проекта и анализа безопасности, которая передается разработчикам контроля и управления в качестве руководства для последующей работы над проектом систем контроля и управления.

b) Общая валидация/оценка безопасности.

В соответствии с требованиями настоящего стандарта общая верификация и валидация каждой распределенной функции, важной для безопасности, описываются в отчете о полной интеграции и приемке системы.

В области атомной техники оценка соответствия этого отчета требованиям безопасности рассматривается в рамках процедуры лицензирования.

c) Системы контроля и управления и архитектура контроля и управления.

Системы контроля и управления, рассматриваемые в настоящем стандарте, эквивалентны электрическим, электронным системам и системам программируемой электроники по МЭК 61508. В настоящем стандарте архитектура системы (см. раздел 5) определяет набор отдельных систем определенных классов, соответствующих требованиям независимости, которые выполняют функции, важные для безопасности. Для каждой из этих систем разделом 6 настоящего стандарта установлен индивидуальный жизненный цикл безопасности. В МЭК 61508 любое разбиение на несколько систем рассмотрено в части 2.

Это различие во избежание недоразумений следует иметь в виду.

d) Уровень значимости функциональной безопасности и классификация.

МЭК 61508 устанавливает уровень значимости функциональной безопасности, требующийся для компьютерной системы, в соответствии со степенью снижения риска, которую система должна обеспечить. Это достигается установлением жесткой связи между риском, обусловленным некими опасностями, прогнозируемой частотой опасных событий, с защитой, которую должна обеспечить система с целью снижения риска до допустимого уровня.

Атомная отрасль традиционно использовала детерминистический метод определения значимости системы для безопасности и ее влияние на величину риска, связанного с выходом радиоактивных веществ (см. IAEA Safety Guides и МЭК 61226).

Для любой системы, предназначенной для предотвращения или ограничения последствий радиоактивного выброса, в основном, предполагается необходимое обеспечение наибольшей реально достижимой степени защиты. Низкий уровень значимости безопасности может быть приемлемым лишь для вспомогательных систем, которые непосредственно не решают задачи предотвращения или ограничения выбросов. Поэтому не существует эквивалентной схемы для снижения с позиций надежности или риска уровней значимости функциональной безопасности, предложенных в МЭК 61508, для широкого применения в атомной технике. Такой детерминистический подход в атомной отрасли признается, в общем, достаточным и приводит на практике к установлению высоких требований ко всем защитным функциям. Однако атомная отрасль признает также и количественный подход, а методы вероятностного анализа безопасности могут ставить более четкие задачи по обеспечению необходимой надежности компьютерных систем.

Установление уровней значимости функциональной безопасности по МЭК 61508 почти полностью соответствует категоризации в атомной отрасли. Однако имеются существенные различия в процедурных вопросах:

- в МЭК 61508 установление уровней значимости функциональной безопасности основано на анализе возможных опасностей и вероятностной оценке риска;
- в МЭК 61226 установление категорий основано на детерминистическом критерии и инженерном опыте оценки последствий в случае отказа.

D.2 Сопоставление МЭК 61508-1 и МЭК 61513

МЭК 61508-1	МЭК 61513
5 Документация	5.5 Выходная документация
6 Управление функциональной безопасностью	5.4.1 В соответствии с МАГАТЭ 50-С-QA (Редакция 1) вся деятельность на АС регламентируется программой обеспечения качества
7 Требования к полному жизненному циклу функциональной безопасности	5 Структура жизненного цикла безопасности контроля и управления
7.1 Основные положения	
Полный жизненный цикл функциональной безопасности охватывает системы контроля и управления электрической, электронной технологий, технологии программируемой электроники и др. технологий, внешние меры по сокращению риска	Полный жизненный цикл безопасности охватывает функции контроля и управления и связанные с ними системы и оборудование, важные для безопасности, и общую архитектуру систем контроля и управления [см. пункт а) в разделе D.1]
7.2 Концепция	
Описание объектов, находящихся под контролем, требуемых функций управления и физической среды	Рассмотрение основ проекта безопасности АС (5.1): - установление условий окружающей среды (5.1.3); - функции контроля и управления, важные для безопасности; - взаимодействие автоматики и оператора
Определение источников опасности	Внутренние и внешние источники опасности устанавливаются при разработке основ проекта безопасности АС и являются объектами контроля и управления (5.1.3) [см. пункт а) раздела D.1]
7.3 Определение области действия	
Определение границ объекта контроля	Выявление ограничений (требований) со стороны проекта АС или границ области действия контроля и управления
Определение объема анализа источников опасности и риска, а также событий, приводящих к аварии	Постулированные исходные события определяются основами проекта обеспечения безопасности АС и представляют собой исходные данные для разработки контроля и управления
7.4 Анализ источников опасности и риска	
Установление опасности объекта контроля...	Не рассматривается настоящим стандартом, является частью основ проекта АС [см. пункт а) раздела D.1]

Продолжение таблицы D.2

МЭК 61508-1	МЭК 61513
... и системы управления объектом контроля	Детерминированные ограничения контроля и управления, например, критерий единичного отказа для функций категории А, функциональное разделение, накладываются основами проекта АС
Определение последовательности следствий опасных событий	Последовательности постулируемых исходных событий определяются в основах проекта обеспечения безопасности АС и являются исходными для контроля и управления (см. 5.1) [см пункт а) раздела D.1]
Определение риска объекта контроля	Категоризация ФСО (см 5.1.2) является исходной для контроля и управления [см. пункт а) раздела D.1]
7.5 Общие требования безопасности	5.2 Общие требования к ФСО
Необходимо специфицировать функции безопасности. Они включают в себя:	Общие спецификации требований к функциям, важным для безопасности, вытекают из основ проекта АС. Они включают в себя:
Спецификации требований к функциям безопасности	Спецификации требований к функциональности и характеристикам [пункт 1) перечисления а) из 5.2]
Спецификация требований к значимости функциональной безопасности	Категоризация функций контроля и управления и связанного с ними оборудования [пункт 3) перечисления а) из 5.2]. Спецификация требований независимости [пункт 3) перечисления а) из 5.2]
Общая спецификация требований безопасности к системам контроля и управления (с использованием электрической, электронной технологий и технологии программируемой электроники), системам с использованием других технологий, а также к устройствам снижения риска	Альтернативная технология и меры по снижению риска определяются в основах проекта безопасности АС в соответствии с принципами глубокоэшелонированной защиты. Настоящим стандартом не рассматриваются [см. пункт а) раздела D.1]
7.6 Распределение требований безопасности	5.3.1 Проект архитектуры контроля и управления 5.3.2 Назначение функций
Распределение функций безопасности по системам и присвоение уровня значимости безопасности каждой функции. Рассматривается возможность отказа по общей причине (см. 7.6.2.7) и задача обеспечения безопасности ограничивается значимостью для отдельной системы, выполненной с применением электрической, электронной технологий или технологии на основе программируемой электроники (см. 7.6.2.11)	Разделение полного контроля и управления на отдельные системы соответствующего класса. Распределение функций контроля и управления по системам контроля и управления в соответствии с классификацией, глубокоэшелонированной защитой, принимая во внимание возможность отказа по общей причине
Общее планирование	5.4 Общее планирование
6 Управление функциональной безопасностью	5.4.1 Общая программа обеспечения качества
7.8 Общее планирование валидации безопасности	5.4.3 Общие планы интеграции и приемки
	5.4.2 Общий план обеспечения защищенности
7.7 Общее планирование эксплуатации и обслуживания	5.4.4 Общий план эксплуатации
	5.4.5 Общий план обслуживания
7.10 Реализация: системы, выполненные с использованием электрической, электронной технологий или технологии с применением программируемой электроники	6 Жизненный цикл безопасности системы

Окончание таблицы D.2

МЭК 61508-1	МЭК 61513
См. МЭК 61508-2 (системные аспекты)	См. раздел 6 (жизненный цикл безопасности системы)
См. МЭК 61508-3 (требования к программному обеспечению)	Программное обеспечение в настоящем стандарте не рассматривается
7.11 Реализация: другая технология	Не входит в область распространения настоящего стандарта [см. пункт а) раздела D.1]
7.12 Реализация: внешние устройства снижения риска	Не входит в область распространения настоящего стандарта [см. пункт а) раздела D.1]
7.13 Общие внедрение и приемка системы	7 Общие интеграция и приемка системы
7.14 Общая валидация безопасности Валидация того, что системы, выполненные с использованием электрической, электронной технологий или технологии с применением программируемой электроники, соответствуют общим требованиям в соответствии с распределением функций	7.1 Общая приемка Верификация и валидация функций, важных для безопасности, распределенных более чем по одной системе 6.4 Квалификация системы
7.15 Общие эксплуатация, обслуживание и ремонт	6 Общие эксплуатация и обслуживание
7.16 Общие модификация и модернизация	1 Область применения Настоящий стандарт (или его часть) применим к системам контроля и управления на новых атомных станциях, так же как и к реконструируемым и модернизируемым системам на существующих АС
7.17 Снятие с эксплуатации или утилизация	Настоящим стандартом не рассматривается
7.18 Верификация	5.4.1 Общие программы обеспечения качества
7 Оценка функциональной безопасности Получение подтверждения о достижении функциональной безопасности системами, выполненными с применением электрической или электронной технологии или технологии программируемой электроники	В атомной отрасли эта оценка связывается с лицензированием и зависит от национальных регулирующих органов

D.3 Сопоставление МЭК 61508-2 и МЭК 61513

МЭК 61508-2	МЭК 61513
5 Документация	6.3 Выходная документация
6 Управление функциональной безопасностью	5.4.1 Общая программа обеспечения качества
7 Требования к жизненному циклу безопасности Э/Э/ЭП-систем, выполненных с применением различных технологий (электрической или электронной или технологии на основе программируемой электроники)	5 Жизненный цикл безопасности системы Жизненный цикл безопасности системы включает цели и требования к отдельным системам контроля и управления, входящим в архитектуру контроля и управления [см. пункт с) раздела D.1]
7.1 Общие положения В таблице 1 для каждой фазы приведены цели и требования области действия, требуемые входная информация и результаты	В таблице 3 для каждой фазы приведены цели и требования, требуемые входная информация и результаты
Требования безопасности к Э/Э/ЭП-системам включают в себя: - требования к функциям безопасности	6.1.1 Спецификация требований системе включает в себя: требования к прикладным функциям; требования к сервисным функциям; условиям окружающей среды (см. 6.1.1.5)

Окончание таблицы D.3

МЭК 61508-2	МЭК 61513
- требования к значимости функциональной безопасности	категоризацию функций контроля и управления (входные данные из 5.2); требования к ограничениям при проектировании системы (см. 6.1.1.2); классификацию системы
Примечание — Указанные выше разделы МЭК 61508 и МЭК 61513 охватывают основные положения, но в МЭК 61513 делается различие между требованиями к функциям контроля и управления и требованиями к системам контроля и управления, осуществляющим эти функции.	
7.3 Планирование валидации безопасности Э/Э/ЭП-систем	Планирование систем
	План валидации системы (см. 6.2.4). Функциональная валидация требований к прикладным функциям (см. 6.1.3.1.1). Квалификация системы (см. 6.4)
7.4 Проектирование и разработка Э/Э/ЭП-системы	6.1.2 Спецификация системы 6.1.3 Детальное проектирование и внедрение системы
7.4.2 Общие требования	Ограничивающие требования для проектирования (см. 6.1.1.2). Архитектура системы
7.4.3 Требования к значимости функциональной безопасности технических средств системы	Требования, связанные с ограничениями проекта. Приложение С. Требования по способности к тестированию (см. 6.1.1.2.4)
7.4.4 Требования к исключению отказов	Цикл безопасности системы (см. раздел 6)
7.4.5 Требования к контролю систематических сбоев	Защита от развития и побочных эффектов отказов (см. 6.1.2.2.3)
7.4.6 Требования к поведению системы по выявлению дефекта	Архитектура системы (см. 6.1.1.2.1). Самотестирование и устойчивость к отказам (см. 6.1.1.2.3)
7.4.7 Требования при внедрении Э/Э/ЭП-систем	Выбор оборудования (см. 6.1.2.1)
7.4.8 Требования к передаче информации	Внутреннее поведение системы (см. 6.1.2.2.2)
7.5 Интеграция Э/Э/ЭП-системы	6.1.4 Интеграция системы
7.6 Эксплуатационные процедуры и процедуры обслуживания Э/Э/ЭП-системы	6.2.6 План эксплуатации системы
7.7 Валидация функциональной безопасности Э/Э/ЭП-системы	6.1.5 Валидация системы
7.8 Модификация Э/Э/ЭП-системы	6.1.7 Модификация системы
7.9 Верификация Э/Э/ЭП-системы	6.2.1.1 План верификации системы
8 Оценка функциональной безопасности (см. МЭК 61508-1)	См. раздел D.2

D.4 Сопоставление наиболее важных терминов и определений МЭК 61508-4 и МЭК 61513 и в области применения ядерных технологий

Тема: анализ риска	
МЭК 61508-4	**МЭК 61513**
3.1.2 Опасность Потенциальный источник разрушения (ИСО/МЭК Руководство 51[1]). Примечание — Термин включает в себя понятие опасности для людей, возникающей за счет быстропротекающих процессов (например, пожар и взрыв), а также медленных процессов, влияющих на здоровье людей (например, выделение токсических веществ).	**3.27 Опасность**

Тема: глубокоэшелонированная защита	
МЭК 61508-4	**МЭК 61513**
3.4.3 Устройства снижения риска Меры по снижению или ограничению рисков, которые реализуются без использования Э/Э/ЭП-систем и систем на основе других технологий	**Концепция глубокоэшелонированной защиты** (см. раздел А.3) Концепция снижения риска обязательно реализуется при анализе безопасности АС с использованием концепции глубокоэшелонированной защиты и линий (барьеров) защиты

Тема: системы, важные для безопасности	
МЭК 61508-4	**МЭК 61513**
3.4.1 Система, связанная с безопасностью Проектируемая система, которая: - выполняет требуемые функции безопасности, необходимые для достижения и поддержания безопасного состояния контролируемого объекта, и - предназначается для достижения с ее помощью или совместно с другими системами, связанными с безопасностью, или внешними устройствами снижения риска, необходимого уровня значимости (надежности) для требуемых функций безопасности	**3.37 Системы, важные для безопасности**

Тема: системы контроля и управления	
МЭК 61508-4	**МЭК 61513**
3.2.6 Электрическая/электронная/использующая программируемую электронику система (Э/Э/ПЭ) Система, основанная на применении электрической (Э) и/или электронной (Э) и/или основанной на применении программируемой электроники (ПЭ) технологии	**3.35 Система контроля и управления**

[1] Руководство 51 ИСО/МЭК:1990 Аспекты безопасности — руководящие принципы включения их в стандарты.

Тема: надежность	
МЭК 61508-4	**МЭК 61513**
3.5.2 Значимость функциональной безопасности Вероятность удовлетворительного выполнения системой, связанной с безопасностью, требуемых функций безопасности при всех определенных условиях в течение определенного периода времени. Примечание — При определении значимости функциональной безопасности все случаи отказов (как случайных отказов оборудования, так и систематических отказов), которые приводят к опасным состояниям, должны быть рассмотрены, например, отказы оборудования, отказы, связанные с программным обеспечением, и отказы в результате электрических помех. Некоторые из указанных типов отказов, в частности случайные отказы оборудования, могут быть охарактеризованы количественно, используя такие средства, как определение частоты опасных отказов или вероятности отказа связанной с безопасностью системы защиты выполнить необходимую функцию по требованию. Однако значимость функциональной безопасности системы зависит также от множества факторов, которые не могут быть аккуратно учтены количественно и должны оцениваться качественно.	**Надежность** В настоящем стандарте надежность оценивается обычно на основе качественных представлений (см. 6.1.1.1.1) (См. 6.1.1.1 и 6.1.3.1.1)

Тема: классификация систем, важных для безопасности	
МЭК 61508-4	**МЭК 61513**
3.5.6 Уровень значимости безопасности Дискретный уровень (один из четырех возможных) для определения требований значимости функциональной безопасности тех функций, которые должны выполняться Э/Э/ЭП-системами, связанными с безопасностью. 4-й уровень соответствует высшему уровню значимости функциональной безопасности, 1-й уровень — низшему уровню	**3.4 Класс системы контроля и управления** Все компоненты, сборки и системы, связанные с безопасностью, классифицируются на основе их функций и значимости для безопасности и проектируются, изготавливаются и устанавливаются в соответствии с этой классификацией (см. раздел 68 МАГАТЭ 75-INSAG-3). Подраздел 8.2.2 МЭК 61226 устанавливает предельное значение для надежности (10^{-4}), которое может быть принято для систем, имеющих программное обеспечение. Для некоторых систем необходимая надежность может превышать реально достижимую. Если необходимо обеспечить такую высокую функциональную надежность, то используют дополнительные, независимые системы, каждая из которых способна выполнять назначенную функцию безопасности. Разнообразие и физическое разделение таких систем снизит вероятность отказа по общей причине (о надежности см. 4.2.2.3.132 МАГАТЭ 75-INSAG-3)

Тема: отказ по общей причине	
МЭК 61508-4	**МЭК 61513**
3.6.10 Отказ по общей причине Отказ, который является результатом одного или более событий, вызывающих одновременный отказ двух или более отдельных каналов многоканальной системы, приводящий к отказу системы.	**3.37 Отказ по общей причине**
Примечание — В 7.6.2.7 МЭК 61508-1 приводятся требования к независимости двух систем. В подразделе 7.6.2.7 указывается, что при анализе можно получить удовлетворительную независимость, даже если не все указанные требования могут быть удовлетворены.	См. 5.3.1.5

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 60709:1981	IDT	ГОСТ Р МЭК 60709 — 2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
МЭК 60780:1984	—	*)
МЭК 60880:1986	IDT	ГОСТ Р МЭК 60880 — 2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
МЭК 60880-2:2000	IDT	ГОСТ Р МЭК 60880 — 2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
МЭК 60964:1989	—	*)
МЭК 60965:1989	—	*)
МЭК 60987:1989	IDT	ГОСТ Р МЭК 60987 — 2010 «Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризованных систем»
МЭК 61000-4-1:2000	MOD	ГОСТ Р 51317.4.1 — 2000 «Совместимость технических средств электромагнитная. Испытания на помехоустойчивость. Виды испытаний»
МЭК 61000-4-2:1995	MOD	ГОСТ Р 51317.4.2 — 99 «Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний»
МЭК 61000-4-3:1995	MOD	ГОСТ Р 51317.4.3 — 99 «Совместимость технических средств электромагнитная. Устойчивость к радиочастотному электромагнитному полю. Требования и методы испытаний»
МЭК 61000-4-4:1995	MOD	ГОСТ Р 51317.4.4 — 99 «Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Требования и методы испытаний»
МЭК 61000-4-5:1995	MOD	ГОСТ Р 51317.4.5 — 99 «Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Требования и методы испытаний»
МЭК 61000-4-6:1996	MOD	ГОСТ Р 51317.4.6 — 99 «Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам, наведенным радиочастотными электромагнитными полями. Требования и методы испытаний»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 61069-1:1991	—	*)
МЭК 61226:1993	IDT	ГОСТ Р МЭК 61226 — 2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
МЭК 61500:1996	—	*)
МЭК 61508-1:1998	IDT	ГОСТ Р МЭК 61508-1 — 2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования»
МЭК 61508-2:2000	IDT	ГОСТ Р МЭК 61508-2 — 2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
МЭК 61508-4:1998	IDT	ГОСТ Р МЭК 61508-4 — 2007 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения»
ИСО/МЭК 12207:1995	IDT	ГОСТ Р ИСО/МЭК 12207 — 1999 «Информационная технология. Процессы жизненного цикла программных средств»
ИСО 9001:1994	IDT	ГОСТ Р ИСО 9001 — 2008 «Системы менеджмента качества. Требования»
МАГАТЭ 50-C-D (Редакция 1):1988	—	**)
МАГАТЭ 50-C-QA (Редакция 1):1988	—	**)
МАГАТЭ 50-SG-D1:1979	—	**)
МАГАТЭ 50-SG-D3:1980	—	**)
МАГАТЭ 50-SG-D8:1984	—	**)
МАГАТЭ 50-SG-D11:1986	—	**)
МАГАТЭ 75-INSAG-3:1988	—	**)

*) 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.

**) Текст документа на русском языке доступен на http.//gost.e-ecolog.ru

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

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Библиография

[1]	IEEE 610:1992	IEEE Standard Computer Dictionary, Compilation of IEEE Standard Computer Glossaries
[2]	IEEE 830:1998	IEEE Recommended Practice for Software Requirements Specifications
[3]	IEEE 828:1998	IEEE Standard for Software Configuration Management Plans
[4]	NUREG-0800	USNRC Standard Review Plan, Section 7.0 (6/97)
[5]	EWICS Position paper 6 (1/85)	System requirements specification for safety related systems
[6]	IEC 61069-2:1993	Industrial—process measurement and control — Evaluation of system properties for the purpose of system assessment — Part 2: Assessment methodology
[7]	IEC 61131-1:1992	Programmable controllers — Part 1: General information
[8]	IEC 61225:1993	Nuclear power plants — Instrumentation and control systems important for safety — Requirements for electrical supplies

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; категории функций безопасности; классификация систем; жизненный цикл; верификация; отказ по общей причине

Редактор *В. Н. Колысов*
Технический редактор *В. Н. Прусакова*
Корректор *С. И. Фирсова*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 07.02.2012. Подписано в печать 22.03.2012. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 9,30 Уч.-изд. л. 8,90. Тираж 108 экз. Зак. 198

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru