ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61513— 2020

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНОЙ СТАНЦИИ

Общие требования

(IEC 61513:2011,
Nuclear power plants — Instrumentation and control important to safety — General requirements for systems,
IDT)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 февраля 2020 г. № 66-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61513:2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования» (IEC 61513:2011 «Nuclear power plants — Instrumentation and control important to safety — General requirements for systems», IDT).

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

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

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

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

6 ВЗАМЕН ГОСТ Р МЭК 61513—2011

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

© Стандартинформ, оформление, 2020

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: эксплуатирующиеся и вновь проектируемые станции 1
1.3 Структура 2
2 Нормативные ссылки 4
3 Термины и определения 5
4 Обозначения и сокращения 17
5 Общий жизненный цикл безопасности систем контроля и управления 17
5.1 Общие положения 17
5.2 Получение требований систем контроля и управления из проектных основ безопасности атомной станции 20
5.3 Выходная документация 22
5.4 Проектирование общей архитектуры систем контроля и управления и назначение функций систем контроля и управления 23
5.5 Общее планирование 28
5.6 Выходная документация 33
6 Жизненный цикл системы безопасности 34
6.1 Общие положения 34
6.2 Требования 36
6.3 Планирование системы 48
6.4 Выходная документация 53
6.5 Квалификация системы 57
7 Общая интеграция и ввод в эксплуатацию 62
7.1 Общие положения 62
7.2 Цели, которые должны быть достигнуты 62
7.3 Выходная документация 63
8 Общая эксплуатация и техническое обслуживание 63
8.1 Общие положения 63
8.2 Цели, которые должны быть достигнуты 63
8.3 Выходная документация 63
Приложение А (справочное) Основные вопросы безопасности атомных станций 64
Приложение В (справочное) Категоризация функций и классификация систем 67
Приложение С (справочное) Качественный анализ мер защиты от отказов по общей причине 71
Приложение D (справочное) Взаимосвязь настоящего стандарта с серией стандартов МЭК 61508 и стандартами атомной отрасли 75
Приложение Е (справочное) Изменения, которые следует внести в последующие издания стандартов подкомитета ПК 45 А для их адаптации с настоящей версией МЭК 61513. . . . 82
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам 83
Библиография 85

Введение

a) Технический опыт, основные вопросы и организация стандарта

МЭК 61513 устанавливает требования к системам контроля и управления (СКУ), которые предназначены для выполнения функций, важных для безопасности на атомных станциях (АС), а также к оборудованию этих СКУ. Стандарт демонстрирует отношения между:

- целями обеспечения безопасности АС и требованиями к общей архитектуре СКУ, важными для безопасности;
- общей архитектурой СКУ и требованиями отдельных систем, важных для безопасности.

Предполагается, что настоящий стандарт будет использоваться проектировщиками, эксплуатирующими организациями, аудиторами и регулирующими органами.

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

МЭК 61513 относится к первому уровню документов подкомитета ПК 45 А МЭК и устанавливает общие требования к системам. Он является базовым среди серии стандартов подкомитета ПК 45 А МЭК.

Более подробная информация о структуре серии стандартов подкомитета ПК 45 А МЭК приведена в пункте d) введения.

c) Рекомендации и ограничения в отношении применения настоящего стандарта

Необходимо отметить, что этот стандарт не устанавливает дополнительных функциональных требований для систем безопасности.

Для того чтобы стандарт сохранял свое значение в будущем, основное внимание в нем уделяется принципиальным вопросам, а не конкретным технологиям.

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

Документом верхнего уровня серии стандартов подкомитета ПК 45 А МЭК является стандарт МЭК 61513. Он содержит общие требования по безопасности к СКУ и оборудованию, которые используют для выполнения функций, важных для безопасности АС. Стандарт МЭК 61513 структурирует серию стандартов подкомитета ПК 45 А МЭК.

МЭК 61513 напрямую ссылается на другие стандарты подкомитета ПК 45 А МЭК по общим темам, связанным с категоризацией функций и классификацией систем, квалификацией, разделением систем, защитой от отказов по общей причине, программными аспектами компьютеризированных систем, аппаратными аспектами компьютеризированных систем и проектированием пунктов управления. Стандарты, указанные непосредственно на этом (втором) уровне, должны рассматриваться вместе с МЭК 61513, как согласованный набор документов.

На третьем уровне в серии стандартов подкомитета ПК 45 А МЭК представлены стандарты, не имеющие прямого отношения к МЭК 61513, являющиеся стандартами, относящимися к конкретному оборудованию, техническим методам или конкретным видам деятельности. Обычно эти документы, ссылающиеся по общим темам на документы второго уровня, могут использоваться сами по себе.

Четвертый уровень, расширяющий серию стандартов подкомитета ПК 45 А МЭК, соответствует техническим отчетам, которые не являются нормативными документами.

МЭК 61513 заимствовал формат представления из базовой публикации серии стандартов по безопасности МЭК 61508 с общей моделью жизненного цикла безопасности и схемой жизненного цикла системы. Что касается ядерной безопасности, то МЭК 61513 обеспечивает интерпретацию общих требований МЭК 61508-1 [1], МЭК 61508-2 и МЭК 61508-4 в отношении ядерной безопасности для сектора ядерных приложений. В этой структуре МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 [2] в части применения в области использования атомной энергии.

В МЭК 61513 приведены ссылки на стандарты ИСО, а также на IAEA 50-C-QA (заменен IAEA 50-C/SG-Q) по темам, связанным с обеспечением качества.

Серия стандартов подкомитета ПК 45 А МЭК последовательно реализует и детализирует принципы и основные аспекты безопасности, представленные МАГАТЭ в кодексе по безопасности АС и серии стандартов МАГАТЭ по безопасности. В частности, это относится к документам: «Требования SSR-2/1», который устанавливает требования безопасности, связанные с проектированием атомных станций, и «Руководство по безопасности NS-G-1.3», который касается систем контроля и управления, важных для безопасности атомных станций. Термины и определения, используемые стандартами подкомитета ПК 45 А, соответствуют используемым МАГАТЭ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНОЙ СТАНЦИИ

Общие требования

Instrumental and control systems important to safety of nuclear power plants.
General requirements

Дата введения — 2020—07—01

1 Область применения

1.1 Общие положения

Системы контроля и управления (СКУ), важные для безопасности, могут быть реализованы на традиционном аналоговом оборудовании, оборудовании, основанном на применении компьютерной технологии (КТ), или с использованием комбинации оборудования обоих типов (см. примечание 1). Настоящий стандарт устанавливает требования и рекомендации (см. примечание 2) для общей архитектуры СКУ, которая может быть построена с использованием указанных технологий.

В настоящем стандарте придается большое значение полноте и точности требований, вытекающих из целей, связанных с безопасностью атомных станций (АС), как предусловия для выработки всесторонних требований к полной архитектуре СКУ, а следовательно, к отдельным СКУ, важным для безопасности.

В настоящем стандарте вводится понятие «концепция безопасности жизненного цикла» архитектуры СКУ в целом и для каждой системы в отдельности. Благодаря этому на первый план выдвигаются отношения между целями безопасности АС и требованиями к архитектуре СКУ, важные для безопасности, а также взаимосвязи между общей архитектурой СКУ и требованиями к отдельным системам, важным для безопасности. Жизненные циклы, представленные и рассмотренные в настоящем стандарте, не являются единственно возможными; могут применяться и другие жизненные циклы, если будут достигнуты цели, заявленные в настоящем стандарте.

Примечание 1 — СКУ могут также использовать электронные модули на основе сложных электронных компонентов, таких как СИС или ПЛИС. В зависимости от цели и функциональности этих компонентов, они могут быть разработаны как в соответствии с руководящими указаниями для обычного электронного оборудования, так и для компьютерного оборудования. Значительная часть руководства для компьютерного оборудования также применима к проектированию оборудования со сложными электронными компонентами, в том числе включая вопросы повторного применения существующих проектов, а также оценку проектных ошибок в программном обеспечении и сложных проектах аппаратного обеспечения.

Примечание 2 — Далее термин «требования» обозначает как собственно требования, так и рекомендации. Если необходимо, то различие между этими терминами отмечается, при этом требования характеризуются словом «должен», а рекомендации — словами: «следует», «целесообразно».

1.2 Применение: эксплуатирующиеся и вновь проектируемые станции

Стандарт применим как к СКУ на новых АС, так и к реконструируемым и модернизируемым СКУ на действующих станциях.

Для действующих станций применима Часть требований, объем применимых требований следует определять в начале любого проекта.

Издание официальное

1.3 Структура

Стандарт состоит из четырех нормативных разделов: (описание приведено на рисунке 1):

- раздел 5 посвящен общей архитектуре СКУ, важных для безопасности, в том числе:

  - определению (на основе анализа безопасности АС) требований к функциям контроля и управления и связанным с этими функциями СКУ и соответствующим оборудованием АС, категоризации функций контроля и управления, к компоновке оборудования и его эксплуатации;

  - декомпозиции общей архитектуры СКУ с разделением ее на ряд систем и распределение функций контроля и управления между ними. Определяются проектные критерии, включая глубокоэшелонированную защиту и возможности минимизации отказа по общей причине (ООП);

  - планированию общей архитектуры СКУ;

- раздел 6 посвящен требованиям к отдельным СКУ, важным для безопасности, в частности требованиям к компьютеризированным системам. Раздел включает дифференцирование требований в зависимости от категории безопасности реализованных функций СКУ;

- разделы 7 и 8 посвящены общей интеграции, вводу в эксплуатацию, эксплуатации и техническому обслуживанию СКУ.

Примечание — На рисунке 1 представлена структура стандарта. На рисунке не представлена информация по временной последовательности выполнения работ, которые могут выполняться либо параллельно, либо в режиме итераций.

Дополнительно стандарт содержит справочные приложения:

- приложение А приводит взаимосвязи между концепциями МАГАТЭ и общими концепциями безопасности, которые приведены по тексту настоящего стандарта;

- приложение В содержит информацию о принципах категоризации/классификации;

- приложение С приводит примеры чувствительности СКУ к отказам по общей причине (ООП);

- приложение D содержит рекомендации по сравнению настоящего стандарта с частями 1, 2 и 4 МЭК 61508. В этом приложении исследуются основные требования МЭК 61508 для целей верификации того, что аспекты, важные для безопасности, в достаточной степени учтены, а также рассматривается однообразное применение терминов и объясняются предпосылки применения дополнительных методик и терминов;

- приложение Е указывает изменения, которые будут внесены в последующие издания дочерних стандартов МЭК 61513, чтобы привести их в соответствие и свести к минимуму пересечения в их содержаниях.

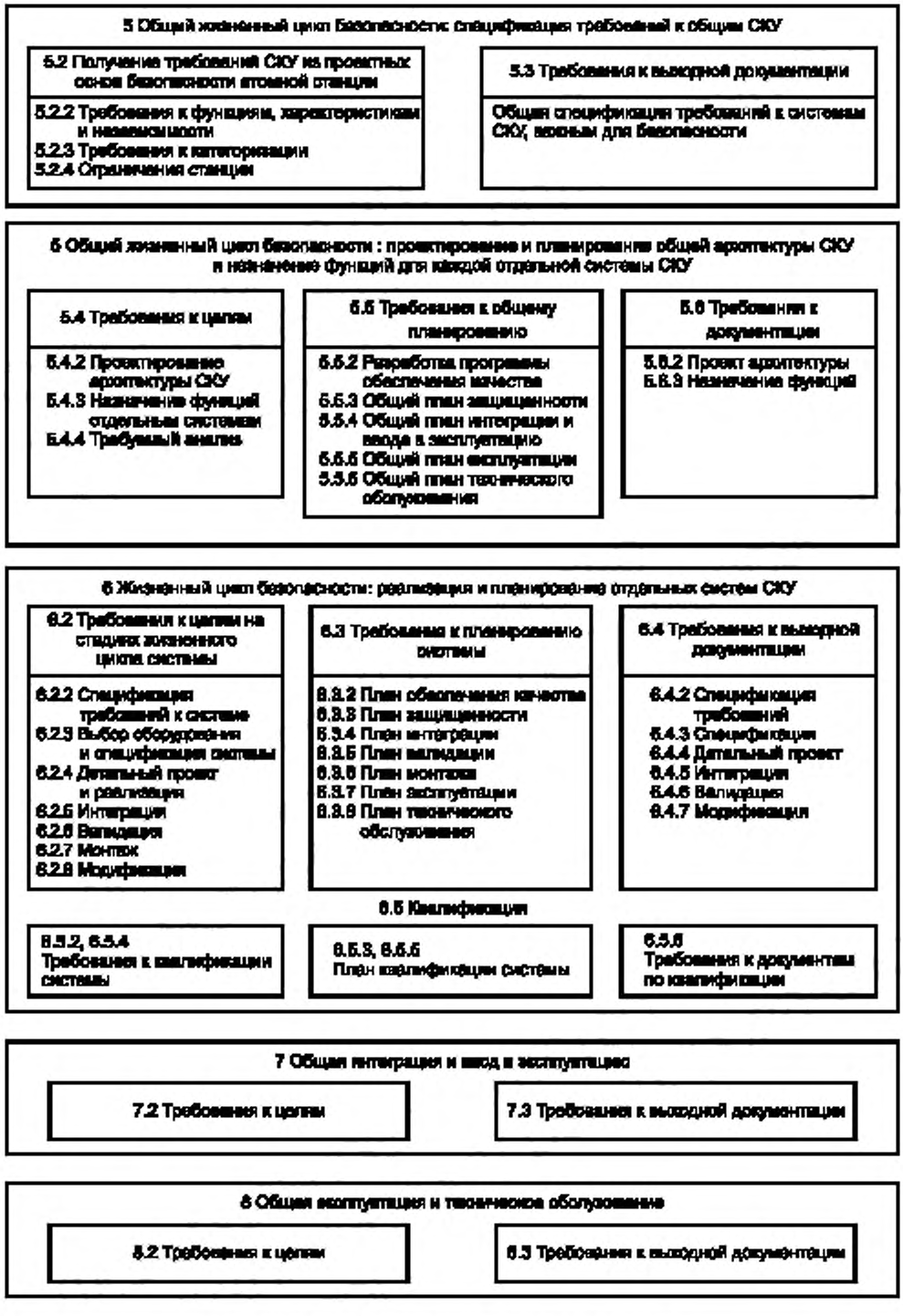


Рисунок 1 — Общая структура настоящего стандарта

2 Нормативные ссылки

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

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

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

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

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

IEC 60964:2009[2)], Nuclear power plants — Control rooms — Design (МЭК 60964:2009, Атомные станции. Пункты управления. Проектирование)

IEC 60965, Nuclear power plants — Control rooms — Supplementary control points for reactor shutdown without access to the main control room (МЭК 60965, Атомные станции. Пункты управления. Дополнительные пункты управления для остановки реактора без доступа к блочному пункту управления)

IEC 60980, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations (МЭК 60980, Рекомендуемые практики для сейсмической квалификации электрического оборудования системы безопасности для атомных станций)

IEC 60987:2007, Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems (МЭК 60987:2007, Атомные станции. Контроль и управление, важные для безопасности. Требования к аппаратному обеспечению компьютеризированных систем)

IEC 61000-4-1[3)], Electromagnetic compatibility (EMC) — Part 4-1: Testing and measurement techniques — Overview of IEC 61000-4 series [МЭК 61000-4-1, Электромагнитная совместимость (ЭМС). Часть 4-1. Тестирование и техники измерений. Обзор серии МЭК 61000-4]

IEC 61000-4-2, Electromagnetic compatibility (EMC) — Part 4-2: Testing and measurement techniques — Electrostatic discharge immunity test [МЭК 61000-4-2, Электромагнитная совместимость (ЭМС). Часть 4-2. Тестирование и техники измерений. Устойчивость к электростатическим разрядам]

IEC 61000-4-3, Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques — Radiated, radio-frequency, electromagnetic field immunity test [МЭК 61000-4-3, Электромагнитная совместимость (ЭМС). Часть 4-3. Тестирование и техники измерений. Устойчивость к радиочастотному электромагнитному полю]

IEC 61000-4-4, Electromagnetic compatibility (EMC) — Part 4-4: Testing and measurement techniques — Electrical fast transient/burst immunity test [МЭК 61000-4-4, Электромагнитная совместимость (ЭМС). Часть 4-4. Тестирование и техники измерений. Устойчивость к наносекундным импульсным помехам]

IEC 61000-4-5, Electromagnetic compatibility (EMC) — Part 4-5: Testing and measurement techniques — Surge immunity test ([ЭК 61000-4-5, Электромагнитная совместимость (ЭМС). Часть 4-5. Тестирование и техники измерений. Испытание на устойчивость к броскам]

IEC 61000-4-6, Electromagnetic compatibility (EMC) — Part 4-6: Testing and measurement techniques — Immunity to conducted disturbances, induced by radio-frequency fields [МЭК 61000-4-6, Электромагнитная совместимость (ЭМС). Часть 4-6. Тестирование и техники измерений. Устойчивость к кондуктивным помехам, наведенным радиочастотными электромагнитными полями]

IEC 61226:2009, Nuclear power plants — Instrumentation and control systems important to safety — Classification of instrumentation and control functions (МЭК 61226:2009, Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления)

[1)] *Заменен на IEC/IEEE 60780-323:2016.*

[2)] *Заменен на IEC 60964:2018.*

[3)] *Заменен на IEC/TR 61000-4-1:2016.*

IEC 61500, Nuclear power plants — Instrumentation and control important to safety — Data communication in systems performing category A functions (МЭК 61500, Атомные станции. Контроль и управление, важные для безопасности. Передача данных в системах, выполняющих функции категории А)

IEC 61508-2:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (МЭК 61508-2:2010, Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 2. Требования к системам)

IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safetyrelated systems — Part 4: Definitions and abbreviations (МЭК 61508-4:2010, Функциональная безопасность электрических/электронных/программируемых электронных систем, связанных с безопасностью. Часть 4. Термины и определения)

IEC 62138:2004[1)], Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions (МЭК 62138:2004, Атомные станции. Контроль и управление, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории В или С)

IEC 62340, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF) [МЭК 62340, Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине (ООП)]

ISO 9001:2008[2)], Quality management systems — Requirements (ИСО 9001:2008, Системы менеджмента качества. Требования)

IAEA INSAG-10:1996, Defence in Depth in Nuclear Safety (МАГАТЭ INSAG-10:1996, Глубокоэшелонированная защита в ядерной безопасности)

IAEA NS-R-1:2000[3)], Safety of Nuclear Power Plants: Design (МАГАТЭ NS-R-1:2000, Безопасность атомных станций: Проектирование)

IAEA GS-R-3:2006, The Management System for Facilities and Activities Safety — Requirements (МАГАТЭ GSR Part 2:2017, Лидерство и менеджмент для обеспечения безопасности. Общие требования безопасности)

IAEA GS-G-3.1:2006, Application of the Management System for Facilities and Activities — Safety Guide (МАГАТЭ GS-G-3.1:2006, Применение системы управления для установок и деятельности. Руководство по безопасности)

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

IAEA 75-INSAG-3 Rev.1 — INSAG 12:1999, Basic Safety Principles for Nuclear Power Plants (МАГАТЭ 75-INSAG-3 Rev.1 — INSAG 12:1999, Основные принципы безопасности для атомных станций)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **прикладная функция** (application function): Функция СКУ, которая выполняет задачу, связанную в большей степени с контролируемым процессом, а не с работой самой системы.

Примечание 1 — См. также термины «СКУ функция», «СКУ», «прикладное программное обеспечение».

Примечание 2 — Прикладная функция обычно является подфункцией СКУ функции.

3.2 **прикладное программное обеспечение** (application software): Часть программного обеспечения СКУ, которая обеспечивает выполнение прикладных функций.

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

Примечание 2 — Прикладное программное обеспечение отличается от системного программного обеспечения.

[1)] *Заменен на IEC 62138:2018.*

[2)] *Заменен на ISO 9001:2015.*

[3)] *Заменен на IAEA SSR-2/1 (Rev.1):2016.*

Примечание 3 — См. также рисунок 2.

Примечание 4 — В некоторых случаях для данного стандарта, в области сложных электронных компонентов, термин «прикладная логика» может являться заменой термину «прикладное программное обеспечение».

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

Примечание 1 — Если используется ранее разработанное оборудование, такая библиотека считается частью системного программного обеспечения и квалифицируется соответствующим образом.

Примечание 2 — См. также рисунок 2.

3.4 **категория функции СКУ**[1] (category of an I&C function): Одно из трех возможных обозначений (A, B, C) функций СКУ, устанавливаемое в результате рассмотрения влияния выполняемой функции на безопасность.

Примечание 1 — См. также термины: «класс СКУ», «функция СКУ».

Примечание 2 — МЭК 61226 определяет категории функций СКУ. Каждой категории соответствует набор требований, применяемый как к каждой функции (относительно их спецификаций, проекта, реализации, верификации и валидации), так и к целому набору элементов, которые необходимы для реализации функции (относительно свойств и требуемой квалификации) независимо от того, как эти элементы распределены в ряду взаимосвязанных СКУ. Для большей ясности этот стандарт определяет категории функций СКУ и классы СКУ и устанавливает связь между категорией функции и минимальным требуемым классом соответствующих систем и оборудования.

3.5 **канал**[2] (channel): Совокупность взаимосвязанных элементов в системе, которая выдает один выходной сигнал[3].

[Глоссарий МАГАТЭ, издание 2007] [3]

3.6 **класс СКУ**[4] (class of an I&C system): Одно из трех возможных обозначений (1, 2, 3) СКУ, важных для безопасности, присваиваемое в результате рассмотрения требований, предъявляемых к выполнению функций СКУ, имеющих разное значение для безопасности.

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

3.7 **ввод в эксплуатацию** (commissioning): Процесс, посредством которого системы и элементы сооруженных установок и деятельности приводят в рабочее состояние и проверяют на их соответствие проекту и требуемым рабочим параметрам.

Примечание — Ввод в эксплуатацию может включать в себя как неядерные и/или нерадиоактивные, так и ядерные и/или радиоактивные испытания.

[Глоссарий МАГАТЭ, издание 2007]

3.8 **отказ по общей причине ООП**[5] (CCF, common cause failure): Отказ двух или более конструкций, систем и компонентов вследствие единичного события или причины.

Примечание 1 — Общие причины могут быть внутренними или внешними к СКУ.

Примечание 2 — Определение МЭК отличается от определения МАГАТЭ в двух местах:

1) термин «конкретный» был удален, потому что иначе определение ООП не согласовывается с определением «общий отказ» (CMF, common mode failure). Кроме того, это дополнительное слово не является необходимым для понимания этого определения;

---

[1] *Категория функции. Управляющим и информационным функциям категории назначаются в соответствии с федеральными нормами и правилами НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций».*

[2] *Определение канала (системы, функциональной группы) приведено в федеральных нормах и правилах НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций».*

[3] *Канал теряет свою идентичность, когда сигналы одного выхода объединяются с сигналами, поступающими от других каналов (например, от контрольно-измерительного канала или канала обслуживания устройств безопасности).*

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

[5] *Определение «отказов по общей причине» приведено в НП-001-15 «Общие положения обеспечения безопасности атомных станций»: отказы систем (элементов), возникающие вследствие одного отказа или ошибки персонала или внутреннего или внешнего воздействия (события), или иной причины.*

2) слово «и» было заменено на «или», потому что эксперты подкомитета ПК 45 А МЭК полагают, что это была опечатка. В онлайн-словаре МАГАТЭ (NUSAFE) это изменение уже выполнено.

[Глоссарий МАГАТЭ, издание 2007, модифицировано]

3.9 **сложность** (complexity): Степень, при которой проектирование, реализация или поведение системы или элемента является трудной для понимания или верификации.

[IEEE 610, модифицировано] [4]

3.10 **компонент** (component): Одна из составных частей системы. Компонент может представлять собой аппаратное или программное обеспечение и может сам состоять из других компонентов.

[IEEE 610]

Примечание 1 — См. также термины «СКУ», «оборудование».

Примечание 2 — Термины «оборудование», «компонент» и «модуль» часто используют как взаимозаменяемые. Взаимоотношения между этими терминами пока не стандартизованы.

Примечание 3 — Это определение подкомитета ПК 45 А МЭК в принципе совместимо с определением термина «компонент», приведенным в группе терминов Глоссария МАГАТЭ издания 2007 г. под названием «Structures Systems and Components (SCC)» (Структуры систем и компонентов). Тем не менее, поскольку там приведены примеры только компонентов аппаратного обеспечения, что может ввести в заблуждение читателя, подкомитет ПК 45 А МЭК предпочитает использовать определение, которое явно касается и компонентов программного обеспечения[1)].

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

Примечание — Эквивалент — цифровая система, система с программным обеспечением, программируемая система.

3.12 **управление конфигурацией** (configuration management): Процесс определения и документирования характеристик конструкций, систем и компонентов установки (в том числе компьютерных систем и программного обеспечения), а также обеспечения того, чтобы изменения этих характеристик должным образом прорабатывались, оценивались, утверждались, распространялись, вводились, проверялись, регистрировались и включались в документацию установки.

[Глоссарий МАГАТЭ, издание 2007]

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

[IEEE 610, модифицировано]

Примечание — См. рисунок 2.

3.14 **глубокоэшелонированная защита** (defence-in-depth): Применение более чем одной защитной меры для достижения какой-либо конкретной цели безопасности, так чтобы эта цель была достигнута, даже если одна из принятых защитных мер окажется безрезультатной.

[Глоссарий МАГАТЭ, издание 2007]

Примечание — См. также раздел А.4.

3.15 **разнообразие**[2)] (diversity): Наличие двух или более резервных систем или компонентов для выполнения одной определенной функции, при котором разные системы или компоненты наделяются различными признаками таким образом, чтобы уменьшалась возможность отказа по общей причине.

[Глоссарий МАГАТЭ, издание 2007, модифицировано]

[1)] *Следует учитывать, что в Глоссарии МАГАТЭ (издание 2007 г.) приводится группа терминов «Structures Systems and Components (SCC)» (структуры систем и компонентов), а в НП-001-15 «Общие положения обеспечения безопасности атомных станций» применяемые для реализации проекта АС средства разделяют и определяют в двучленной форме — «систем» и «элементов». Дополнительно в НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций» для управляющих систем, важных для безопасности, дано определение понятию «функциональная группа».*

[2)] *Понятие «принцип разнообразия» определено в НП-001-15 «Общие положения обеспечения безопасности атомных станций».*

Примечание 1 — Если термин «разнообразие» используют в сочетании с дополнительными признаками, то собственно разнообразие имеет основное значение «существование двух или более различных путей или средств достижения конкретной цели», а дополнительные признаки указывают характеристики применяемых различных путей, т. е. функциональное разнообразие, разнообразие оборудования, разнообразие сигнальных устройств.

Примечание 2 — См. также термин «функциональное разнообразие».

3.16 **оборудование** (equipment): Одна или более частей системы. Единица оборудования — отдельный (обычно заменяемый) элемент или часть системы.

Примечание 1 — См. также термины «компонент», «СКУ».

Примечание 2 — Оборудование может включать в себя программное обеспечение.

Примечание 3 — Термины «оборудование», «компонент», «модуль» часто используются как взаимозаменяемые. Взаимоотношение между этими терминами пока не стандартизировано.

Примечание 4 — Это определение отличается от приведенного определения в МЭК 60780. Отклонение оправдано тем, что МЭК 61513 рассматривает термин «оборудование» как часть системы, тогда как МЭК 60780 рассматривает оборудование как объект квалификации.

3.17 **комплекс оборудования**[1)] (equipment family): Набор аппаратных и программных компонентов, которые могут работать совместно в одной или более определенных архитектурах или конфигурациях.

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

Примечание 2 — Комплекс оборудования может быть как продуктом от определенного производителя, так и набором продуктов, соединение и адаптация которых выполнены поставщиком.

Примечание 3 — Термин «платформа оборудования» иногда используется как синоним термина «комплекс оборудования».

3.18 **ошибка** (error): Различие между рассчитанным, наблюдаемым или измеренным значением или состоянием и истинным, установленным или теоретическим значением или состоянием.

Примечание — См. рисунок 3.

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

[МЭК 61069-1:1991, пункт 2.2.2] [5]

3.20 **отказ** (failure): Потеря возможности конструкции, системы или компонента функционировать в пределах критериев приемлемости.

[Глоссарий МАГАТЭ, издание 2007, модифицировано]

Примечание 1 — Оборудование считается отказавшим, когда оно становится неспособным функционировать, независимо от того, требуется ли его функционирование в данный момент или нет. Отказ, например, в резервной системе может не проявляться до тех пор, пока система не будет задействована во время испытаний либо при отказе резервируемой системы.

Примечание 2 — Отказ является результатом дефекта аппаратного обеспечения, дефекта программного обеспечения, дефекта системы или ошибки оператора или технического обслуживания и связан с траекторией сигнала, которая приводит к отказу.

Примечание 3 — См. также термины: «дефект», «дефект программного обеспечения».

Примечание 4 — Эксперты подкомитета ПК 45 А МЭК считают, что в определении МАГАТЭ не учтено, что отказ является событием, а не состоянием. Эксперты подкомитета ПК 45 А МЭК предложили модифицировать определение с учетом данной точки зрения.

3.21 **дефект** (fault): Неисправность в аппаратуре, программном обеспечении или в компоненте системы.

[1)] *Разработка конфигураций, специфичных для станции, и соответствующего прикладного программного обеспечения может поддерживаться инструментальными программными средствами. Комплекс оборудования обеспечивает набор стандартных функциональностей (например, библиотеку прикладных функций), которые могут быть объединены с целью реализации специального прикладного программного обеспечения.*

Примечание 1 — См. также рисунок 3.

Примечание 2 — Дефекты могут быть результатом случайных отказов, которые возникают, например, из-за деградации аппаратуры в результате старения; возможны систематические дефекты, например дефекты в программном обеспечении, возникающие из-за ошибок при проектировании.

Примечание 3 — 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 4 — См. также термин «дефект программного обеспечения».

3.22 **функциональное разнообразие** (functional diversity): Применение разнообразия на уровне прикладных функций производственных процессов (например, приведение в действие механизма автоматического отключения при достижении предельных значений давления и температуры).

[МЭК 60880:2006, пункт 3.19, модифицировано]

Примечание — Глоссарий МАГАТЭ по безопасности издания 2007 года не дает определения функционального разнообразия, но приводит примеры средств по его достижению. Это определение подкомитета ПК 45 А МЭК совместимо со средствами достижения, обозначенными в Глоссарии МАГАТЭ по безопасности.

3.23 **функциональная валидация** (functional validation): Верификация правильности спецификаций прикладных функций относительно функциональных и рабочих требований верхнего уровня. Функциональная валидация дополняет системную валидацию, которая верифицирует соответствие системы спецификации функций.

3.24 **функциональность** (functionality): Характеристика функции, которая определяет действия, преобразующие входную информацию в выходную информацию.

Примечание — Функциональность прикладных функций обычно влияет на работу станции. Входная информация может быть получена от датчиков, операторов, иного оборудования или программного обеспечения. Выходная информация может воздействовать на исполнительные механизмы, операторов, прочее оборудование и программное обеспечение (см. МЭК 61508-2).

3.25 **угроза** (hazard): Событие, обладающее потенциалом причинить вред здоровью персонала станции или привести к повреждению компонентов, оборудования или структур. Угрозы подразделяют на внутренние и внешние[1)].

Примечание 1 — Внутренние угрозы представляют собой, например, пожар и затопление, внутренние опасности могут являться последствиями ПИС (например, авария с потерей теплоносителя, разрыв паропровода).

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

3.26 **ошибка персонала**[2)] [human error (or mistake)]: Действие персонала, которое приводит к непредвиденному результату.

[МЭК 60880:2006, пункт 3.21]

3.27 **архитектура СКУ** (I&C architecture): Организационная структура СКУ станции, которые являются важными для безопасности.

Примечание 1 — См. также термины: «архитектура СКУ», «СКУ».

Примечание 2 — Организационная структура определяет, главным образом, основные функции, класс и границы каждой системы, взаимосвязь и независимость систем, приоритетность и голосование между одновременно действующими сигналами, ЧМИ.

[1)] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» введены определения «внутренних воздействий» и «внешних воздействий». Внутренние воздействия (события) — воздействия, возникающие при нарушении нормальной эксплуатации, вызванные отказами элементов АС или ошибками персонала, включая ударные волны, струи, летящие предметы, изменение параметров среды (например, давления, температуры, химической активности), пожары, затопления. Внешние воздействия (события) — воздействия характерных для площадки АС природных явлений и деятельности человека, например землетрясение, высокий и низкий уровень наземных и подземных вод, ураганы, аварии на воздушном, водном и наземном транспорте, пожары, взрывы на прилегающих к АС объектах и другие.*

[2)] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» введено определение «ошибка персонала», под которой понимается единичное непреднамеренное неправильное действие или единичный пропуск правильного действия при управлении системами и элементами АС, или единичное непреднамеренное неправильное действие, или пропуск правильного действия при техническом обслуживании или ремонте систем и элементов АС.*

Примечание 3 — В этом стандарте термин определяет только часть общей архитектуры СКУ станции. Позднее включаются также неклассифицируемые системы и оборудование.

Примечание 4 — Для простоты использования термин «общая архитектура СКУ» используется как краткая форма термина «общая архитектура СКУ, важных для безопасности».

3.28 **функция СКУ** (I&C function): Функция контроля, управления и/или наблюдения за определенной частью процесса[1)].

Примечание 1 — Термин «функция СКУ» используется инженерами-технологами, чтобы структурировать функциональные требования к СКУ. Функция СКУ определена следующим образом:

- дает полное представление о функциональных целях;
- может быть категоризирована в соответствии с ее степенью важности для безопасности;
- для достижения функциональной цели учитывает малейшие сущности: от датчика до исполнительного устройства.

Примечание 2 — Функция СКУ может быть подразделена на несколько подфункций (например, на функцию измерения, функцию управления, функцию приведения в действие) в целях распределения по СКУ.

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

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

Примечание 1 — См. также термины «система», «функция СКУ».

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

Примечание 3 — В соответствии с их типовой функциональностью МАГАТЭ устанавливает различие между системами автоматического и ручного управления, системами взаимодействия «человек — машина», системами защиты и блокировки (см. раздел В.4).

3.30 **архитектура СКУ, функциональная структура СКУ** (I&C architecture): Организационная структура СКУ.

Примечание — См. также термин «архитектура СКУ».

3.31 **независимое оборудование**[2)] (independent equipment): Оборудование, которое обладает двумя следующими характеристиками:

1) способность выполнять требующуюся функцию не зависит от работы или отказа другого оборудования;

2) способность выполнять предназначенную функцию не зависит от эффектов, возникающих в результате постулируемого в проекте исходного события, при наступлении которого оно должно функционировать.

[Глоссарий МАГАТЭ, издание 2007]

Примечание — Средствами достижения независимости в проекте является электрическая изоляция (в документах МАГАТЭ употребляется также термин «функциональная изоляция»), физическое разделение и коммуникационная независимость.

[1)] *В НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций» определено понятие «функциональной группы» — совокупности элементов управляющей системы, важной для безопасности, выполняющей управляющую или информационную функцию в установленном проектом АС объеме. А выполняемые этими системами функции разделены на управляющие (как автоматические, так и автоматизированные) и информационные.*

[2)] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» введено определение «принцип независимости», под которым понимается принцип повышения надежности путем применения функционального и/или физического разделения каналов (элементов), при котором отказ одного канала (элемента) не приводит к отказу другого канала (элемента). Под «каналом» (системы, функциональной группы) понимается часть системы (функциональной группы), выполняющая функцию системы (функциональной группы) в установленном проектом АС объеме (НП-026-16).*

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

[IEEE 610] [4]

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

Узлы, важные для безопасности, включают:

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

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

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

[Глоссарий МАГАТЭ, издание 2007]

Примечание 1 — Определение охватывает все аспекты ядерной безопасности.

Примечание 2 — В этом стандарте рассматриваемые элементы будут, главным образом, СКУ или функциями СКУ.

Примечание 3 — См. также «функции СКУ».

3.34 **общий жизненный цикл безопасности СКУ** (overall I&C safety life cycle): Необходимая деятельность, относящаяся к реализации систем и оборудования, важных для безопасности, общей архитектуры СКУ и выполняемая в течение периода времени, который начинается с формирования требований СКУ из проектных основ безопасности АС и заканчивается, когда ни одна из СКУ не доступна к использованию.

[МЭК 61508-4:2010, пункт 3.7.1, модифицировано] [6]

Примечание 1 — Общий жизненный цикл системы контроля и управления (жизненный цикл СКУ) определяет требования к жизненным циклам безопасности отдельных систем.

Примечание 2 — См. также термин «жизненный цикл безопасности системы».

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

[Глоссарий МАГАТЭ, издание 2007]

3.36 **существующие узлы** (pre-existing items). Аппаратное или программное обеспечение или оборудование с программным обеспечением, которые уже существуют как коммерческий или специализированный продукт и доступно для применения.

Примечание — Это определение включает ранее разработанное программное обеспечение, см. МЭК 60880:2006, пункт 3.28.

3.37 **проектная организация**[2] (project organisation): Организация(и) или лица, которые несут ответственность на всех стадиях общего жизненного цикла безопасности СКУ и/или жизненных циклов СКУ определять и осуществлять всю управленческую и техническую деятельность, связанную с функциями СКУ, системами и оборудованием, важными для безопасности.

---

[1] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» определено понятие «элементы АС (элементы)» как изделия (в т. ч. приборы, средства измерения, контроля, управления и автоматики, кабели и др.), обеспечивающие выполнение заданных функций самостоятельно или в составе систем и рассматриваемые в проекте АС в качестве структурных единиц при выполнении анализов надежности и безопасности. Элементы АС разделены на «важные для безопасности» и «остальные, не влияющие на безопасность». При этом под «безопасностью АС (ядерной и радиационной)» понимается свойство АС обеспечивать надежную защиту персонала, населения и окружающей среды от недопустимого в соответствии с федеральными нормами и правилами в области использования атомной энергии радиационного воздействия.*

[2] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» определено понятие «разработчики проекта АС (РУ) — организации, разрабатывающие проект АС (РУ) и обеспечивающие его научно-техническое, в том числе конструкторское, сопровождение на всех этапах полного жизненного цикла АС (РУ)».*

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

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

Примечание 1 — Квалификационные требования получают из определенного класса СКУ и из особого контекста применения.

Примечание 2 — СКУ, как правило, создают на основе взаимодействующих комплектов оборудования. Такое оборудование может быть разработано как часть проекта или это может быть существующее оборудование (т. е. разработанное в рамках предыдущего проекта или быть коммерческим стандартным продуктом). Обычно квалификация «СКУ» осуществляется поэтапно: на первом этапе осуществляется квалификация отдельного существующего оборудования (обычно на раннем этапе процесса реализации системы); на втором этапе осуществляется квалификация интегрированной СКУ (т. е. финальный реализованный проект).

Примечание 3 — Квалификация СКУ всегда является определенной деятельностью для конкретного приложения и применения на станции. Однако она может основываться в значительной степени на работе по квалификации, выполненной вне рамок конкретного проекта станции (эта деятельность называется «общая квалификаци» или «предварительная квалификация»). Предварительная квалификация может значительно снизить трудозатраты на специальную станционную квалификацию, однако следует продемонстрировать соответствие требованиям для конкретного применения.

3.39 **качество** (quality): Степень, с которой совокупность собственных характеристик выполняет требования.

[ИСО 9000:2005] [6]

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

[Глоссарий МАГАТЭ, издание 2007]

Примечание — Это определение соответствует определению ИСО 8402:1994, пункт 3.5 [7].

3.41 **план качества** (quality plan): Документ, определяющий специальные меры в области качества, ресурсы и последовательность действий в отношении конкретного продукта, проекта или контракта.

3.42 **резервирование**[1)] (redundancy): Использование альтернативных (одинаковых или неодинаковых) конструкций, систем и элементов таким образом, чтобы все они могли выполнять требующуюся функцию независимо от эксплуатационного состояния или отказа (выхода из строя) любого из них.

[Глоссарий МАГАТЭ, издание 2007]

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

[Глоссарий МАГАТЭ, издание 2007, модифицировано]

Примечание 1 — Надежность компьютеризированной системы включает в себя надежность его аппаратного обеспечения, которая обычно определяется количественно, и надежность его программного обеспечения, которая обычно является качественной мерой, т. к. не существует общепризнанных средств для определения количественной оценки надежности программного обеспечения.

Примечание 2 — Это определение отличается от издания Глоссария МАГАТЭ по безопасности 2007 года в части «вероятность того, что система или компонент будут удовлетворять минимальным требованиям в отношении рабочих характеристик, когда это требуется». Эксперты подкомитета ПК 45 А МЭК указали, что в определение МАГАТЭ не включено понятие «время выполнения задания», что не согласовывается с общей практикой.

3.44 **требование** (requirement): Выражение в содержании документа, передающее критерии, которые необходимо выполнить в случае заявления о соответствии данному документу и отклонение от которых недопустимо.

[ИСО/МЭК Директивы, часть 2, 2004, пункт 3.12.1] [8]

---

1) *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» определено схожее понятие «принцип резервирования», под которым понимается принцип повышения надежности путем применения нескольких одинаковых или неодинаковых элементов (каналов, систем) таким образом, чтобы каждый из них мог выполнить требуемую функцию независимо от состояния, в том числе отказа, других элементов (каналов, систем), предназначенных для выполнения этой функции.*

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

требования безопасности — требования, налагаемые полномочными органами (законодательными органами, регулирующими органами или органами по стандартизации) и проектными организациями, по безопасности АС с точки зрения воздействия на людей, общество и окружающую среду в течении жизненного цикла АС;

функциональные и эксплуатационные требования — функциональные требования определяют действия, которые будут совершены системой в ответ на определенные сигналы или условия, а эксплуатационные требования определяют характеристики, такие как время отклика и точность;

производственные требования — требования к производственной мощности и возможности станции, налагаемые эксплуатирующей организацией;

требования к проекту станции — технические требования к общему проекту станции по выполнению требований безопасности и производственных требований;

требования к проекту системы — требования проекта к отдельным системам для целей реализации проекта станции в целом, отвечающего требованиям к проекту станции;

требования к оборудованию — требования к отдельному оборудованию для выполнения требований к проекту системы.

Примечание 2 — Глоссарий МАГАТЭ по безопасности 2007 года содержит следующее определение:

требуемый, требование — требуемый (национальными или международными) законами или регулирующими положениями, либо основами безопасности или требованиями безопасности МАГАТЭ.

Это определение МАГАТЭ полезно в структуре публикаций МАГАТЭ, но слишком узкое для использования в техническом стандарте. Оно соответствует определению подкомитета ПК 45 А МЭК «требование безопасности», приведенному в примечании 1.

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

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

[IEEE 610, модифицировано]

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

[Глоссарий МАГАТЭ, издание 2007]

3.47 **система безопасности**[1)] (safety system): Система, важная для безопасности, обеспечивающая безопасный останов реактора или отвод остаточного тепла из активной зоны, либо ограничивающая последствия ожидаемых при эксплуатации событий и проектных аварий.

[Глоссарий МАГАТЭ, издание 2007]

3.48 **защищенность, информационная безопасность (кибербезопасность)** (security): Способность компьютеризированной системы защитить информацию и данные так, чтобы не допустить их прочтения или изменения неавторизованными системами и отдельными лицами, и для того, чтобы авторизованные системы и лица не получали отказов.

[ИСО/МЭК 12207:2008, пункт 4.39, модифицировано] [9]

3.49 **единичный отказ** (single failure): Потеря способности компонента выполнять предписанные ему функции безопасности (функцию безопасности), а также любые последующие отказы, являющиеся результатом этого.

[Глоссарий МАГАТЭ, издание 2007, модифицировано]

Примечание — Это определение отличается от определения Глоссария МАГАТЭ издания 2007 г.[2)] в части «Отказ, который приводит к потере способности системы или элемента выполнять предписанные им функции безопасности, а также любые последующие отказы, являющиеся результатом этого». Термин «система» был удален, потому что эксперты подкомитета ПК 45 А МЭК считают, что оригинальное определение МАГАТЭ для единичного отказа является несоответствующим, т. к. единичный отказ не должен приводить к потере системной функции. В системах, которые соответствуют критерию единичного отказа, не должно быть единичного отказа. Это приводит к порочному кругу в отношении соответствия критерию единичного отказа. Кроме того, модифицированное определение МАГАТЭ соответствует определению подкомитета ПК 45 А МЭК для «отказа».

[1)] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» определено понятие «системы (элементы) безопасности» — системы (элементы), предназначенные для выполнения функций безопасности при проектных авариях.*

[2)] *Определение МАГАТЭ в большей степени, чем определение МЭК, согласуется с принятой в Российской Федерации методологией анализа безопасности.*

3.50 **критерий единичного отказа**[1] (single failure criterion): Критерий (или требование), применяемый к системе таким образом, чтобы она обязательно сохраняла способность выполнять свою функцию в случае любого единичного отказа.

[Глоссарий МАГАТЭ, издание 2007]

Примечание — См. также МАГАТЭ SSR-2/1 (Rev.1), для руководства, как критерий единичного отказа достигается и как это применяется к группе безопасности.

3.51 **программное обеспечение** (software): Программы (т. е. набор упорядоченных команд), данные, правила и любая связанная с этим документация, имеющая отношение к работе компьютеризированной СКУ.

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

Примечание 1 — Все отказы программного обеспечения являются следствием дефектов проектирования, т. к. программное обеспечение состоит исключительно из проектирования и не изнашивается или подвергается физическим отказам. Т. к. запуск активации дефектов программного обеспечения происходят случайным образом в период эксплуатации системы, то отказы программного обеспечения также происходят случайно.

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

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

Примечание — См. также термин «отказ».

3.54 **надежность программного обеспечения** (software reliability): Компонент надежности системы, связанный с отказами программного обеспечения.

3.55 **спецификация**[2] (specification): Документ, определяющий в полной, точной, верифицируемой форме требования, проект, поведение или другие характеристики системы либо компонента, и, зачастую, процедуры для определения, были ли эти требования удовлетворены.

[МЭК 60880:2006, пункт 3.39]

3.56 **система**[3] (system): Совокупность компонентов, взаимодействующих в соответствии с проектом, в котором элемент системы может представлять собой другую систему, называемую подсистемой.

[МЭК 61508-4:2010, пункт 3.3.1, модифицировано]

Примечание 1 — См. также термин «СКУ».

Примечание 2 — СКУ отделяют от механических систем и электрических систем АС.

Примечание 3 — Это определение подкомитета ПК 45 А МЭК полностью соответствует определению «системы», данному в Глоссарии МАГАТЭ издания 2007 года в группе терминов «структуры систем и компонентов (SCC)».

3.57 **жизненный цикл безопасности системы** (system safety life cycle): Необходимая деятельность, относящаяся к реализации СКУ, важных для безопасности, и выполняемая в течение периода времени, который начинается со спецификации системных требований на стадии концепта и заканчивается, когда СКУ не доступна к использованию.

Примечание 1 — Жизненный цикл безопасности системы ссылается к деятельности в рамках жизненного цикла СКУ.

Примечание 2 — См. также термин «общий жизненный цикл безопасности системы контроля и управления (жизненный цикл СКУ)».

---

[1] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» определено понятие «принцип единичного отказа», в соответствии с которым система должна выполнять требуемые функции при любом требующем ее работы исходном событии и при учитываемом в проекте АС независимом от исходного события отказе одного из элементов этой системы.*

[2] *Термином «спецификация» в стандартах единой системы конструкторской документации и в стандартах единой системы программной документации обозначаются документы с иным установленным составом и содержанием. В указанных российских системах документации к определению «specification» более близки по своему содержанию документы «техническое задание» либо «технические условия».*

[3] *В НП-001-15 «Общие положения обеспечения безопасности атомных станций» определено понятие «система (система АС)» — совокупность элементов АС, предназначенных для выполнения заданных функций.*

3.58 **системное программное обеспечение** (system software): Программное обеспечение, спроектированное для определенной компьютерной системы или семейства компьютерных систем с целью упрощения эксплуатации и обслуживания компьютерной системы и связанных программ, например операционные системы, ЭВМ, утилиты. Системное программное обеспечение обычно состоит из программного обеспечения операционной системы и инструментальных программ.

Примечание 1 — Программное обеспечение операционной системы: программы, исполняемые в заданном процессоре в течение времени работы системы, такие как операционная система, драйверы ввода/вывода, обработчик исключений, коммуникационное программное обеспечение, библиотеки прикладного программного обеспечения, онлайн-диагностика, управление избыточностью и амортизацией отказов (мягкой деградацией).

Примечание 2 — Инструментальные программы: программное обеспечение, применяемое для разработки, тестирования или обслуживания другого программного обеспечения и систем, такое как компиляторы, генераторы кода, графический редактор, офлайн-диагностика, средства верификации и валидации и т. д.

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

Примечание 4 — См. также рисунок 2.

3.59 **валидация системы** (system validation): Подтверждение путем проверки и предоставления других свидетельств того, что система полностью удовлетворяет спецификации требований, как запланировано (функциональность, время отклика, устойчивость к дефектам и ошибкам, надежность).

[МЭК 60880:2006, пункт 3.42]

Примечание — Глоссарий МАГАТЭ издания 2007 г. предоставляет два следующих определения:

валидация — процесс определения пригодности продукта или услуги для удовлетворительного выполнения определенных функций. Валидация по своему содержанию шире, чем верификация, и может включать более значительный элемент суждения;

валидация компьютерной системы — процесс испытаний и оценки интегрированной компьютерной системы (аппаратные средства и программное обеспечение) с целью обеспечения соблюдения функциональных, эксплуатационных и интерфейсных требований;

во-первых, определение «системная валидация» является частным случаем валидации. Это относится к определенному продукту, а именно к валидации СКУ. Это согласовывается с определением МАГАТЭ. Во-вторых, определение МЭК определяет базу для валидации, а именно, это спецификация требований, тогда как определение МАГАТЭ только ссылается на «определенную функцию».

3.60 **систематический дефект** (systematic fault): Дефект, связанный детерминированным образом с какой-либо причиной, который может быть исключен только путем модификации проекта или производственного процесса, эксплуатационных процедур, документации либо других важных факторов.

[МЭК 61508-4:2010, пункт 3.6.6, модифицировано]

3.61 **типовое(ые) испытание(я)**[1)] [type test(s)]: Испытание на соответствие, проводимое на одном или более образцах, представляющих продукцию.

[МЭК 60050-394:2007, пункт 40-02] [10]

3.62 **верификация**[2)] (verification): Подтверждение исследованием и представлением объективного доказательства того, что результаты деятельности соответствуют целям и требованиям, определенным для этой деятельности.

[МЭК 62138:2004, пункт 3.35]

Примечание 1 — Глоссарий МАГАТЭ издания 2007 г. предоставляет два следующих определения:

валидация — процесс определения пригодности продукта или услуги для удовлетворительного выполнения определенных функций. Валидация по своему содержанию шире, чем верификация, и может включать более значительный элемент суждения;

верификация — процесс определения соответствия качества или характеристик продукта, или услуги тому, что предписывается, предопределяется или требуется.

Определение МАГАТЭ «верификация» очень похоже на определение МАГАТЭ «валидация», поскольку оба адресованы к конечному продукту или сервису.

[1)] *В стандартах системы разработки и постановки продукции на производство (например, ГОСТ 15.309—98) установлено отличающееся по содержанию определение «типовые испытания».*

[2)] *В НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций» определено понятие «верификация» — подтверждение на основе представления объективных свидетельств того, что результат деятельности на стадии жизненного цикла управляющей системы АС, важной для безопасности, получен с соблюдением требований, предъявляемых к этой системе на данной стадии жизненного цикла системы.*

В стандартах подкомитета ПК 45 А МЭК термины «верификация» и «валидация» относятся к процессам жизненного цикла определенных продуктов, а именно, оборудования и СКУ, но не к услугам в целом.

Кроме того, «верификация» и «валидация» применяются для идентификации двух разных и дополняющих друг друга типов оценок.

«Верификация» отражает оценку результатов отдельной деятельности на соответствие ее входам.

«Валидация» отражает оценку конечного продукта на соответствие задокументированным целям и требованиям.



Рисунок 2 — Характерные взаимосвязи между аппаратным обеспечением и программным обеспечением компьютерной системы



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

4 Обозначения и сокращения

АС — атомная станция;
АСУ ТП — автоматизированная система управления технологическим процессом;
ООП — отказ по общей причине;
ППВМ — программируемая пользователем вентильная матрица;
ОК (QA) — обеспечение качества;
ПИС (PIE) — постулированное исходное событие;
ПЛИС — программируемая логическая интегральная схема;
ПНР — пусконаладочные работы;
СКУ (I&C) — система контроля и управления;
СМР — строительно-монтажные работы;
ЧМИ (HMI) — человеко-машинный интерфейс;
СВ — оборудование, основанное на применении компьютерной технологии;
COTS — готовый коммерческий продукт;
FAT — заводские приемочные испытания;
SAT — приемочные испытания на площадке;
SIT — интеграционные испытания на площадке

5 Общий жизненный цикл безопасности систем контроля и управления

5.1 Общие положения

Целью данного раздела является определение:

- требований к архитектуре СКУ, важных для безопасности, исходя из проектных основ безопасности АС (см. разделы А.2 и А.3); и
- требований к отдельным СКУ, важным для безопасности, исходя из этих общих требований.

Для того чтобы убедиться, что все требования безопасности, которым должны соответствовать СКУ, учтены, выполнены и подтверждены, требуется системный подход. Системный подход достигается путем помещения деятельности, связанной с разработкой, реализацией и эксплуатацией СКУ, в контекст жизненного цикла безопасности всей СКУ. Этот жизненный цикл связан, в свою очередь, с жизненными циклами безопасности отдельных СКУ (см. раздел 6).

Этапы типового общего жизненного цикла безопасности СКУ включают следующее:

a) рассмотрение проектных основ безопасности АС, включая (см. 5.2):
   - функциональные и эксплуатационные требования, а также требования к независимости;
   - функциональную категоризацию;
   - ограничения в рамках проекта станции;

b) определение общей спецификации требований к функциям СКУ, системам и оборудованию, важным для безопасности (см. 5.3);

c) проектирование общей архитектуры СКУ и назначение функций СКУ отдельным системам и оборудованию (см. 5.4);

d) общее планирование (см. 5.5);

e) реализацию отдельных систем (см. раздел 6),

f) общую интеграцию СКУ и ввод в эксплуатацию систем (см. раздел 7);

g) общую эксплуатацию СКУ и техническое обслуживание (см. раздел 8).

В скобках указаны раздел и подраздел настоящего стандарта, в которых рассматривается соответствующий этап, а в таблице 1 представлена информация о цели, исходных данных, результатах и назначении каждой стадии (этапа).

Связи между рассматриваемым общим жизненным циклом и жизненными циклами безопасности отдельных СКУ упрощенно показаны на рисунке 4:

a) общий жизненный цикл безопасности СКУ является итеративным процессом, где выходы каждого этапа должны быть верифицированы на согласованность со входами предшествующей деятельности. Этап может начаться, даже если деятельности предыдущих этапов не завершены, если при этом применяются адекватные средства контроля конфигурации, которые гарантируют, что общая последовательность процесса разработки сохраняется;

b) этап должен быть закончен, только если все предшествующие этапы завершены.

Таблица 1 — Обзор общего жизненного цикла безопасности СКУ

Раздел или подраздел	Входы	Цели деятельности	Объект	Выходы
5 Требования, распространяемые на общий жизненный цикл СКУ, и их связь с жизненными циклами систем				
5.2 Получение требований СКУ из проектных основ безопасности АС				
5.2.2 Рассмотрение функциональных и эксплуатационных требований, требований к независимости	Документы по проектным основам безопасности станции. Принципы работы станции	Определить: - общие функциональные и эксплуатационные требования к СКУ, важным для безопасности; - концепцию глубокоэшелонированной защиты станции и требования к независимости, распространяемые на функции СКУ; - автоматические функции и ручное управление	Системы станции и связанные СКУ, важные для безопасности	Определение входных требований для 5.3
5.2.3 Рассмотрение требований к категоризации	Категоризация безопасности станции	Определить категории функций СКУ. Верифицировать полноту. Верифицировать выполнимость комплексных требований	Функции СКУ, важные для безопасности	Определение входных требований для 5.3
5.2.4 Рассмотрение ограничений проекта станции	Документы по размещению станции и исходные данные для проектирования	Определить: - границы систем станции и СКУ; - ограничения вспомогательных систем и размещения станции, условий окружающей среды; - источники потенциальных внутренних и внешних опасностей; - принципы эксплуатации станции и техническое обслуживание	Схема размещения станции. Системы станции. СКУ	Определение ограничений станции для проекта архитектуры (см. 5.4) и спецификации требований к отдельным СКУ (см. 6.2)
5.3 Выходная документация	Выходы 5.2	Разработать общую спецификацию требований к СКУ, важным для безопасности, в терминах функциональных и эксплуатационных требований, требований к независимости и категоризации	СКУ	Общая спецификация требований к СКУ для 5.4
5.4 Проектирование общей архитектуры СКУ и назначение функций СКУ				
5.4.2 Проектирование архитектуры СКУ	Выход 5.3	Спроектировать общую архитектуру СКУ, подходящую для реализации спецификации общих требований СКУ, важных для безопасности. Разработать соответствующие меры против потенциального отказа по общей причине	Функции СКУ и СКУ	Детальный проект архитектуры безопасности СКУ в терминах автоматизированных систем, ЧМИ и взаимосвязей, инструментальных средств (см. 5.6.2)

Окончание таблицы 1

Раздел или подраздел	Входы	Цели деятельности	Объект	Выходы
5.4.3 Назначение функций	Выходы 5.4.2 и 5.5 (итерация с выхода 6.4)	Назначить функции СКУ отдельным системам и оборудованию СКУ. Разработать требования (границы, классификация, функциональность, надежность и другие требуемые характеристики) к отдельным системам	Функции СКУ и СКУ	Требования к прикладным функциям систем и ЧМИ, проекту СКУ и инструментальным средствам (см. 5.6.3)
5.4.4 Необходимый анализ	Выходы 5.4.2 и 5.4.3	Оценить надежность и защиту от ООП. Оценить человеческие факторы	Функции СКУ и СКУ	Оценка надежности и защиты от ООП (5.4.4.2). Оценка человеческих факторов (5.4.4.3)
5.5 Общее планирование	Выход 5.4	Разработать планы ОК, защищенности, интеграции, ввода в эксплуатацию, эксплуатации и технического обслуживания системы	Совместно работающие СКУ	Планы для указанной деятельности
6 Жизненный цикл безопасности системы	Выход 5.6	Определить и создать СКУ, соответствующие спецификации архитектуры СКУ (см. раздел 6)	Отдельные СКУ	Выходы, представленные в таблице 3
7 Общая интеграция и ввод в эксплуатацию	Выходы 5.5.4 и 6.3.6	Испытать и ввести в эксплуатацию взаимосвязанные системы архитектуры СКУ	СКУ архитектуры СКУ	Полностью интегрированные и принятые в эксплуатацию системы. Отчет об общем вводе в эксплуатацию (см. 7.3)
8 Эксплуатация и техническое обслуживание	Выходы 5.5.5, 5.5.6 и 7.2	Эксплуатировать, выполнять техническое обслуживание и ремонт систем для того, чтобы безопасность была обеспечена	СКУ архитектуры СКУ	Непрерывное выполнение функций. Записи по эксплуатации и техническому обслуживанию (см. 8.3)

Примечание — Сравнение приведенных в таблице этапов с этапами по МЭК 61508-1 дано в приложении D.

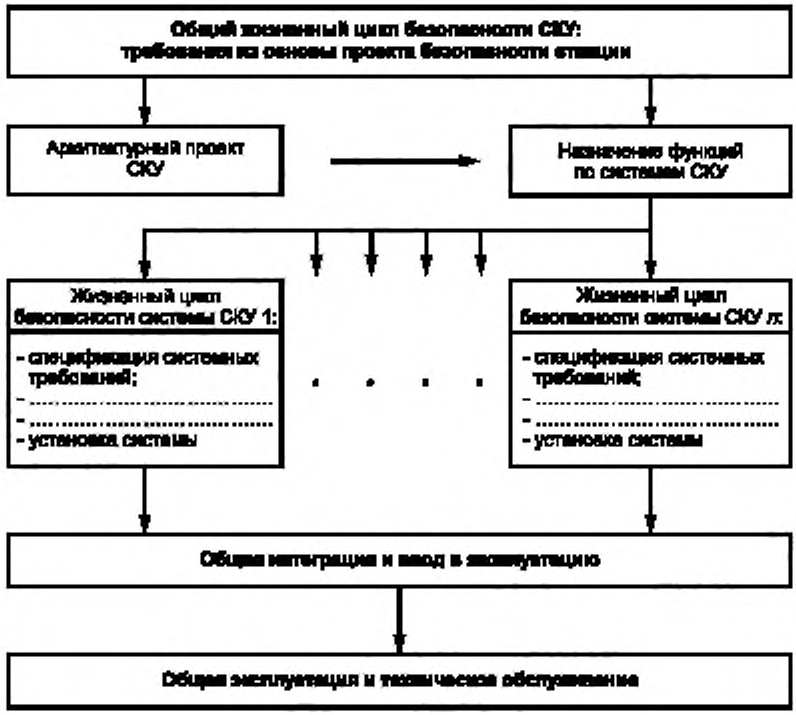


Рисунок 4 — Связь между общим жизненным циклом безопасности СКУ и жизненными циклами безопасности отдельных СКУ

5.2 Получение требований систем контроля и управления из проектных основ безопасности атомной станции

5.2.1 Общие положения

Цель требований данного подраздела состоит в том, чтобы получить входные требования для спецификации СКУ и определить входные ограничения для проекта архитектуры СКУ, вытекающие из проектных основ безопасности АС и требований проекта АС.

75-INSAG-3 определяет набор отдельных «принципов безопасности», которые совместно образуют «интегрированный подход к общей безопасности», обеспечивающий безопасность АС. Эти принципы будут использоваться в проекте МАГАТЭ SSR-2/1 (Rev.1) за счет рассмотрения всех возможных ПИС и последовательных физических барьеров, ограничивающих радиационное воздействие на персонал, население и окружающую среду в рамках установленных пределов (см. разделы А.2, А.3 и А.4). В соответствии с этим подходом в проектные основы безопасности станции определяют соответствующий уровень качества для функций станции и систем, необходимый для поддержания нормальной эксплуатации станции, обеспечения должной реакции на все ПИС и осуществления долговременного управления станции после аварии.

5.2.2 Рассмотрение функциональных и эксплуатационных требований, требований к независимости

Функциональные и эксплуатационные требования и требования к независимости функций СКУ, важных для безопасности, а также принципы эксплуатации станции определяются в проектных основах безопасности станции и являются неотъемлемой частью проекта по проектированию СКУ. Требования, касающиеся взаимодействий человек—машина, учитывают как принципы эксплуатации, так и эргономики, для целей минимизации отказов вследствие человеческого фактора.

Для процесса проектирования СКУ требуется предоставить следующие входные данные из проектных основ безопасности станции:

- концепцию глубокоэшелонированной защиты станции (см. раздел А.4) и группы функций, предназначенных при устранении последствий ПИС для достижения целей безопасности (см. раздел А.3);

Примечание 1 — В тех случаях, когда требуется очень высокая надежность функции, в спецификации требований к станции и СКУ оговаривают различные уровни защиты от одного и того же ПИС, например два или более независимых и функционально разнообразных физических критерия инициирования и, если возможно, вторая, функционально разнообразная, независимая, резервируемая, механическая система для управления аварией.

Примечание 2 — Уровни глубокоэшелонированной защиты могут включать как функции, важные для безопасности, так и другие функции. Требования настоящего стандарта распространяются только на те функции, которые являются важными для безопасности.

- функциональные и эксплуатационные требования к важным для безопасности функциям станции, которые должны соответствовать общим требованиям безопасности (см. раздел А.4);

Примечание 3 — Там, где требуется функциональная валидация (см. 6.2.4.2), в проектных основах указывают начальные условия, допустимые пределы и допустимые скорости изменения параметров станции, которые должны управляться СКУ, важными для безопасности.

- роль автоматизации и регламентированные действия оператора при управлении ожидаемыми эксплуатационными событиями и в аварийных условиях (см. раздел А.4);
- анализ задач в соответствии с 6.3 МЭК 60964:2009, определяющий, какие функции следует назначать оператору, а какие — автоматике;
- переменные, которые должны отображаться оператору для выполнения им действий вручную;
- принципы приоритетности между действиями, инициированными автоматически и вручную, принимая во внимание функциональные категории, пункты или посты управления.

5.2.3 Рассмотрение требований к категоризации

5.2.3.1 Допущения данного стандарта, касающиеся категоризации функций и классификации систем

Функции, системы и оборудование на АС классифицируют в соответствии с их важностью для безопасности (см. С.1). Настоящий стандарт различает категоризацию функций СКУ и классификацию СКУ в соответствии с МЭК 61226[1)].

Примечание 1 — Термины «категоризация» и «классификация» иногда используются как синонимы даже в МЭК 61226. Для ясности в настоящем стандарте термин «категоризация» относят к функциям, а термин «классификация» — к системам.

Эти категории характеризуются набором требований к спецификации, проектированию, реализации, верификации и валидации функций СКУ, а также требованием к свойствам систем в соответствии с категориями, их квалификацией, прикладным функциям, сервисным функциям, функциям системного программного обеспечения системы соответственно.

Согласованные требования применяют ко всей цепочке элементов, которые необходимы для реализации функции данной категории, независимо от того, как она распределяется в ряде взаимосвязанных СКУ. Поэтому целесообразно определить классы систем, которые подходят для реализации функций СКУ вплоть до определенной категории.

Категоризация функций СКУ является частью проектных основ безопасности станции и находится за рамками настоящего стандарта. Этот стандарт предполагает, что в проектных основах безопасности станции отдельные важные для безопасности функции СКУ распределены по трем категориям: А, В или С и что основные требования проекта к системам и оборудованию, связанные с этими категориями, согласуются с требованиями раздела 7 МЭК 61226:2009. Кроме того, требования категории А согласуются с требованиями МАГАТЭ к системам безопасности.

Примечание 2 — Нормативные базы для категоризации функций могут варьироваться в разных странах и отклоняться от базы данного стандарта (МЭК 61226). Особый случай может также возникнуть при применении этого стандарта к существующим станциям, где новые требования к категоризации действительны только для части элементов в рамках проекта модернизации. В таких случаях может потребоваться специальный анализ для определения минимальных требований для каждого класса системы.

[1)] *Классификация важных для безопасности элементов по степени влияния отказа этих элементов на безопасность АС установлена в НП-001-15. Категоризация функций, важных для безопасности управляющих систем, определена в НП-026-16.*

Классификацию СКУ определяет проектная организация СКУ на этапе проектирования архитектуры СКУ до назначения функций СКУ системам (см. 5.4.2 и 5.4.3).

5.2.3.2 Требования:

a) категоризация функций СКУ должна содержаться в проектных основах безопасности станции и должна формировать исходные данные к спецификации общих требований СКУ (см. 5.3);

b) проектная организация СКУ должна рассматривать категоризацию и верифицировать ее на полноту и выполнимость. В случае невыполнимости (например, назначение высокой категории для функции, которая не может удовлетворить критерию единичного отказа из-за проекта станции) определение и категоризация функций СКУ должны быть рассмотрены на соответствие функциональным требованиям СКУ станции. Рассмотрение функциональных требований и связанная с ними категоризация должны повторяться, пока не будет найдено приемлемое решение.

5.2.4 Рассмотрение ограничений проекта станции

Контекст проекта станции накладывает ограничения на проект архитектуры СКУ.

a) Проектная организация СКУ должна определить ограничения, накладываемые на оборудование СКУ схемой размещения станции, интерфейсами с оборудованием станции и событиями вне СКУ, включая:

- границы между системами и оборудованием СКУ и системами станции, в том числе взаимодействие с электрическими/механическими исполнительными системами и вспомогательными системами, такими как системы электроснабжения и кондиционирования;
- диапазон переходных и стационарных условий окружающей среды в нормальных условиях и при отклонении от нормальных условий, включая аварии, при которых СКУ должны функционировать;
- диапазон переходных и стационарных условий генерируемой и потребляемой мощности в нормальных условиях, при отклонении от нормальных условий и аварийные условия, при которых СКУ должны функционировать;
- общие ограничения по трассировке и прокладке кабелей;
- особые ограничения по трассировке и прокладке кабелей к центрам их концентрации, таким как пункт управления и помещения для разводки кабеля;
- ограничения по заземлению и распределению электропитания;
- внешние и внутренние опасности, рассматриваемые в соответствии с допущениями об опасностях на станции. Они включают следующее: пожар, подтопление, обледенение, удар молнии, действие повышенного напряжения, электромагнитные помехи, землетрясение, взрыв или химическое воздействие.

b) Проектная организация СКУ должна определить ограничения, накладываемые на оборудование СКУ принципами эксплуатации, т. е. ограничениями со стороны:

- защищенности;
- эксплуатации и технического обслуживания (см. 5.6 МЭК 60964:2009);
- техническое обслуживание СКУ во время эксплуатации.

Обычно это приводит к дополнительным требованиям, определяющим деление архитектуры СКУ на отдельные подсистемы. При этом необходимо учитывать следующее:

- станция обычно подразделяется на отдельные системы, которые сгруппированы на участках таким образом, чтобы организовать деятельность по инжинирингу, монтажу, пуску и испытаниям;
- оптимальное планирование работ по техническому обслуживанию, периодическим испытаниям и модификации отдельных подсистем станции и подсистем СКУ следует выполнять при полной работоспособности остальных подсистем;
- влияние распределения и разделения обязанностей обслуживающего персонала следует проанализировать и принять во внимание при разделении СКУ;
- требования следует определять в отношении инструментальных средств и рабочих станций для технического обслуживания и диагностики, включая интерфейсы инженерных систем. Эти требования могут касаться человеко-машинного интерфейса для обслуживающего СКУ персонала, интерфейсов с центральными системами управления станцией и т. д.

5.3 Выходная документация

Выходная документация о деятельности, описанной в 5.2, представляет собой спецификации требований для отдельных СКУ, важных для безопасности.

Примечание 1 — Спецификации требований охватывают всю функцию СКУ в целом, начиная от ее входов (датчиков, операторов или другого оборудования) и заканчивая выходами (направленными на исполнительные устройства, операторов или другое оборудование). Дальнейшее разбиение этих спецификаций требований будет формировать спецификации требований к подфункциям на уровне каждой СКУ. Это будет зависеть от выбранной архитектуры СКУ (см. 5.4) и от того, как функции реализуются распределенным оборудованием (измерительные приборы, обработка и исполнительные механизмы).

a) Спецификация требований должна быть установлена для каждой функции СКУ. Она должна включать:

1) спецификацию функциональных требований, определяющих, каким образом функция преобразует входную информацию в выходную с целью эксплуатации или мониторинга работы станции;

2) спецификацию эксплуатационных требований, определяющую диапазон, точность и динамические характеристики функции.

Примечание 2 — Сюда включают требования к своевременности реакции, которые раньше для аппаратных систем могли не учитываться;

3) спецификацию категории функции.

Примечание 3 — Категория однозначно определяет минимальные классификационные требования к СКУ, требуемых для реализации функции (см. таблицу 2).

b) Общая спецификация требований должна определять любую зависимость между функциями, которые задают ограничения при назначении функций СКУ. Это включает следующее:

1) комбинации функций, подлежащие мониторингу, для управления защитными действиями;

2) комбинации функций, обеспечивающих глубокоэшелонированную защиту;

3) комбинации функций, образующих группу безопасности.

c) Спецификации требований всех функций СКУ должны быть верифицированы, чтобы гарантировать, что полный и согласованный набор функций и ограничений определен для целей назначения функций системам и разработки спецификаций этих систем (см. 6.2).

Примечание 4 — Когда начинается подготовка спецификации требований функции СКУ, возможны ситуации, где полный набор датчиков или исполнительных механизмов, связанных с этой функцией, не будет полностью определен. В дальнейшем будет необходимо постепенно доработать спецификацию, для того чтобы все датчики и исполнительные устройства были в нее включены. Также управление каким-либо дополнительным исполнительным механизмом, которое могло быть ранее не учтено, требуется оценить и категорировать. Это возможно осуществлять итеративно при работе со спецификацией требований.

5.4 Проектирование общей архитектуры систем контроля и управления и назначение функций систем контроля и управления

5.4.1 Общие положения

Данный подраздел описывает:

- применение ограничений по 5.2.4 и требования по 5.3 к проектированию общей архитектуры СКУ, важных для безопасности (кратко — «архитектура СКУ»);
- назначение отдельной СКУ функции СКУ.

5.4.2 Проектирование архитектуры СКУ

5.4.2.1 Общие положения

Проект архитектуры СКУ обеспечивает верхнеуровневое определение СКУ АС, связи между этими системами и инструментальные средства, необходимые для обеспечения согласованного интерфейса между этими системами.

5.4.2.2 Общие требования:

a) проект архитектуры СКУ должен охватывать все СКУ, необходимые для реализации функций СКУ, важных для безопасности, определенных в 5.3;

b) проект архитектуры СКУ должен декомпозировать всю СКУ на соответствующие системы и оборудование, чтобы соответствовать требованиям:

- по независимости функций на различных уровнях защиты;
- соответствующему разделению систем различных классов;
- выполнению ограничений по физическому разделению и электрической изоляции в соответствии с ограничениями окружающей среды и компоновочными ограничениями, анализом опасностей, а также с ограничениями, связанными с работами по пуску-наладке, испытаниями, техническим обслуживанием и эксплуатацией (см. 5.2.4);

c) проект архитектуры СКУ должен обеспечивать достаточное разделение систем и подсистем так, чтобы принцип единичного отказа выполнялся для функций категории А во всех допустимых конфигурациях систем и станции (см. 4.17 — 4.21 МАГАТЭ NS-G-1.3:2002);

d) каждая СКУ должна быть классифицирована в соответствии с ее пригодностью выполнять функции СКУ в соответствии с определенной категорией;

Таблица 2 — Соотношение между классами СКУ и категориями функций СКУ

Категории функций контроля и управления, важных для безопасности			Соответствующий класс СКУ, важных для безопасности
A	(B)	(C)	1
	B	(C)	2
		C	3
Примечание — Особый случай рассмотрен в 7.3.2.1 МЭК 61226:2009.			

e) интерфейсы со станцией и взаимосвязи между СКУ должны быть указаны как часть проекта архитектуры с целью определения:

- совместного использования сигналов (измерений) по различным функциям, важным для безопасности;
- мажоритарной логики и приоритета между исполнительными сигналами от различных систем;
- путей прохождения сигналов и оборудования, которые являются общими для выполнения автоматического или ручного приведения в действие функций на различных линиях защиты;

f) описание систем, оборудования и их взаимодействия в проектной архитектуре СКУ должно быть достаточно подробным, чтобы выполнить анализ вопросов безопасности СКУ.

5.4.2.3 Человеко-машинные интерфейсы:

a) проект архитектуры СКУ должен структурировать системы ЧМИ разных помещений станции, предназначенных для управления и контроля, включая блочный пункт управления, дополнительные пункты управления, местные пульты управления и противоаварийный пункт управления, с такой степенью резервирования и удобства пользования, чтобы были учтены ограничения, накладываемые эксплуатацией и техническим обслуживанием станции (см. 5.2.4);

b) проект архитектуры СКУ должен соответствовать принципам эксплуатации станции, установленным в проектных основах станции (см. 5.2.2), включая:

- принципы приоритетности между автоматическими сигналами и сигналами управления, инициируемыми вручную;
- принципы приоритетности между различными системами ЧМИ при нормальной, аварийной и послеаварийной эксплуатациях;
- принципы приоритетности между основными и резервными системами ЧМИ;
- принципы условий переключения между основными и резервными системами ЧМИ;

c) проект архитектуры должен определять, каким образом информация о дефектах и отказах, обнаруживаемая оборудованием диагностики отдельных систем, предоставляется оператору станции. Форма представления должна быть такой, чтобы оператор мог:

- немедленно по индикации опознавать отказ и отличать его от других отображаемых эксплуатационных данных;
- решить, следует ли применить ручное управление для перевода станции в безопасное состояние;
- обозначить обслуживающему персоналу системы, работа которых вызывает сомнения.

Примечание 1 — Под ручными управляющими воздействиями понимается использование элементов управления и дисплеев для получения информации. Прямое вмешательство в оборудование СКУ, например путем установления имитации на разъемах или отсоединения проводов, не подразумевается;

d) должна быть продемонстрирована согласованность проекта архитектуры СКУ с основными решениями, касающимися технологии систем ЧМИ (например, компьютеризированная или традиционная). Для представления информации операторам следует применять более сложные системы, если это снижает влияние человеческого фактора на возникновение отказа и если это влияние можно умень-

шить благодаря получению более полной информации. Возможность ООП компьютеризированных информационных систем следует рассматривать с учетом возможности отказов вследствие влияния человеческих факторов,

e) проект архитектуры СКУ должен:

- назначить функции ручного или автоматического управления в соответствии с анализом задачи проектных основ станции (см. 5.2.2);
- определить техническую возможность СКУ, необходимую для обработки информации и выполнения задач, определенных для взаимодействия с оператором (см. 6.3.3 МЭК 60964:2009);
- гарантировать, что информация по характеристикам ЧМИ и времени, имеющаяся у оператора для выполнения ручного управления, согласуется с требованиями проектных основ станции (см. 5.2.2);

f) для обеспечения эффективности ЧМИ в проекте блочного пункта управления и других пунктов управления станции должна быть учтена методология учета человеческого фактора, основанная на МЭК 60964 и МЭК 60965.

Примечание 2 — Первоначально для анализа человеческого фактора должны быть рассмотрены соответствующие задачи оператора и их эксплуатационные требования, которые приводят к надлежащей интеграции дисплеев и органов управления, особенно задачи, которые будут выполняться часто, в режиме цейтнота или с повышенным риском в случае человеческой ошибки;

g) при анализе проекта должны быть приняты во внимание задачи оператора и оптимизация требований ЧМИ при выполнении как важных для безопасности, так и не влияющих на безопасность задач.

5.4.2.4 Передача данных

Передача данных между системами, образующими архитектуру СКУ, включает все связи, обеспечивающие передачу одного или более сигналов или сообщений по одному или более путям с использованием последовательной передачи данных.

a) Линии связи должны удовлетворять общим спецификациям эксплуатационных требований (см. 5.3) при всех требуемых состояниях станции.

b) Архитектура и технология линий связи должны гарантировать, что выполняются требования по независимости между системами. При этом дополнительно к физическому разделению и электрической изоляции в проекте должны быть предусмотрены средства, обеспечивающие, что отказы и нарушения в линиях связи не влияют на результаты работы модулей обработки сигналов с точки зрения безопасности.

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

d) Для смягчения последствий отказов следует предусматривать резервирование линий связи.

e) Линии связи должны быть спроектированы так, чтобы передача данных и выполнение функции более высокой категории безопасности не нарушались при передаче данных систем более низкого класса.

Подробнее см. МЭК 61500 и МЭК 60709.

5.4.2.5 Инструментальные средства

a) Проект архитектуры СКУ должен включать инструментальные средства, обычно на базе компьютеров (см. раздел 14 МЭК 60880:2006 и 5.1.4, 6.1.4 МЭК 62138:2004), которые необходимы для обеспечения соответствия данных при обмене между СКУ, работающими совместно, и гарантировали бы согласованность данных с базой данных АС.

Примечание — Инструментальные средства, специфичные для отдельных систем, определяются на этапе спецификации системы (см. 6.2.3.2).

b) Инструментальные средства следует использовать на всех этапах общего жизненного цикла СКУ, если могут быть достигнуты улучшение качества и надежность функций, важных для безопасности, например для поддержки:

- всех аспектов, связанных с проектированием интерфейсов между СКУ;
- общей интеграции и ввода в эксплуатацию распределенных функций.

c) Инструментальные средства должны быть выбраны и методы для достижения должного качества вывода должны быть определены в соответствии с требованиями МЭК 60880 (для 1-го класса систем) и МЭК 62138 (для 2-го и 3-го классов систем) соответственно.

5.4.2.6 Защита от ООП

СКУ с резервированной архитектурой могут отказать, если в двух или более резервных каналах одновременно произойдет отказ (ООП) (т. е. при запросе мажоритарная логика голосования резервных каналов не будет выполняться). Такая ситуация может произойти, если один или более скрытых дефектов существуют в некоторых или во всех резервных каналах на постоянной основе и если существует механизм, который может инициировать такой существующий скрытый дефект в двух или более резервированных каналах так, что они откажут одновременно (см. МЭК 62340).

Происхождение системных скрытых дефектов в основном связано с человеческими ошибками. Они могут быть внесены на любом этапе жизненного цикла СКУ. Применение компьютеров позволяет использовать более сложные алгоритмы и процессы, чем было это возможно ранее только с аппаратным обеспечением. Более того, трудоемкость проектирования СКУ на основе компьютеров, в том числе деятельности, связанной с проектированием лежащей в основе платформы СКУ, выше для аппаратных СКУ, и сам проект может быть более сложным.

Варианты проекта следует оценивать с целью минимизации сложных решений, которых возможно избежать.

Защита СКУ от ООП включает следующие уровни:

a) функциональную валидацию спецификации требований к прикладным функциям следует выполнять для систем класса 1 (см. 6.2.4.2.1) с целью снижения вероятности скрытых дефектов в спецификации требований;

b) четко структурированный инжиниринговый процесс должен выполняться с высоким вниманием ко всем работам по верификации и валидации, для того чтобы уменьшить вероятность скрытых дефектов в проекте. Объем трудозатрат следует дифференцировать по классам систем 1, 2 и 3;

c) СКУ класса безопасности 1 и их обеспечивающие системы следует проектировать так, чтобы они работали независимо от влияющих факторов производственных процессов станции, чтобы минимизировать возможность проявления потенциально скрытых дефектов (например: компоненты аппаратного обеспечения, предназначенные для смягчения ПИС, не должны подвергаться воздействию неблагоприятных условий окружающей среды, вытекающих из этого ПИС; порядок выполнения программного обеспечения не должен зависеть от сигналов станции).

Примечание 1 — Эта рекомендация соответствует требованию МЭК 62340, что СКУ следует работать независимо от «режима работы станции»;

d) для СКУ класса безопасности 1 должен быть выполнен анализ по выявлению возможных источников ООП и механизмов, которые могут вызвать постулируемые в проекте скрытые дефекты, приводящие к отказу. В рамках этого анализа особое внимание следует уделять линиям связи и механизмам передачи данных и компонентам, работающим в режиме срабатывания на требование. Возможные состояния отказа и последствия отказа таких компонентов следует оценивать с учетом возможных источников и эффектов ООП. В анализ следует также включать такие системы из рассматриваемой группы безопасности, которые предназначены для смягчения воздействий постулированного ООП систем класса 1.

Проект для преодоления ООП необходим, если постулируемый отказ важных для безопасности функций приводит к неприемлемым последствиям[1)]. Это является общим случаем для функций категории А и для подмножества функций категории В (см. 5.3.2 и 5.3.3 МЭК 61226:2009);

e) в проекте архитектуры СКУ следует использовать принцип разнообразия, где требуется высокая надежность для группы безопасности, и, следовательно, должны быть рассмотрены причины и эффекты ООП. Следует рассматривать функциональное, сигнальное и аппаратное разнообразие. Если разнообразие используется при защите от ООП, проект должен включать анализ эффективности разнообразных мер, предназначенных для минимизации возможности ООП;

f) системы класса 1 и более низких классов, заявленные в детерминистическом обосновании безопасности как разные уровни глубокоэшелонированной защиты от проектных аварий, должны быть независимыми. СКУ выполняют свои функции безопасности независимо, если постулируемый отказ одной из этих систем не мешает другим системам выполнять свои функции как предусмотрено. Независимые СКУ должны эксплуатироваться на различных сигнальных траекториях. Это может быть обеспечено разнообразием (например, разнообразие оборудования или функциональное разнообразие).

[1)] *Элементы СКУ, классифицируемые по НП-001-15 в зависимости от степени влияния отказов этих элементов на безопасность, определяются в проектах АС, как правило, как элементы классов 2, 3 или 4.*

Дополнительные требования в отношении мер по преодолению ООП в системах, выполняющих функции категории А, приведены в МЭК 62340.

Примечание 2 — На уровне анализа безопасности станции следует осуществить деятельность для верификации того, что проектные меры по обработке/устранению отказов СКУ будут осуществляться определенными функциями категории A/B/C. Эта деятельность затрагивает не только СКУ, но и уровень анализа безопасности всей станции и поэтому выходит за рамки настоящего стандарта.

5.4.3 Назначение функций системам

В процессе функционального назначения распределяют общие требования к функциям СКУ, важным для безопасности, определенным в 5.3, по отдельным системам архитектуры СКУ. При необходимости функции могут быть разложены на несколько подфункций, распределенных по нескольким системам. Все функции или подфункции называют прикладными функциями СКУ (см. 6.2.2.2).

a) Спецификация функциональных и эксплуатационных требований к прикладным функциям должна охватывать общие требованиях к функциям СКУ. Если функция распределена по более чем одной СКУ, то взаимосвязанные системы должны быть выстроены так, чтобы они удовлетворяли общим требованиям, определенным в 5.3.

Примечание 1 — Это включает в себя оценку достижения определенных вероятностных целей.

b) Спецификация функциональных и эксплуатационных требований к прикладным функциям должна включать все сопутствующие валидации, блокировки и функции мониторинга, которые были идентифицированы при проектировании архитектуры СКУ, например состояние и режим работы взаимосвязанных систем, валидация сигналов, полученных от других систем.

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

d) Функции категории А должны быть назначены системам, которые соответствуют критерию единичного отказа.

Примечание 2 — В соответствии с МАГАТЭ SSR-2/1 (Rev.1) именно группа безопасности должна удовлетворять критерию единичного отказа, а не отдельные системы сами по себе.

e) При назначении функций категории А системам одной группы безопасности должны приниматься во внимание меры защиты от ООП в соответствии с 5.4.2.6. Примеры назначения функций различных категорий приведены на рисунке С.1.

f) При назначении прикладных функций системам сложность систем класса 1 должна по возможности быть минимизирована.

Примечание 3 — Это применимо в особенности для новых станций. В случае замены аппаратно-реализованных систем на компьютеризированные системы одни и те же требования, как правило, назначаются прикладным функциям компьютерных систем аналогично предыдущим аппаратно-реализованным системам.

Примечание 4 — Сложность системы может быть уменьшена за счет проектных подходов, таких как:

- избежание сложных алгоритмов и обработки, которые не могут быть четко определены и валидированы;
- сокращение числа различных функций, реализованных в системе;
- использование простых проектных решений для ограничения возможных условий возникновения сложных дефектов.

Тем не менее любое уменьшение сложности не должно приводить к чрезмерным отрицательным воздействиям на проект, таким как увеличение сложности общей архитектуры СКУ или снижение функциональности, связанной с безопасностью, например объем самодиагностики.

g) Требуемая надежность каждой прикладной функции, реализованной в системах, должна быть на уровне достижимых пределов, включая ООП.

Примечание 5 — Оценка пределов может зависеть от рекомендаций стандартов, предварительно проведенных анализов, оценки предыдущего опыта лицензирования и оценок рисков при лицензировании.

h) Записи, полученные от процесса назначения функций системам, должны четко определять, какие системы выполняют какие функции, т. е. должна быть предусмотрена прослеживаемость.

5.4.4 Необходимый анализ

5.4.4.1 Общие положения

Анализ необходим для верификации проекта архитектуры СКУ и назначения функций по СКУ. Такой анализ представляет собой итеративный процесс и выполняется вместе с процессом проектирования (см. раздел 6).

5.4.4.2 Оценка надежности и защиты от ООП

a) Следует выполнять оценку надежности СКУ, важных для безопасности. Оценку следует проводить с учетом в зависимости от обеспечивающих систем, таких как электрические и пневматические, источники питания, установки отопления и вентиляции.

b) Первоначальная оценка может быть основана на оценке надежности, достижимой для функций различных систем системы, в дальнейшем оценку следует верифицировать после завершения процесса проектирования на основе оценки надежности отдельных систем (см. 6.2.4.2.2).

c) Оценка уязвимости от ООП групп безопасности, выполняющих функций категории А, должна быть выполнена таким образом, чтобы оценить эффективность мер защиты от ООП и определить потенциально слабые места общей архитектуры.

d) Проектная документация на системы (см. 6.4.4) должна быть проанализирована с целью определить общие или идентичные компоненты аппаратного или программного обеспечения, которые поддерживают различные функции группы безопасности, включая функции категории А. Если общие или идентичные элементы будут найдены на различных уровнях защиты, то обоснование должно показать, что вероятность ООП является достаточно низкой, согласуется с задачей по безопасности на этих уровнях.

e) Не существует общепринятого метода количественной оценки вероятности ООП, поэтому применяемые методы преимущественно качественные (см. приложение С). Методы, которые будут использоваться, следует определить в начале проекта.

Примечание 1 — Одной из целей вышеупомянутых рекомендаций и требований является исключение необходимости внесения изменений на поздних этапах планирования и проектирования системы в ответ на изменения в требованиях, которые в дальнейшем могут привести к возникновению ООП вследствие ошибок из-за этих изменений.

Примечание 2 — Уровень детального анализа ООП может зависеть от категории функций, поддерживаемых системами, и будет обоснован.

Примечание 3 — Требования к анализу ООП для системы класса 1, связанного с программным обеспечением, приведены в 13.3 МЭК 60880:2006.

5.4.4.3 Оценка человеческого фактора

Для оптимизации проекта систем ЧМИ в верификацию проекта архитектуры следует включать анализ требований, связанных с влиянием человеческого фактора.

5.5 Общее планирование

5.5.1 Общие положения

Данный пункт устанавливает требования к разработке общих планов, которые обеспечивают соблюдение требований общего жизненного цикла СКУ ко всем отдельным СКУ, а также которые гарантируют, что требования к функциям СКУ, важным для безопасности, распределенным среди СКУ, будут достигнуты и поддержаны в течение жизненного цикла систем.

Требования настоящего раздела согласуются и дополняют планы, рассмотренные в 6.3, для отдельных СКУ.

Примечание — Следующие требования к планам не исключают того, что планы могут быть выполнены в виде различного числа документов.

Общие планы должны быть разработаны, прежде чем начнется предусмотренная в них деятельность.

5.5.2 Разработка программы обеспечения качества СКУ

Настоящий стандарт предполагает, что программа обеспечения качества или, что более предпочтительно, интегрированная система менеджмента, соответствующая требованиям МАГАТЭ GSR, часть 2, и МАГАТЭ GS-G-3.1, существует как неотъемлемая часть проекта АС и что она обеспечивает контроль соответствующей деятельности.

a) Программы обеспечения качества должны разрабатываться и реализоваться для каждой деятельности, связанной с общим жизненным циклом безопасности СКУ.

b) Программы обеспечения качества должны включать всю деятельность, которая необходима для достижения качества, а также деятельность, которая верифицирует, что требуемое качество было достигнуто.

c) Деятельности по верификации должны быть определены в планах верификации. Планы верификации включают ресурсы, процесс и результаты на каждом этапе общего жизненного цикла СКУ и определяют:

- процедуры и инструментальные средства для деятельности по верификации;
- записи, которые должны храниться и верифицироваться;
- важные для безопасности аспекты, которые необходимо верифицировать;
- процедуры по устранению отказов и несоответствий;
- критерии, определяющие завершение каждого этапа;
- разрабатываемые финальные отчеты, демонстрирующие соответствие результатов этапа исходным требованиям и устранение аномалий.

d) Программы обеспечения качества следует планировать и включать в общую программу обеспечения качества проекта АС, а входящие в них деятельности следует включать в общий план-график деятельности по проекту АС.

5.5.3 Общий план защищенности

Меры защиты необходимы для защиты обрабатываемой в системах, важных для безопасности, информации от несанкционированных изменений, включая несанкционированные управляющие действия (целостность), нарушение доступа (доступности) и несанкционированное раскрытие (конфиденциальность).

Примечание 1 — В СКУ АС требования к целостности и доступности превалируют над требованиями к конфиденциальности.

Программное обеспечение (программные коды, а также параметры и данные) может быть особенно уязвимым в процессах проектирования и технического обслуживания. Угрозы, которые необходимо учитывать, включают умышленные вредоносные изменения, которые приводят к ошибочной работе программного обеспечения в целом или к сбоям, возникающим в определенное время, или к ограничению доступа к данным.

Примечание 2 — Угрозы, возникающие в связи с непреднамеренными изменениями, рассматриваются в спецификации системных требований (см. 6.2.2.5).

Общий план защищенности содержит организационные мероприятия и технические меры, которые необходимо предпринять, чтобы защитить архитектуру СКУ от преднамеренных и спланированных атак, которые могут поставить под угрозу выполнение функций, важных для безопасности. Положения плана информационной защиты СКУ могут иметь различные требования для систем классов 1, 2 и 3.

a) Требования к защищенности функций и систем, важных для безопасности, должны быть определены в плане защищенности системы (см. 6.3.3).

b) Риск, возникающий от несанкционированного доступа и модификации информации, должен систематически управляться на всех этапах жизненного цикла от начальной стадии до вывода из эксплуатации. Это включает системы разработки и инжиниринга, а также СКУ, которые будут установлены на станции. Должны быть рассмотрены физический и удаленный доступы.

c) Меры по обеспечению защищенности системы должны быть такими, чтобы они не имели значительного влияния на надежность или доступность.

d) Для поддержки защищенности систем на постоянно высоком уровне должна быть определена специальная для объекта эксплуатации политика защищенности. Она должна содержать процедуры, связанные с интерфейсом между административной и технической защищенностью, доступ к системам, аспекты защищенности обработки данных, аспекты защищенности модификации и технического обслуживания, аудит и отчетность по защищенности и обучение защищенности.

e) Системы, выполняющие функции, важные для безопасности, должны быть физически защищены от несанкционированного доступа (см. 4.51 МАГАТЭ NS-G-1.3:2002). Контроль доступа должен включать идентификацию и аутентификацию персонала для систем, выполняющих функции категории А, и надежную идентификацию персонала для систем, выполняющих функции категорий В и С.

f) Средства удаленного доступа (внешние по отношению к станции) не должны применяться для систем, выполняющих функции категорий А и В, и их не следует применять для систем, выполняющих функции категории С. Если средства удаленного доступа через линии передачи данных предусмотрены (внутренние или внешние по отношению к станции), то они должны быть проанализированы и необходимо продемонстрировать, что это не приводит к появлению недопустимого риска несанкционированного доступа к системе или недопустимого риска отказа системы.

Примечание 3 — Предотвращение доступа не исключает отправку данных из системы.

g) Доступ к системам (включая попытки доступа) следует регистрировать. Это подразумевает запись персонала, тип доступа, время и выполненные действия.

h) Журналы безопасности должны формально инспектироваться через определенные промежутки времени для систем, выполняющих функции категории А, и их следует периодически проверять в случае систем, выполняющих функции категорий В и С.

5.5.4 Общая интеграция и ввод в эксплуатацию СКУ

5.5.4.1 Общие положения

Общая интеграция СКУ является совокупностью всех технических и административных действий, позволяющей осуществлять монтаж на объекте, соединение, испытания, калибровку и подготовку к эксплуатации СКУ.

Общий ввод в эксплуатацию является совокупностью всех технических и административных действий, связанных с необходимостью дать гарантию, что установленные системы и станция являются пригодными для эксплуатации до начала их работы (см. 4.4 МАГАТЭ 75-INSAG-3:1999).

Примечание 1 — Общий ввод в эксплуатацию СКУ является частью ввода в эксплуатацию станции и включает все системы станции, а не только СКУ (см. 3.7).

Процессы общей интеграции и общего ввода в эксплуатацию завершаются валидацией и установкой отдельных систем (см. 6.2.6 и 6.2.7). При этом применяют следующие требования:

a) после интеграции СКУ на объекте общие функциональные и эксплуатационные спецификации функций СКУ, важные для безопасности, распределенные между системами, должны быть валидированы для всех установленных режимов работы станции;

b) объем деятельности по интеграции и вводу в эксплуатацию, который будет выполняться в целом, может быть определен с учетом объема испытаний на других фазах проекта, например: испытания функций и интеграции, выполняемые на площадке или производстве, или испытания, выполненные на аналогичных станциях, если АС не абсолютно новая. Такие сокращения объема общих верификации и валидации должны быть обоснованы и задокументированы.

Примечание 2 — Минимизация количества испытаний интегрированной СКУ на площадке за счет выполнения значительной части интеграционного тестирования на производстве является хорошей практикой. Общую стратегию по распределению требуемых испытаний к различным внешним условиям (тестирование с использованием симуляции или эмуляции, интеграционное тестирование на производстве, испытания на площадке) следует разрабатывать на ранней стадии проекта, см., например, 7.18 МАГАТЭ NS-G-1.3:2002.

Как правило, эти испытания являются частью процесса приемки СКУ владельцем станции. МЭК 62381 [11] представляет практические рекомендации по реализации и документированию заводских приемочных испытаний (FAT), приемочных испытаний на площадке (SAT) и интеграционных испытаний на площадке (SIT).

5.5.4.2 Общий план интеграции СКУ

Общий план интеграции СКУ должен быть разработан в рамках программы обеспечения качества. В дополнение к общим требованиям 5.5.2 по обеспечению качества и верификации применимы следующие требования:

a) испытания взаимосвязанных систем следует проводить для подтверждения того, что:

- все интерфейсы взаимосвязанных систем работают правильно;
- выявление отказов, корректирующие действия и представление соответствующих данных осуществляются в соответствии со спецификацией требований к функциям СКУ;

b) верификацию защищенности от электромагнитных помех взаимосвязанных систем следует проводить в соответствии с требованиями МЭК 61000-4-1—МЭК 61000-4-6.

Примечание — Для верификации защищенности, как правило, необходимы два измерения (например, воссоздание условий на площадке), испытания (например, подсистем) и анализ. Другие части серии стандартов МЭК 61000-4 предоставляют руководство по измерениям и испытаниям;

c) необходимо верифицировать, что заземление и эквипотенциальные соединения всего оборудования и экранов кабелей выполнены правильно;

d) если требуется, должны быть проведены испытания отклика систем при потере и восстановлении внешнего энергоснабжения и перепадах напряжения для верификации поведения и доступности систем в случае прерывания и восстановления энергоснабжения;

e) условия окружающей среды по месту размещения СКУ должны быть верифицированы на соответствие;

f) аналоговые и логические сигналы обмена между системами должны быть испытаны для демонстрации того, что различным функциям, важным для безопасности, передаются корректные значения сигналов и состояний. Если функции отображения информации, сигнализации, записи и выполнения расчетов выполняются системой, не влияющей на безопасность, то такие испытания следует проводить совместно с такой системой, если невозможно предложить более простой способ проверки правильности передачи всех данных;

g) функции контуров управления и функции логического управления должны быть испытаны от входа до выхода, включая исполнительные устройства, интерфейсы оператора и передачу управления (например, ручное/автоматическое);

h) испытания должны подтверждать, что правильная информация поступает в каждую систему в случае отказа резервного оборудования, линий связи, датчиков или исполнительных устройств. Испытаниями следует подтверждать, что переключение режима управления и временной интервал являются корректными;

i) связи передачи данных должны быть проверены на правильную передачу данных и приемлемое время отклика, от выдачи команд до получения подтверждения правильности индикации состояния устройства управления. Испытания следует проводить при имитации нормальных условий эксплуатации, нарушений нормальных условий эксплуатации, наихудших возможных условий в условиях имитации наличия отказов аппаратного обеспечения.

5.5.4.3 Общий план ввода в эксплуатацию

Общий план для завершения валидации СКУ должен быть разработан в рамках программы ввода в эксплуатацию систем станции (см. 4.4.253 МАГАТЭ 75-INSAG-3:1999). Следующие требования, связанные со спецификой СКУ, включают в общую программу ввода станции в эксплуатацию:

a) установка заданных значений, пороговых значений, параметров и значений калибровочных величин приборов должна быть верифицирована и скорректирована при вводе в эксплуатацию систем станции, чтобы подтвердить, что функциональность и работа систем соответствуют общей спецификации требований;

b) процедуры эксплуатации и испытаний СКУ должны верифицироваться и обновляться при вводе станции в эксплуатацию.

5.5.5 Общий план эксплуатации

Общий план эксплуатации описывает эксплуатацию взаимосвязанных СКУ. Общий план эксплуатации дополняет планы эксплуатации отдельных СКУ (см. 6.3.7).

Общий план эксплуатации должен разрабатываться в рамках программы обеспечения качества. В дополнение к общим требованиям 5.5.2 по обеспечению качества и верификации применяют следующие требования:

a) документация должна описывать:

- средства запуска, инициализации и поддержания взаимосвязанных систем в полностью рабочем состоянии;
- средства верификации готовности систем к выполнению функций, важных для безопасности;
- регламентные операции, например периодические испытания, которые необходимо выполнять при эксплуатации станции для поддержания требуемой надежности функций, важных для безопасности;

b) план должен определять условия, при которых может выполняться модификация системных параметров или управляющих воздействий, и влияние таких модификаций на работу систем, на эксплуатацию и безопасность станции. В документации должно быть указано, какие модификации могут быть выполнены:

- только под административным контролем;
- под административным контролем и после согласования с проектировщиком при соответствующих испытаниях и верификациях.

Примечание — Процесс модификаций и уполномоченные органы, которые дают разрешения на проведение модификаций, могут зависеть от эксплуатирующей организации и национального законодательства;

c) план должен определять все режимы эксплуатации взаимосвязанных систем и устанавливать, как системы должны эксплуатироваться в каждом из рассматриваемых режимов, включая:

- действия, которые необходимо предпринять, и ограничения к эксплуатации систем и станции в случае отказа системы или внешнего непредвиденного воздействия на системы;

- ограничения эксплуатации систем и станции при проведении периодических испытаний, технического обслуживании и/или внесения модификаций;

- процедуры возврата к нормальной эксплуатации и процедуры подтверждения, что нормальная эксплуатация достигнута, когда вышеуказанные ограничения могут быть сняты.

5.5.6 Общий план технического обслуживания

Общий план технического обслуживания описывает обслуживание на уровне взаимосвязанных СКУ. Он дополняет и координирует планы технического обслуживания отдельных СКУ (см. 6.3.8).

Общий план технического обслуживания должен быть разработан в рамках программы обеспечения качества. В дополнение к общим требованиям, указанным в 5.5.2 по обеспечению качества и верификации, применяют следующие требования:

a) на деятельность по техническому обслуживанию отдельных СКУ должны быть наложены ограничения так, чтобы любое воздействие на безопасность станции было приемлемым. В частности, если требуется, системы должны продолжать соответствовать критерию единичного отказа в период технического обслуживания. План должен определять, какое оборудование может быть выведено из эксплуатации, последовательность его вывода, последствия вывода, а также средства корректного возвращения оборудования в эксплуатацию и верификации его корректности;

b) должен быть реализован системный подход к испытаниям и замене, чтобы ООП был маловероятным в тех местах архитектуры СКУ, которые подвергаются воздействию измененных условий окружающей среды в случае аварии. Таким подходом следует обеспечить, чтобы те части системы, которые подвергаются воздействию облучения и связанному с ним ускоренному старению или изменению физических свойств (кабели, датчики) или чья нагрузка изменяется в ответ на воздействие (например, переключение усилителей мощности, реле), заменялись до проявления недопустимого ухудшения их способности выполнять функции безопасности.

Примечание 1 — Интервалы замены могут быть определены по результатам ускоренного старения образца оборудования.

Примечание 2 — См. МЭК 62342 [12] для руководства по управлению старением;

c) если деятельность по техническому обслуживанию включает настройку конфигурации или данных калибровки, то для нее должны быть разработаны документированные процедуры, которые должны обеспечивать:

- эксплуатационную регулировку в установленных пределах (такие пределы могут устанавливаться проектом системы или проектными основами станции, в этом случае никакие формальные ограничения не должны накладываться на действия обслуживающего персонала);

- применение требований 5.5.5, если такие регулировки выполняются, когда система находится в эксплуатации;

- сохранение записи обо всех выполненных регулировках.

5.5.7 Планирование обучения

5.5.7.1 Программа обучения

В данном пункте рассматривают требования, связанные с обучением персонала станции, работающего с СКУ.

a) Программа обучения для эксплуатирующего и обслуживающего персонала должна быть разработана для операторов станции и специалистов по контролю и управлению.

Примечание — Обучение операторов станции будет сосредоточено на интерфейсах оператора с основами технологии СКУ, технического обслуживания и аспектов диагностики, тогда как обучение персонала по СКУ в соответствии с их задачами будет сосредоточено на диагностике при техническом обслуживании и модификациях.

b) Программу обучения следует разрабатывать на основе систематического подхода, который включает:

1) анализ задач категорий участвующего персонала и установление целей обучения, общий график и общее назначение учебных курсов;

2) наличие компетентных преподавателей и учебного материала для преподавателей и учащихся;

3) оценку проведенного обучения;

4) расширенное использование обратной связи для улучшения обучения.

c) Обучение оператора должно быть нацелено на эксплуатацию станции при нормальных условиях и при отклонениях от нормальных условий с использованием всех соответствующих устройств интерфейса оператора и функций СКУ.

d) Специальное обучение по распознаванию отказов аппаратных средств и аномалий программного обеспечения следует также включать в программу.

5.5.7.2 Пользовательская документация

a) Пользовательская документация СКУ должна быть предоставлена операторам и обслуживающему персоналу.

b) В пользовательской документации следует определить каждое устройство интерфейса оператора. Каждая функция каждого устройства должна быть объяснена и проиллюстрирована в соответствии с ее сложностью.

c) Обучение должно предоставить операторам и обслуживающему персоналу возможность познакомиться с пользовательской документацией, важной для выполнения их задач.

5.5.7.3 Тренажерные системы

В дополнение к занятиям в классе, обучение следует основывать на использовании тренажерных систем. Для обучения оператора следует использовать полномасштабные и целевые тренажеры.

a) Обучение оператора и обслуживающего персонала следует проводить на тренажерных системах, чьи характеристики полностью соответствуют характеристикам рабочих систем и оборудования. Ограничения в возможностях и в использовании тренажерных систем должны быть известны и задокументированы.

b) Тренажеры для обучения операторов должны обеспечивать реальные интерфейсы пункта управления и иметь возможность моделировать поведение станции в реальном времени, включая СКУ. Тренажер должен быть способен моделировать нормальные условия реактора и условия с отклонениями от нормальных, включая комбинацию отказов и отклонений оборудования.

5.6 Выходная документация

5.6.1 Общие положения

Выходная документация проекта архитектуры СКУ и процесс функционального назначения являются источниками необходимых исходных данных для спецификации требований к отдельным системам архитектуры СКУ (см. 6.2.2).

5.6.2 Документация по проекту архитектуры

a) Выходная документация должна определять для отдельных СКУ:

- ограничения проекта, основанные на границах проекта станции (см. 5.2.4);
- ограничения проекта из проекта архитектуры (см. 5.4.2);
- физические и функциональные границы между системами.

b) Используемые инструменты инжиниринга следует документировать, описывая, каким образом каждое инструментальное средство используется для поддержки деятельности по проектированию жизненного цикла системы.

Примечание — Требования к методам инжиниринга программного обеспечения и инструментальным средствам для систем класса 1 приведены в разделах 7, 14 и 15 МЭК 60880:2006 и в 5.1.1, 6.1.1 МЭК 62138:2004 для систем классов 2 и 3.

5.6.3 Документация по назначению функций

a) Выходная документация должна определять функциональные, эксплуатационные требования и требования к надежности выполнения прикладных функций (см. 5.4.3), назначенных каждой системе. Требования могут быть задокументированы в виде текста, блок-схем, матриц, структурных схем и пр., обеспечивая ясное представление о функциях.

b) Спецификацию требований к прикладным функциям следует определять максимально независимо от применяемой для реализации технологии, например компьютеры, реле.

c) Основными пользователями документов по требованиям являются разработчики спецификаций системных требований к отдельным СКУ и операторы станции. Программные методы и средства, а также методы и средства системной разработки следует выбирать в соответствии с ролями персонала.

6 Жизненный цикл системы безопасности

6.1 Общие положения

Проект архитектуры СКУ определяет отдельные СКУ, которые реализуют функции, важные для безопасности (см. 5.4.2). Настоящий раздел устанавливает цели и требования для таких систем. Требования раздела относятся к компьютеризированным системам.

Примечание — Большая часть этих требований может применяться и к СКУ, не основанным на применении компьютерной технологии.

Для обеспечения того, что все связанные с безопасностью требования, которым должна соответствовать система, учтены, реализованы и поддерживаются, необходим системный подход. Это достигается за счет ведения деятельности, связанной с разработкой, реализацией и эксплуатацией системы в рамках жизненного цикла безопасности системы. Этот жизненный цикл, в свою очередь, ссылается на деятельность общего жизненного цикла безопасности СКУ (см. раздел 5 и рисунок 4). Этапы типового жизненного цикла безопасности системы включают:

- спецификацию требований к системе;
- спецификацию системы;
- детальные проект и реализацию системы;
- интеграцию системы;
- валидацию системы;
- монтаж системы;
- модификацию проекта системы (при наличии).

Квалификацию системы рассматривают отдельно, поскольку ее можно выполнить частично независимо от жизненного цикла безопасности системы. Этот подход учитывает современную практику, которая все больше основывается на применении уже существующего оборудования.

На рисунке 5 приведен типовой жизненный цикл системы и показаны связи с жизненными циклами программного обеспечения и аппаратного обеспечения в соответствии с МЭК 60880, МЭК 62138 и МЭК 60987.

В таблице 3 приведен обзор целей, входов и выходов для деятельности в рамках типового жизненного цикла системы и приведены ссылки на соответствующие подразделы.

Настоящий раздел включает:

- общие требования, одинаково предъявляемые ко всем системам, важным для безопасности;
- требования, предъявляемые в дополнение к предыдущим, к определенным классам систем или категориям функций.

Жизненный цикл системы — это итеративный процесс. Этап может начинаться, прежде чем деятельность в рамках предыдущего этапа завершится; однако этап должен считаться завершенным, только если предыдущие этапы завершены и если его выходы согласуются со входами, полученными в рамках предыдущих деятельностей.

Таблица 3 — Обзор жизненного цикла безопасности системы

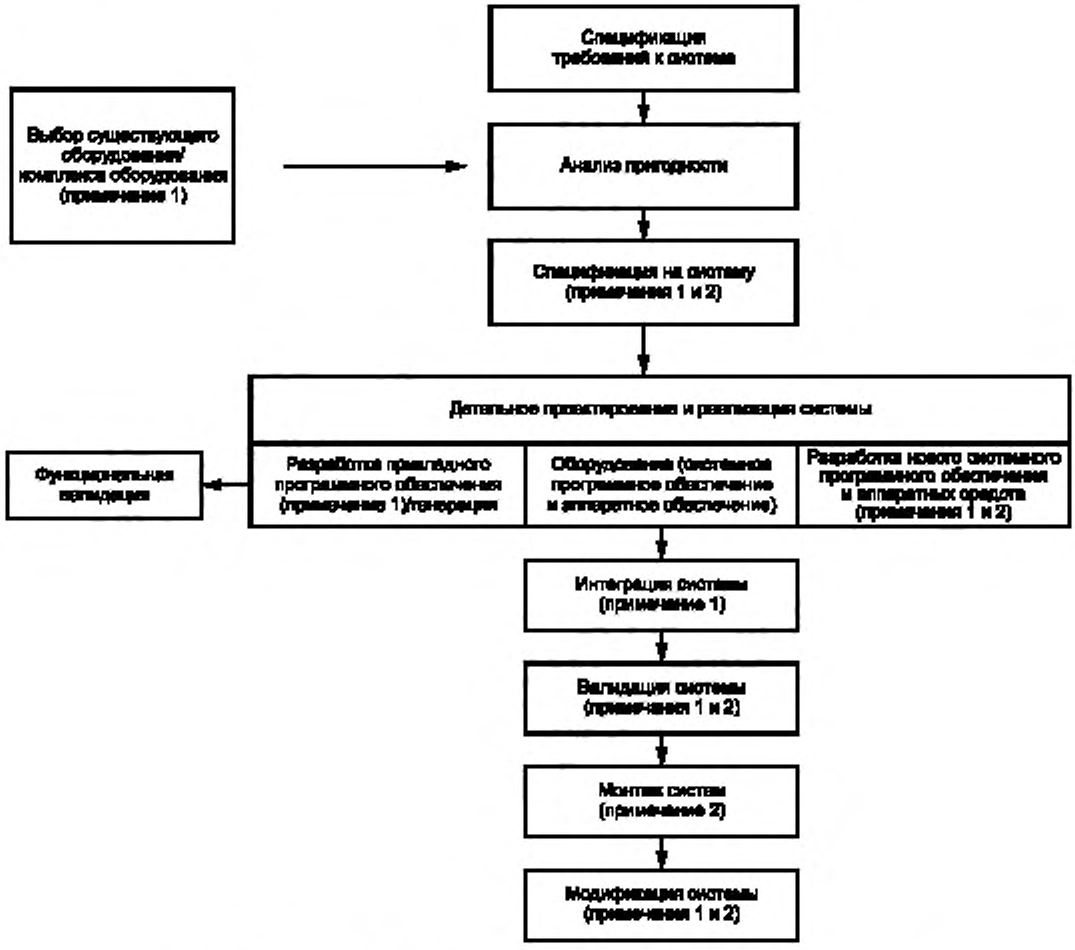
Раздел или подраздел	Входы	Цели деятельности	Выходы
6 Требования к жизненному циклу системы и его связи с общим жизненным циклом безопасности СКУ			
6.2.2 Спецификация требований к системе	Выходы 5.6, 5.5. Выходы 6.3.2, 6.3.3	Разработать спецификации требований: - к функциям; - проектным ограничениям; - границам и интерфейсам с другими системами и инструментальными средствами; - интерфейсам взаимодействия с человеком; - условиям окружающей среды	Спецификация требований к системе. Спецификация требований к прикладным функциям

Окончание таблицы 3

Раздел или подраздел	Входы	Цели деятельности	Выходы
6.2.3 Спецификация системы	Выходы 6.2.2. Документация на возможное для применения существующее оборудование. Выходы 6.3.2, 6.3.3	Проанализировать и оценить пригодность потенциального существующего оборудования для интеграции в проект системы. Разработать проект архитектуры системы для целей реализации спецификации требований к системе. Назначить прикладные функции подсистемам	Документация на спецификацию системы (см. 6.4.3), включая: - перечень выбранного оборудования и анализ его пригодности; - архитектуру системы; - спецификацию программного обеспечения
6.2.4 Детальный проект системы и реализация	Выходы 6.2.3. Выходы 5.2.2. Выходы 6.3.2, 6.3.3	Расширить и уточнить архитектуру системы. Разработать аппаратное обеспечение и (системное или прикладное) программное обеспечение. Провести валидацию требований к прикладным функциям	Детальная проектная документация на систему (см. 6.3.3). Функциональная валидация и оценка надежности (см. 6.2.4.2). Системы и компоненты аппаратного и программного обеспечения
6.2.5 Интеграция системы	Выходы 6.2.4. Выходы 6.3.2, 6.3.3, 6.3.4	Сборка отдельных компонентов аппаратного обеспечения и программного обеспечения, образующих систему	Отчет об интеграции. Интегрированная система
6.2.6 Валидация системы	Выходы 6.2.3 и 6.2.5. Выходы 6.3.2, 6.3.3, 6.3.5	Валидация системы (см. примечание 1)	Отчет о валидации системы
6.2.7 Монтаж системы	Выходы 6.2.6. Выходы 6.3.2, 6.3.3, 6.3.6	Монтаж и испытание системы	Отчет о монтаже. Смонтированная и испытанная на площадке система
6.2.8 Модификации проекта системы	Запрос на модификацию (при наличии). Выходы 6.3.2, 6.3.3, 6.3.8	Сделать исправления, улучшения или адаптацию системы	Отчеты о модификации. Модифицированная система
6.3 Планирование системы	Выходы 5.5, 6.2	Разработать план валидации, план монтажа, план эксплуатации и технического обслуживания системы, план информационной безопасности	Планы системы
6.5 Квалификация системы	Выходы 6.3.2, 6.3.3	Разработать план по квалификации, выполнить его	Квалификационная документация

Примечание 1 — Валидация отдельных СКУ осуществляется в рамках общей интеграции СКУ и ввода в эксплуатацию станции (см. 5.5.4). Работы по вводу станции в эксплуатацию находятся за рамками области применения настоящего стандарта.

Примечание 2 — Для сравнения приведенных определений этапов с определениями МЭК 61508-2 см. приложение D.



Примечание 1— Требования к программному обеспечению для данной деятельности определены в МЭК 60880 и МЭК 61138, включая применение существующего программного обеспечения.

Примечание 2— Для систем классов 1 и 2 требования к аппаратному обеспечению на данной стадии определены в МЭК 60987.

Рисунок 5 — Жизненный цикл безопасности системы

6.2 Требования

6.2.1 Общие положения

Данный подраздел определяет требования к жизненному циклу системы.

Эти требования охватывают аспекты, относящиеся:

- к конкретным функциям, назначенным системе в процессе назначения функций;
- основным характеристикам, которые в соответствии с классификацией системы делают систему пригодной для выполнения важных для безопасности функций.

Примечание — Раздел 7 МЭК 61226:2009 содержит базовые требования к функциям СКУ и особые требования к различным классам СКУ и оборудования. Эти требования учтены в настоящем стандарте при разработке требований к системам и функциям соответственно.

6.2.2 Спецификация требований к системе

6.2.2.1 Общие положения

Целью данного этапа является выполнение высокоуровневого описания требований к системе, не связанного с возможным использованием конкретных технических решений. Тем не менее специфичные требования, определенные на уровне общей архитектуры СКУ, могут накладывать ограничения на используемую технологию, например учет ООП.

Выходная документация, описывающая архитектуру СКУ и назначение функций (см. 5.6), является входом для спецификации требований к системе.

Выходная документация этого этапа устанавливает базовый документ, используемый для установления связи между теми, кто описывает постановку задачи («разработчик спецификации»), и теми, кто реализует техническое решение («проектировщик»).

Спецификация требований к системе должна определять:

- функции системы;
- эксплуатационные требования верхнего уровня;
- ограничения на проект системы;
- границы и интерфейсы с другими системами;
- интерфейсы пользователей;
- условия окружающей среды, применимые к системе;
- требуемую квалификацию.

6.2.2.2 Функции

6.2.2.2.1 Общие положения

Рассматриваемые требования включают требования к отдельным прикладным функциям и системным сервисным функциям. Применимо следующее.

6.2.2.2.2 Прикладные функции

Спецификации требований к прикладным функциям, важным для безопасности, определяют в рамках процесса назначения функций (см. 5.4.3).

a) Спецификация требования к каждой прикладной функции должна устанавливать.

1) функциональность, включающую диапазоны входа/выхода и заданных значений (соответственно допустимые диапазоны). Для функций отключений спецификация определяет допустимые границы между заданными значениями и допустимыми значениями (т. е. значениями величин с учетом всех неточностей вследствие ошибок калибровки или дрейфов нуля);

2) производительность, включающую точность и время отклика. Если применимо, эксплуатационные требования определяют для различных исходных условий на станции и ПИС;

3) для реализации всех режимов работы и для минимизации возможности ложных срабатываний необходимо определить соответствующую фильтрацию и валидацию сигналов, а также блокировки.

b) Спецификация требований к каждой прикладной функции должна устанавливать ее категоризацию и наличие ограничений со стороны других функций в группе безопасности.

Процесс назначения функций определяет для каждой категории функций минимальный класс СКУ. Вместе с требованиями к независимости между функциями одной и той же группы безопасности (критерий единичного отказа, проект защиты от ООП) такие факторы позволяют проводить качественную оценку надежности функции или группы функций в группе безопасности.

Целевая количественная оценка надежности может быть связана с каждой прикладной функцией для дополнения детерминистического процесса проектирования и для упрощения верификации проекта системы и проектных основ станции. Для аппаратного обеспечения возможность оборудования соответствовать целевой оценке может быть оценена путем применения хорошо известных методов, однако не существует общепринятого метода, пригодного для количественной оценки надежности программного обеспечения (см. 6.2.4.2.2).

6.2.2.2.3 Сервисные функции

Сервисные функции, в отличие от прикладных, напрямую не связаны с работоспособностью функций, обеспечивающих технологический процесс, но относятся к специальным деятельностям, включая функции, необходимые для конфигурации, валидации, квалификации, монтажа, ввода в эксплуатацию, эксплуатации, периодических испытаний, технического обслуживания, внедрения модификаций проекта и информационной безопасности.

Спецификации требований к сервисным функциям определяет разработчик системы. Точность требований к этим функциям определяют в зависимости от конкретного случая. В некоторых случаях они могут быть окончательно сформулированы в спецификациях на систему и на этапе проектирова-

ния архитектуры СКУ после выбора подходящего технического решения в отношении аппаратного и программного обеспечения.

В требованиях к сервисным функциям следует принимать во внимание взаимодействия и ограничения, вытекающие из системных планов (см. 6.3).

Примечание — Например, для управления изменением параметров следует соблюдать соответствие с положениями планов по безопасности системы (см. 6.3.3), эксплуатации системы (см. 6.3.7) и техническому обслуживанию системы (см. 6.3.8).

6.2.2.3 Проектные ограничения

6.2.2.3.1 Общие положения

Следующие требования определяют ограничения, которые регламентируют выбор потенциально возможных решений при проектировании системы и назначение функций в системе. Ограничения зависят от класса системы и категории функции и должны учитываться при разработке спецификации системы и проектировании архитектуры СКУ для того, чтобы:

- выполнить требования, связанные с категоризацией прикладных функций;
- гарантировать, что система будет функционировать как предусмотрено;
- позволить или облегчить демонстрацию корректной работы системы.

6.2.2.3.2 Архитектура системы

Архитектура системы ограничена категорией функций, которые должны выполняться системой (см. 5.4.3), и концепцией глубокоэшелонированной защиты (см. МАГАТЭ SSR-2/1 (Rev.1) и 3.8 и 4.23 МАГАТЭ NS-G-1.3:2002).

a) Система может реализовать функции высшей категории, соответствующей ее классу (см. 5.4.3), и функции более низких категорий. Система может включать подсистемы более низких классов, если обеспечено выполнение следующих требований:

1) требования проекта к каждой подсистеме не должны быть ниже, чем требования к функциям высшей категории, реализуемые подсистемой;

2) проект системы должен гарантировать, что требования к подсистемам или оборудованию более высоких классов выполняются в случае отказа оборудования более низкого класса.

b) Проект системы должен включать резервирование и другие меры, необходимые для обеспечения устойчивости к отказу (см. 6.2.3.3.4) и иметь назначения прикладных функций, важных для безопасности (см. 6.2.3.5).

Примечание 1 — Система может также включать резервирование для выполнения требования по доступности. Необходимость в таком резервировании определяется на уровне проекта системы.

c) Проект системы должен удовлетворять совокупности требований к независимости (см. МЭК 60709 и 6.2.3.3.3) с целью:

- предотвратить распространение отказов от систем, менее важных для безопасности;
- предотвратить распространение отказов между резервными цепочками, поддерживающими функции категории А.

d) Проект систем в группах безопасности, выполняющих функции категории А, должен включать достаточное резервирование, чтобы удовлетворить критерию единичного отказа в период эксплуатации и технического обслуживания [см. перечисление e) в 6.2.3.5].

Примечание 2 — 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, как это делается при проектировании аппаратного обеспечения. Возможное воздействие ООП из-за программного обеспечения на каждом уровне защиты и между резервными подсистемами рассматривается на уровне каждой системы и архитектуры СКУ (см. МЭК 62340).

6.2.2.3.3 Внутреннее поведение системы

a) При проектировании компьютеризированной системы следует гарантировать предсказуемое поведение, согласующееся с эксплуатационными требованиями к реализуемым функциям.

Примечание 1 — Компьютеризированная система имеет ожидаемое поведение, если временная задержка между воздействием и откликом имеет гарантированные максимум и минимум при всех требуемых условиях.

b) Коммуникационная технология должна быть выбрана и соответствовать эксплуатационным требованиям при всех загрузках данных, генерируемых при переходных процессах станции (включая лавинообразные изменения состояния в случае полной потери энергоснабжения).

c) Чтобы обеспечить высокую степень гарантии детерминированного поведения, системы класса 1 следует разрабатывать с применением технологий, как, например, приведенных в приложении В МЭК 60880:2006 (особенно В 2.d «Время выполнения» и В 2.e «Прерывания»). Технологии, использующие статическое расписание операций (см. примечание 2), предпочтительнее технологий с использованием прерываний.

Примечание 2 — Слово «статическое» означает постоянное при выполнении компьютерной программы (примерами являются структуры данных, которые не создаются и не уничтожаются во время работы после запуска, или параметры расписания, которые фиксируются после запуска). Таким образом, в статическом расписании расписание инструкции или задачи не меняется в зависимости от числа внешних событий и не приводит к изменениям использования компьютерных ресурсов, хотя при этом может быть конечное число различных расписаний в зависимости от порядка выполнения.

Примечание 3 — См. 5.5.3 МЭК 60880:2006 относительно роли приложений к стандарту и того, что требуется, если применяются практики, отличные от приведенных в приложениях.

d) Системы класса 2 могут разрабатываться с применением методов, отличающихся от приведенных в перечислении c). В этих случаях при проектировании системы следует обеспечить, что система будет работать необходимым образом при всех требуемых условиях станции (подробнее см. МЭК 62138).

e) Для увеличения возможности систем классов 1 и 2 работать в непредусмотренных условиях:

- должны быть обоснованы адекватность границ проекта, установленных для использования ресурсов (мощность вычислительного устройства, память, полоса пропускания каналов связи, ресурсы операционной системы), и внутреннее время задержки в системе;
- следует предусмотреть меры для слежения за любыми отклонениями от детерминированного поведения и подтверждения корректного режима станции в случае временной потери входной информации, например таймер, циклическое обновление, выполняемое для изменения состояния, запускающего регистрацию событий на станции.

6.2.2.3.4 Самотестирование и устойчивость к отказам

a) Системы следует проектировать так, чтобы ошибки и отказы регистрировались как можно раньше с целью поддержания требуемой доступности системы. Обнаружение отказов с помощью средств самодиагностики следует соотносить со сложностью, привносимой ими. Требования 6.2 и А.2.2 МЭК 60880:2006 по самоконтролю следует выполнять, насколько это возможно, для каждого класса системы.

b) Адекватную, своевременную и корректно представленную диагностическую информацию по отказам следует предоставлять операторам станции таким образом, чтобы они могли выполнять соответствующие корректирующие действия.

c) В проект системы следует включать безопасное восстановление работоспособности с помощью включения резервного режима работы при обнаружении отказов (частичная деградация, отказоустойчивый характеристики; переключения выходов в случае отказа).

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

6.2.2.3.5 Способность к тестированию

a) Системы должны иметь средства тестирования, которые позволяют верифицировать их способность выполнять функции, важные для безопасности.

Примечание — В соответствии с 4.83 МАГАТЭ NS-G-1.3:2002 предпочтительными тестами являются те, с помощью которых осуществляется проверка от датчиков до исполнительных устройств, но допустимыми являются и тесты, с помощью которых проводится проверка частей каналов с перекрытием этих частей. Тесты включают в основном следующее:

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

b) прерывание прохождения сигналов и подтверждение того, что устройство сбора данных определит отказ и выполнит корректирующее действие;

c) тестирование и калибровку датчиков;

d) тестирование исполнительных устройств.

b) Следует применять принципы МЭК 60671.

6.2.2.3.6 Ремонтопригодность

a) Система должна быть спроектирована таким образом, чтобы она облегчала техническое обслуживание, а в случае отказа обеспечивала простую диагностику, безопасный ремонт или замену, повторную калибровку (см. 4.97 — 4.100 МАГАТЭ NS-G-1.3:2002).

b) Средства технического обслуживания следует проектировать такими, чтобы при осуществлении технического обслуживания их воздействия на безопасность станции были приемлемы.

c) Человеческие возможности и ограничения в отношении факторов окружающей среды (температура, влажность, размещение, доступность и т. д.) должны быть приняты во внимание, чтобы свести к минимуму риск и нагрузку на персонал во время технического обслуживания.

d) Система должна быть спроектирована так, чтобы имелась возможность подтверждать правильность выполненных действий по ремонту и повторной калибровке. Это должно включать следующие проверки:

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

Примечание — Требования по техническому обслуживанию и тестированию раздела 11 МЭК 60987:2007 применяют к важным для безопасности компьютеризированным системам классов 1 и 2.

e) Особое внимание следует уделять проектированию оборудования, размещаемого в труднодоступных местах (например, в контейменте). Это может повлечь появление дополнительного резервирования или резервных линий связи.

6.2.2.4 Границы и интерфейсы с другими системами и инструментальными средствами

Для того чтобы обеспечить интеграцию системы в архитектуру СКУ в соответствии с требованиями раздела 5, должна быть предоставлена следующая информация:

- предполагаемое размещение и физические ограничения, связанные с установкой системы на станции (см. 5.2.4);
- физические и функциональные интерфейсы системы с обеспечивающими системами и оборудованием (см. 5.2.4).

Примечание — Требования к источникам электропитания СКУ, важных для безопасности, изложены в МЭК 61225 [16];

- физические и функциональные интерфейсы системы с другими системами и оборудованием, с которыми она обменивается информацией (см. 5.4.2.4);
- интерфейсы с программными инструментальными средствами, используемыми для определения обмена данными между системами и верификации целостности этих данных (см. 5.4.2.5).

6.2.2.5 Интерфейсы пользователей

Требования к ЧМИ должны гарантировать, что риск ошибки персонала является минимальным, например непредумышленные ошибки, недосмотр, упущения при монтаже, эксплуатации, испытании и техническом обслуживании системы и станции или в процессе проведения модификаций проекта.

Примечание — Защита от злонамеренных изменений рассматривается в плане защищенности (см. 6.3.3).

6.2.2.6 Условия окружающей среды

Нормальные и предельные диапазоны условий окружающей среды, которые система должна выдерживать, должны быть указаны в соответствии с ограничениями, налагаемыми в рамках проекта станции (см. 5.2.4). Условия окружающей среды должны включать:

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

Примечание 1 — В МЭК 61000-6-2 [13] и МЭК 61000-6-4, которые устанавливают минимальные уровни устойчивости и пределы эмиссии, приведены детальные руководства, связанные с электромагнитным воздействием. Серия стандартов МЭК 61000-4 представляет допустимые методы квалификационных испытаний. МЭК 62003 [15] приводит дополнительные разъяснения, касающиеся параметров квалификации и критериев стандартов МЭК 61000, обеспечивающих соответствие требованиям ядерной безопасности, например для систем классов 1 и/или 2;

- условия окружающей среды, связанные с потенциальным опасным воздействием внешних по отношению к системе факторов, включая сейсмические условия или наводнение;

- условия энергоснабжения и отвода тепла.

Примечание 2 — Условия окружающей среды могут также включать факторы, связанные с ультрафиолетовым излучением (например, деградация кабельной оплетки, стирание электронно-перепрограммируемой постоянной памяти EEPROMS), пылью или частицами, дуговой сваркой.

6.2.2.7 Квалификация

Системы, важные для безопасности, должны быть квалифицированы. Для компьютеризированных систем квалификация включает аппаратное обеспечение (включая соответствие применимым условиям окружающей среды), системное и прикладное программное обеспечение, интегрированное в аппаратное обеспечение (см. 6.5).

Примечание 1 — Квалификацию инструментальных средств также необходимо выполнять. Подход, который будет выбран, зависит от требуемой надежности и риска ошибок и отказов, которые могут быть внесены посредством использования инструментальных средств, и в каком объеме будут верифицированы выходы этого инструментального средства. Руководство приведено в МЭК 62138 и МЭК 60880.

Квалификация подтверждает соответствие проекта и оборудования требованиям. Она охватывает все аспекты, предусмотренные в спецификации системы, т. е. соответствие характеристик системы требованиям к системе, как это определено в соответствии с 6.2.2.2—6.2.2.6.

Считается хорошей практикой разделение требований на требования на системном уровне и на требования на уровне уже существующего аппаратного и программного обеспечения для использования в системе. Такой подход облегчает квалификацию с использованием ступенчатого подхода, используя имеющиеся доказательства квалификации для уже существующего оборудования (предварительная квалификация, общая квалификация), квалифицируя компоненты аппаратного и программного обеспечения по отдельности, а затем в заключение рассматривают аспекты интеграции аппаратного и программного обеспечения.

Спецификация системы должна определять методы, которые следует применять в процессе проектирования, с тем чтобы обеспечить возможность квалификации аппаратного и программного обеспечения основного оборудования, а также всей системы. Подраздел 6.5 содержит более подробную информацию.

Примечание 2 — Наиболее эффективным путем для прохождения квалификации является наличие проекта аппаратного и программного обеспечения, выполненного на основе требований и процессов, соответствующих действующим стандартам МЭК. См. также примечание 1 в 1.1.

6.2.3 Спецификация системы

6.2.3.1 Общие положения

Целью данного этапа является предоставление верхнеуровневого описания архитектуры аппаратного и программного обеспечения системы, определение оборудования, которое будет использоваться или разрабатываться для ее реализации, и назначение прикладных функций.

Спецификация требований к системе и документация на потенциально пригодное существующее оборудование являются также исходными данными для спецификации системы.

Подготовленная на этом этапе (см. 6.4.3) документация образует исходные данные для деятельности по реализации комбинированного аппаратного и программного обеспечения системы на последующих этапах жизненного цикла системы.

Этот этап включает деятельность, необходимую для разработки требований к программному обеспечению, требований к аппаратному обеспечению, а также требований по интеграции системы.

Спецификация системы должна определять:

- используемое оборудование;
- архитектуру отдельной СКУ;
- требования к программному обеспечению;
- назначение прикладных функций по подсистемам.

6.2.3.2 Выбор ранее существующих компонентов

Достаточно часто ранее существующие компоненты (отдельные компоненты аппаратного и программного обеспечения или отдельные компоненты комплекса оборудования), в отличие от вновь разработанных, применяют для реализации части или всей «новой» системы.

Примечание 1 — Ранее существующие компоненты могут быть готовыми коммерческими решениями (также называемые COTS от англ. Commercial Off-The-Shelf) или собственным, используемым самим производителем продуктом.

Примечание 2 — Раздел 15 МЭК 60880:2006 посвящен критериям приемлемости повторного применения существующего программного обеспечения функций категории А; 5.2 и 6.2 МЭК 62138:2004 описывает это для функций категорий В и С соответственно. МЭК 60987 содержит руководство по использованию ранее существующего аппаратного обеспечения.

a) Пригодность потенциально возможных компонентов должна анализироваться и оцениваться, чтобы показать, что их характеристики удовлетворяют спецификациям требований к системе.

b) Анализ и оценку пригодности потенциально возможных компонентов следует основывать на сравнении двух комплектов документации: спецификаций требований к системе и документации на ранее существующие компоненты. Документация на ранее существующие компоненты содержит спецификации на изделие и (при наличии) документацию о предварительной квалификации.

c) Применяют следующие требования:

- необходимо проанализировать, определяет ли в полной мере сопровождающая документация функциональность и свойства всех компонентов.

Примечание 3 — Предполагается определять типовые элементы: среду исполнения и загрузку памяти компонентами программного обеспечения, частоту отказов компонентов, режимы отказа и характеристики отказоустойчивости оборудования при аппаратных дефектах и ошибках программного обеспечения, условия окружающей среды для сконфигурированной системы, требования к монтажу в шкафах, разводки и подключения к источнику питания, мощность потребления, сервисные инструментальные средства;

- свойства, которые не в полной мере установлены, должны быть определены на основе анализа или испытаний и уточнены;
- в документации должны содержаться показатели надежности и производительности, которые определены для прикладных функций станции при предполагаемой(ых) конфигурации(ях) компонентов;
- документация должна определять функциональность и свойства связанных инжиниринговых методов и инструментальных средств программирования;
- неиспользуемые функции (т. е. функции, которые включены в оборудование, но не будут применяться) должны быть определены. Также должно быть продемонстрировано, что эти функции не приведут к нарушению выполнения требуемых функций.

Примечание 4 — Если имеются свойства и характеристики ранее существующих компонентов, которые не являются явно определенными в сопровождающей документации, или если использование свойств, характеристик или функций должно быть ограничено для целей соответствия спецификации требований к системе, то может потребоваться выпуск специальной адаптированной версии документации компонента, которая может использоваться для отдельной квалификации компонента (см. 6.5.2). Адаптированная документация с акцентом на безопасное использование компонента иногда называется «документацией по безопасности».

d) Если обнаружатся расхождения между спецификацией требований к системе и спецификацией комплекса оборудования, которые выявят несоответствие оборудования предполагаемому классу системы, то оборудование не должно применяться. Анализ пригодности должен установить, что спецификация возможного к применению оборудования соответствует его назначению в соответствии со спецификацией требований к системе (см. 6.4.3.2).

Примечание 5 — Характеристики доступной продукции и линеек оборудования, обнаруженные во время проведения анализа, могут влиять на последующее проектирование систем или, возможно, могут привести к итерационному процессу проектирования общей архитектуры СКУ.

e) Для систем классов 1 и 2 возможность квалификации в соответствии с 6.5 должна быть верифицирована.

Примечание 6 — Анализ возможности квалификации включает в себя не только технические свойства возможных компонентов, но и контрактные и организационные вопросы, например доступность документации детального проекта, а также наличие достаточного количества времени, учитывая то, что деятельность по квалификации компонента следует инициировать не позже начала разработки спецификации системы.

f) Если будут применяться результаты предварительной квалификации (например, результаты общей независимой программы квалификации или из другого проекта), то свойства, включенные в такую предварительную квалификацию, должны быть четко определены. Доступность соответствующих документальных подтверждений должна быть обеспечена. Дополнительная работа и ограничения, необходимые для проведения специальной станционной квалификации, также должны быть определены.

6.2.3.3 Архитектура системы

6.2.3.3.1 Общие положения

Архитектура системы разделена на ряд взаимосвязанных подсистем и компонентов, которые обеспечивают требуемое резервирование и возможность изменения конфигурации. Целью разделения системы является достижение оптимально простой компоновки аппаратного и программного обеспечений, которая отвечает функциональным и эксплуатационным требованиям, а также соответствует требованиям по надежности и ремонтопригодности.

Компоновка подсистем системы должна:

- удовлетворять ограничениям проекта в соответствии с 6.2.2.3;
- позволить выполнить требования по функциональному назначению прикладных функций (см. 6.2.3.5);
- удовлетворять требованиям к надежности прикладных функций, важных для безопасности (см. 6.2.2.2.2).

6.2.3.3.2 Территориальное распределение подсистем (централизация/децентрализация)

При определении территориального расположения подсистем на станции и каналов передачи между подсистемами следует учитывать следующие факторы:

- может оказаться необходимым разделение резервированных каналов оборудования, построенных по мажоритарному принципу, чтобы снизить влияние локальных угроз, например пожара, и обеспечить соответствие критерию единичного отказа (см. 6.2.2.3.2);
- для удовлетворения требования по контролю несанкционированного доступа может быть необходима централизация функций, важных для защищенности (см. 5.5.3);
- централизация сложного оборудования может упростить эксплуатацию, периодическое тестирование, техническое обслуживание и контроль окружающей среды;
- применение последовательной или мультиплексированной передачи может снизить количество кабелей и упростить реализацию физического разделения.

6.2.3.3.3 Независимость

Независимость включает меры по предотвращению негативного взаимодействия между подсистемами системы или с другими системами, которое может возникнуть в результате некорректной работы или из-за отказа любого компонента в подсистеме или системе, в том числе отказа по общей причине. Негативные взаимодействия могут быть результатом таких явлений, как электромагнитная индукция, короткое замыкание, дефекты заземления, пожары, химический взрыв, падение самолета и распространение поврежденных данных.

a) Когда требуется независимость (см. 6.2.2.3.2), ее следует достигать за счет использования:

- электрической изоляции, которая может быть достигнута посредством применения волоконной оптики, оптических изоляторов, экранирования кабельных линий;
- физического разделения, которое может быть достигнуто посредством отдаления, сооружения барьеров или комбинацией двух этих способов;
- независимости коммуникаций компьютеризированных систем, которая может быть достигнута посредством выбора подходящих архитектур передачи данных и протоколов обмена (см. 5.4.2.4).

Примечание 1 — Требования по электрической изоляции и физическому разделению приведены в 4.36—4.48 МАГАТЭ NS-G-1.3:2002.

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

c) Разделение и изоляция между системами, важными для безопасности, и системами и оборудованием, не важными для безопасности, 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.

6.2.3.3.4 Защита от распространения отказов и их побочных эффектов

Из-за высокой степени концентрации функций в компьютеризированных системах, в соответствии с хорошей практикой проектирования, в дополнение к мерам против распространения отказов между независимыми подсистемами следует принять меры по ограничению последствий отказов в пределах одной подсистемы.

При отказе оборудования не следует требовать слишком много управляющих действий вручную со стороны персонала по устранению последствий отказа. Это утверждение является особенно важным при проектировании замкнутых систем класса 2/класса 3, где предусмотрено резервное ручное управление.

Следующие методы могут быть рассмотрены, чтобы свести к минимуму риск и последствия распространения отказов и их побочных эффектов в архитектуре:

- внутренняя изоляция, когда отказы не могут развиться из-за отсутствия соответствующих каналов и доступных ресурсов;
- система мониторинга с помощью внутренних средств (например, самодиагностика) или внешних средств (например, другие системы или операторы), позволяющая обеспечить раннее выявление поврежденных данных и/или отказавших ресурсов;
- защитные интерфейсы, позволяющие системе или ее подсистемам выявлять поврежденные входные данные и/или ошибочные взаимодействия;
- валидацию в режиме реального времени резервированных входных сигналов, используемых в качестве входных для последующей обработки;
- при выявлении отказов необходимо применять четко определенные режимы работы для снижения возможности и/или влияния эффектов распространения отказа.

Примечание 1 — Для систем класса 1 детальные требования по избежанию подверженных ошибкам структур программного обеспечения и по верификации и испытаниям программных модулей приведены в МЭК 60880.

Примечание 2 — Детальные требования по защите от распространения отказов и их побочных действий приведены в МЭК 62340.

6.2.3.4 Спецификация программного обеспечения

Спецификация программного обеспечения включает спецификацию:

- прикладных функций (спецификации прикладного программного обеспечения);
- архитектуры программного обеспечения.

Примечание 1 — Архитектура программного обеспечения определяет основные компоненты и подсистемы программного обеспечения, как они взаимосвязаны 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, а для систем классов 2 и 3 — МЭК 62138);

- сервисных функций и функций системного программного обеспечения.

Примечание 2 — Если используют уже существующие линейки оборудования, то спецификации системного программного обеспечения являются обычно частью документации на оборудование.

Требования к спецификации программного обеспечения приведены в МЭК 60880 (для систем класса 1) и МЭК 62138 (для систем классов 2 и 3).

6.2.3.5 Назначение прикладных функций в системе

Назначение прикладных функций в системе включает назначение:

- входных сигналов функциям и функций конкретным устройствам обработки;
- процесса голосования, обработки приоритетов, функций защиты оборудования;
- связей выходных управляющих действий с исполнительными устройствами.

Применяют следующие требования:

a) назначение прикладных функций, важных для безопасности, по системам и подсистемам должно соответствовать функциональным, эксплуатационным и категоризационным требованиям спецификации к функциям (см. 6.2.2.2.2);

b) назначение должно учитывать локализацию отказов;

c) обработка резервных функций и сигналов, важных для безопасности, должна быть назначена по отдельным подсистемам, для того чтобы в случае, если отказ или локализованная опасность поражают одну подсистему, система по-прежнему могла бы выполнять свои функции;

d) все функции различных категорий, назначенные одной и той же системе или подсистеме, должны рассматриваться как функции наивысшей категории безопасности, исключая случаи, когда можно показать, что более низкая категория данных и функций не может нарушить работу функций более высокой категории, например вызвать прекращение или ложный вызов срабатывания 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 назначении — см. 5.4);

e) для функций категории А критерий единичного отказа должен выполняться при эксплуатации, даже когда один резервный канал защиты выведен на техническое обслуживание.

6.2.4 Детальное проектирование и реализация системы

6.2.4.1 Общие положения

Целью данного этапа является:

- разработать/приобрести детальный проект аппаратного обеспечения системы;
- разработать (проект и код), приобрести компьютерные программы: операционное и вспомогательное системное программное обеспечение.

Примечание 1 — Нормальной ситуацией (см. 6.2.3.3) является выполнение только ограниченного количества новых разработок, например интерфейсы с другими системами;

- разработать (проект и код) соответственно и автоматически сгенерировать прикладное программное обеспечение системы.

Примечание 2 — В общем случае, когда используется существующий комплекс оборудования, кодирование прикладного программного обеспечения автоматически генерируется теми средствами, которые входят в спецификацию прикладного программного обеспечения (см. 6.2.3.4).

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

Результатами данного этапа являются:

- аппаратное и программное обеспечение подсистем и компонентов для последующего этапа интеграции системы;
- выполняемые в системе компьютерные программы.

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

Требования к разработке программного обеспечения установлены в МЭК 60880 — для систем класса 1, в МЭК 62138 — для систем классов 2 и 3, в МЭК 60987 — требования к аппаратному обеспечению.

6.2.4.2 Требуемый анализ

6.2.4.2.1 Функциональная валидация спецификации требований к прикладным функциям

Функциональную валидацию проводят с целью выявления ошибок и пропусков в спецификации прикладных функций, которые могут быть не обнаружены при валидации системы (см. 6.2.6). Функциональная валидация включает в себя моделирование работы приводов и эксплуатации АС. Эмулятор СКУ, технический симулятор или даже полномасштабный тренажер могут быть использованы как тестовая среда.

a) Корректность соответствия спецификации прикладных функций функциональными и эксплуатационным требованиями функций станции (см. 5.2.2) должна быть валидирована для функций категории А.

b) Функциональную валидацию прикладных функций следует проводить до разработки прикладного программного обеспечения с применением анализа и моделирования. Функциональная валидация может также проводиться на этапе детального проекта, например при испытаниях финальной версии прикладного программного обеспечения на имитационных (расчетных) моделях станции.

Примечание — Пригодность такой валидации зависит от качества симулятора.

6.2.4.2.2 Оценка надежности

a) Надежность прикладных функций, выполняемых системой, должна быть признана как достаточная. Самую тщательную демонстрацию следует выполнять для функций наивысшей категории:

- демонстрация должна быть основана на детерминистическом критерии, дополненном, если применимо, количественным анализом надежности;
- оценка влияния возможных отказов аппаратного обеспечения на надежность функции должна определяться вероятностным количественным анализом, основанным на интенсивности отказов компонентов. Анализ охватывает архитектуру системы и компоненты, при этом следует учитывать как систематические, так и случайные отказы;
- оценку влияния возможных ошибок при проектировании программного обеспечения на надежность функций следует основывать на качественном анализе, принимая во внимание сложность

проекта, качество процесса разработки, с учетом опыта эксплуатации. Оценку следует основывать на ранее согласованных методах и следует продемонстрировать то, что качество программного обеспечения соответствует требуемой надежности.

Примечание — Результаты анализа и имитационных испытаний могли бы быть использованы для количественной оценки, но общепризнанной для применения методики не существует. Для аппаратно-реализованных систем, как правило, количественные показатели для отказов, возникающих из-за ошибок при проектировании, не приводят.

b) Возможность сервисных функций системы негативно влиять на прикладные функции должна быть проанализирована с тщательностью, соответствующей важности прикладных функций для безопасности.

c) Если функция, выполняемая системой, является частью группы безопасности и в этой группе безопасности существуют требования к надежности, накладываемые архитектурой СКУ (см. 5.4.4.2), то анализ надежности должен учитывать эффекты единичных отказов, отказов по общей причине и распространение отказов на все системы, входящие в данную группу безопасности.

d) Для систем класса 1 анализ надежности должен также оценивать соответствие оборудования для тестирования требованиям 6.2.2.3.5.

6.2.5 Интеграция системы

Целью данного этапа является сборка модулей аппаратного и программного обеспечения и верификация совместимости загруженного программного обеспечения и аппаратного обеспечения.

Примечание 1 — При применении 6.2 и 6.3 к сложному программируемому аппаратному обеспечению, такому как ПЛИС или ППВМ, требования к программному обеспечению также являются применимыми к программированию и данным конфигурации этого аппаратного обеспечения.

Интеграция системы состоит из следующих шагов:

- сборка и соединение модулей аппаратных средств и подсистем, как это определено в проектной документации;
- сборка целевого программного обеспечения из программных модулей;
- загрузка целевого программного обеспечения в целевые аппаратные средства;
- верификация следующего:
  - программное обеспечение соответствует спецификации проекта;
  - требования к интерфейсу аппаратных/программных средств удовлетворены;
  - программное обеспечение может работать в конкретной среде аппаратного обеспечения;
- документирование конфигурации и ее формальный выпуск для проведения валидационных испытаний.

Подсистемы и компоненты системы, документация детального проекта, план интеграции системы являются основными исходными данными для этапа интеграции системы. Применяют следующие требования:

a) интеграцию следует проводить в соответствии с планом интеграции и планом управления конфигурацией, указанными в 6.3, на основе модулей аппаратных средств, прошедших заводские испытания;

b) эксплуатационные требования должны быть верифицированы после того, как все прикладное программное обеспечение (разработанное с помощью инструментальных средств серийного оборудования или специально разработанное) интегрировано в систему;

c) система должна быть настолько полной, насколько это целесообразно для проведения испытаний;

d) сценарии испытаний, выбранные для интеграционных испытаний, должны проверять характеристики интерфейса программных модулей и подсистем, а также основные эксплуатационные характеристики самих модулей и подсистем на соответствие характеристикам из спецификации требований (например, синхронизация, особые протоколы приложений). Испытания должны показать, что все оборудование работает корректно;

e) должны быть сценарии испытаний, которые демонстрируют, что каждая отдельная прикладная функция выполняет свою задачу.

Примечание 2 — В зависимости от технологии проектирования, используемой для обеспечения предсказуемого поведения системы (см. 6.2.2.3.3), могут потребоваться тестовые сценарии, включающие случайные данные с высокой скоростью изменения, подаваемые как входные сигналы от других функций внутри этой компьютеризированной системы;

f) оборудование, используемое для верификации системы, должно быть соответствующим образом откалибровано;

g) для программных инструментов, применяемых при верификации, должны быть определены меры по обеспечению качества, соответствующие важности этих инструментов для верификации;

h) отчет об испытаниях интегрированной системы должен быть проанализирован и результаты испытаний оценены группой по верификации, обладающей хорошими знаниями спецификации системы;

i) если устранение дефекта требует модификации какого-либо верифицированного компонента программного или аппаратного обеспечения или какого-либо документа проекта, то о дефекте должно быть сообщено в соответствии с установленной процедурой (см. 6.3.2.4). Любые дефекты, обнаруженные в процессе интеграции системы, которые являются только результатом ошибки самого процесса интеграции и не влияют на проектные документы, могут быть устранены без формального отчета о дефекте.

6.2.6 Валидация системы

Целью данного этапа являются испытания интегрированной системы с целью демонстрации соответствия функциональным, эксплуатационным и интерфейсным спецификациям.

Тестирование следует выполнять с целью валидации системы и ее программного обеспечения, данных программирования и конфигурации на соответствие системным требованиям.

Валидация должна включать тесты, выполненные на системе в окончательной конфигурации сборки, включая окончательную версию программного обеспечения и других программных данных.

Интегрированная система, документация спецификации системы и план валидации системы являются основными исходными данными для этапа валидации системы.

a) Валидацию системы следует выполнять в соответствии с планом валидации, определенным в 6.3.5.

b) Система должна быть проверена с помощью статической и динамической имитации входных сигналов, существующих при нормальной эксплуатации, определенных в проекте эксплуатационных событиях и при авариях, требующих действий со стороны тестируемой системы.

c) Каждая функция системы должна быть подтверждена репрезентативными испытаниями в отношении функциональности, эксплуатационных требований и интерфейсов. Не подтвержденные таким способом требования должны быть обоснованы.

d) Для функций категорий А и В каждый аварийный или защитный параметр должен быть проверен отдельно и в соответствующих комбинациях. Испытания должны:

- репрезентативно охватывать все диапазоны сигнала и диапазоны вычисляемых параметров;
- полностью охватывать голосование и другую логику и логические комбинации;
- проводиться для всех аварийных или защитных сигналов в окончательной конфигурации сборки;
- гарантировать, что точность и время отклика подтверждены и что принимаются правильные действия в ответ на отказ оборудования или комбинацию отказов;
- проводиться для всех других функций, которые имеют непосредственное влияние на безопасность реактора (например, запреты, блокировки).

e) Для функций категории С:

- каждая функция должна быть охвачена соответствующим и обоснованным набором испытаний, основанным на представительном диапазоне сигналов, параметров и комбинаций логики. Каждый индивидуальный сигнал должен быть проверен;
- ответственные требования к точности и времени отклика сигналов должны быть подтверждены испытаниями.

f) Для систем классов 2 и 3 могут потребоваться специфичные испытания, например испытания на восстановление оборудования после отказов или испытания на влияние изменения нагрузки на системы (если система не является независимой от режима работы станции).

g) Система должна быть проверена на обеспечение защиты от ошибок оператора и от отказов другого оборудования, как это указано в спецификации требований к системе.

h) Оборудование, используемое для валидации, должно быть соответствующим образом откалибровано и сконфигурировано (параметры аппаратных и программных средств).

i) Следует показать пригодность оборудования, используемого в процессе валидации, для целей валидации системы.

В отчете о валидации системы должны быть задокументированы результаты валидации системы:

a) в отчете должны быть указаны использованные аппаратные средства, программное обеспечение и конфигурация системы, использованное оборудование и его калибровка, использованные имитационные модели;

b) в отчете должны быть указаны любые несоответствия.

6.2.7 Монтаж системы

Целью данного этапа является монтаж, полное технологическое подключение и испытания системы на площадке.

Последующая деятельность, связанная с общей интеграцией системы с другими системами и общим вводом в эксплуатацию, является частью общего жизненного цикла безопасности СКУ (см. раздел 7).

a) Монтаж системы следует выполнять в соответствии с планом по монтажу, определенным в 6.3.6.

b) Соответствующие средства, например бирки или цветная маркировка, следует использовать для однозначной идентификации компонентов, кабелей и оборудования, составляющего систему, чтобы снизить вероятность ошибок при монтаже, эксплуатации и обслуживании.

6.2.8 Модификация проекта системы

Модификации в проекте системы могут потребоваться вследствие возникновения новых системных требований или обнаружения дефектов проекта системы при анализе эксплуатационных записей и отчетов.

a) Реализацию модификации системы необходимо проводить в соответствии с утвержденными процедурами (см. 6.4.7).

b) После модификации должно быть выполнено тестирование корректности работы системы.

c) Никакие модификации аппаратного или программного обеспечения не должны выполняться в рабочем порядке, кроме предусмотренных процедурами технического обслуживания.

d) Если требуется замена аппаратного обеспечения, то должно быть продемонстрировано/обосновано, что замена соответствует спецификации на оригинальное аппаратное обеспечение.

e) Процесс модификации программного обеспечения должен соответствовать требованиям раздела 11 МЭК 60880:2006 — для систем класса 1 и 5.10, 6.10 МЭК 62138:2004 — для систем классов 2 и 3. Процесс модификации аппаратного обеспечения классов 1 и 2 должен соответствовать разделу 12 МЭК 60987:2007.

6.3 Планирование системы

6.3.1 Общие положения

Целью требований данного подраздела является разработка системных планов, обеспечивающих, что требования к реализуемым в системе функциям СКУ, важным для безопасности, будут достигнуты и будут поддерживаться.

Требования 5.5 относятся к общим планам для функций СКУ, распределенных по взаимосвязанным системам.

Примечание — Следующие требования к планам не исключают того, что планы могут быть изложены в любом другом числе документов.

Планы на систему необходимо разрабатывать на ранней стадии жизненного цикла системы до начала любой предусмотренной деятельности.

6.3.2 План по обеспечению качества

6.3.2.1 Общие положения

a) План по обеспечению качества должен быть разработан и реализован таким образом, чтобы охватывать каждую деятельность в жизненном цикле безопасности системы. Требования к плану по обеспечению качества должны быть основаны на МАГАТЭ GS-G-3.1 и ИСО 9001.

b) План по обеспечению качества должен включать деятельности, которые необходимы для достижения соответствующего качества системы, для верификации того, что требуемое качество достигнуто, а также получения объективных доказательств этого. Требования к деятельности по верификации устанавливают в плане верификации системы (см. 6.3.2.2).

c) План по обеспечению качества должен быть посвящен качеству системы и аспектам качества, связанным с интеграцией аппаратного и программного обеспечения. Планы по обеспечению качества аппаратного или программного обеспечения в настоящем стандарте не рассматриваются.

Примечание — Требования к плану по обеспечению качества программного обеспечения определены в 5.5 МЭК 60880:2006 (для систем класса 1) и 6.1, 5.1 МЭК 62138:2004 (для систем классов 2 и 3).

d) План по обеспечению качества должен включать:

- идентификацию руководящих стандартов и процедур, подлежащих применению в проекте;
- идентификацию этапов жизненного цикла системы, элементарных задач и ожидаемых результатов каждого этапа;
- описание отношений и взаимодействий между различными задачами;
- описание организационной структуры;
- приобретение компонентов у внешних поставщиков;
- идентификацию и прослеживаемость продукта. Соответствующие требования установлены в плане управления конфигурацией (см. 6.3.2.3);
- идентификацию всех процедур инспектирования и испытаний;
- идентификацию деятельности и задач ОК;
- идентификацию персонала/организаций, ответственных за деятельность и задачи ОК, включая требования к организационной независимости между соответствующими деятельностями в жизненном цикле проекта;
- процедуры отчетности и характер несоответствий относительно требований, стандартов и процедур. Процедуры должны включать учет влияния на безопасность АС и должны гарантировать, что все последствия несоответствий определены, например взаимозаменяемость, техническое обслуживание, запчасти, инструкции по эксплуатации и т. д.

e) План по обеспечению качества должен создаваться на ранней стадии жизненного цикла системы и должен быть учтен в общем плане других деятельностей жизненного цикла безопасности СКУ. План может быть частью спецификации на систему или сопроводительным документом (см. 5.5 МЭК 60880:2006 — для систем класса 1 и 6.1, 5.1 МЭК 62138:2004 — для систем классов 2 и 3).

6.3.2.2 План по верификации системы

a) План по верификации системы должен быть разработан и должен описывать:

- процесс верификации на всех этапах жизненного цикла безопасности системы;
- соответствующую организацию и распределение ответственности.

b) Результаты, полученные на каждом этапе жизненного цикла безопасности системы, должны быть верифицированы на соответствие их исходным данным.

c) Каждый шаг верификации должен завершаться отчетом о проделанном анализе и выводами. Когда этап завершен, должен быть выпущен итоговый отчет, показывающий соответствие результатов этапа исходным требованиям и устранение аномалий.

d) Верификация должна проводиться лицами, компетентным в рассматриваемых вопросах, которые хорошо понимают исходные требования, на соответствие которым проводится верификация; рекомендуется привлечение представителей, которые будут использовать результаты верификации.

e) Подробность плана по верификации системы должна быть соразмерна классу безопасности системы. План по верификации должен подчеркивать важные с точки зрения безопасности аспекты, подлежащие верификации, и в нем следует учитывать, что вероятность ошибки или пропуска в сложных элементах больше, чем в простых.

f) Документы, подлежащие верификационному анализу, должны быть определены в плане по обеспечению качества системы.

g) Документы, применяемые в верификационном анализе, например исходные данные и результаты деятельностей, отчеты по верификации и, по-возможности, инструментальные средства, использованные для получения результата, должны управляться в рамках процессов управления конфигурацией.

h) Для систем класса 1 план по верификации должен быть разработан и реализован лицами, независимыми от проектировщиков системы (в соответствии с 8.2.1 МЭК 60880:2006).

6.3.2.3 План по управлению конфигурацией системы

a) Идентификация конфигурации:

- соответствующие базовые конфигурации должны быть определены в контрольных точках жизненного цикла системы, а также должны быть определены объекты, контролируемые в базовых конфигурациях, Контролируемыми объектами могут быть промежуточные или окончательные версии объектов (например, аппаратное обеспечение, программное обеспечение, документация по верификации, пользовательская документация), а также элементы среды поддержки (например, компиляторы, инструментальные средства, испытательные стенды);

- все контролируемые объекты должны быть идентифицированы. Каждый уникальный объект должен иметь уникальный указатель и разные версии должны быть однозначно определены;

- должны устанавливаться и документироваться связи между объектами в базовой конфигурации и объектами, на основе которых они были разработаны;

- система управления конфигурацией должна иметь возможность воссоздать конфигурацию всех базовых конфигураций;

- средства поиска следует предусматривать такими, чтобы была возможность легко идентифицировать связи и многократное вхождение объектов.

b) Управление конфигурацией:

- управление конфигурацией должно обеспечивать средства, необходимые для инициации приостановки проекта. Процедуры и полномочия, требуемые для любой последующей модификации после приостановки проекта, должны быть определены, включая назначение обязанностей и полномочий для деятельности по управлению конфигурацией организациям и отдельным лицам в структуре проекта;

- статус каждого контролируемого объекта должен отслеживаться — это подразумевает наличие сведений о первоначальной утвержденной версии, статусе запрашиваемых изменений и реализации утвержденных изменений;

- план по управлению конфигурацией должен определять аудиты и анализы конфигурации, которые необходимо провести.

Примечание 1 — Хорошей практикой является различать внутренние объекты (т. е. разработанные в рамках проекта) и внешние объекты (предоставляемые поставщиками/субподрядчиками) и определять деятельность по управлению интерфейсом с внешними объектами.

c) План по управлению конфигурацией должен разрабатываться в начале проекта системы и поддерживаться в течение всего жизненного цикла системы.

Примечание 2 — ИСО 10007 [17] приводит определения и руководства по управлению конфигурацией, IEEE 828 [18] приводит руководства по планам по управлению конфигурацией программного обеспечения.

6.3.2.4 Процедуры устранения дефекта

Процедуры для отчетности и устранения дефектов, обнаруженных при верификации интеграции системы, валидации системы и на более поздних этапах, должны быть определены до начала соответствующих этапов.

a) На эти процедуры должны быть ссылки в планах по интеграции и по валидации системы.

b) Эти процедуры следует применять ко всем дефектам, обнаруженным на этапах интеграции и валидации системы, которые требуют модификации верифицированного программного обеспечения, аппаратного обеспечения или документации проекта системы.

c) Процедуры должны гарантировать, что любая повторная верификация проекта системы, аппаратного и программного обеспечения выполняется в соответствии с планом по управлению конфигурацией системы.

d) Процедуры должны гарантировать, что любая необходимая модификация проекта системы, аппаратного и программного обеспечения проводится в соответствии с процедурой модификации 6.2.8 и 6.4.7 и в соответствии с планом по управлению конфигурацией системы.

e) Анализ каждого зарегистрированного дефекта должен быть выполнен, чтобы определить, имеется ли какое-нибудь систематическое отклонение, а также не является ли характер дефекта таким, что дефект следовало бы обнаружить на более ранней стадии верификации.

f) Если это будет иметь место (т. е. дефект следовало бы обнаружить на более ранней стадии), то должно быть проведено исследование этого этапа на предмет систематического отклонения верификации.

g) Если анализ дефектов показывает, что существует систематический недочет верификации, вызывающий дефекты программного или аппаратного обеспечения, то это отклонение должно быть идентифицировано и устранено или обосновано.

6.3.3 План по защищенности

План по защищенности системы разрабатывается в соответствии с общим планом защищенности (см. 5.5.3).

a) При разработке спецификации и проекта системы требования к техническим контрмерам, определенным для системы в общем плане защищенности (см. 5.5.3), следует трансформировать в технические требования к проекту системы и документировать.

b) Для верификации того, что контрмеры, определенные в рамках анализа защищенности системы, были правильно осуществлены, следует проводить оценку документации проекта.

c) При верификации и валидации системы должна быть продемонстрирована эффективность функций защищенности посредством соответствующих испытаний с системой в ее финальной конфигурации.

6.3.4 План по интеграции системы

План по интеграции системы определяет процедурные и технические меры, используемые для интеграции подсистем в систему и интеграции аппаратного и программного обеспечения.

a) В плане по интеграции системы должны быть описаны типы выполняемых испытаний, среда испытаний и критерии приемки.

b) Интеграционный тест должен быть основан на концепции поэтапной интеграции.

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

Примечание — Испытания модулей (аппаратное обеспечение, программное обеспечение, комбинированные модули, программирование сложных электронных компонентов, таких как ПЛИС или ППВМ), выполняемые при разработке продукта, предварительной квалификации или в рамках предыдущих проектов, могут быть использованы для исключения повторения идентичных или ненужных испытаний.

d) В плане по интеграции системы, при имитации любой части системы или ее интерфейсов, должны быть продемонстрированы значимость такой имитации и ее эквивалентность оригиналу. В документации должны быть определены испытания, выполняемые на реальной части системы, и испытания, проводимые с использованием имитации интерфейсов. Должна быть продемонстрирована эквивалентность имитации. Средство имитации должно находиться под управлением конфигурацией.

e) План по интеграции системы должен определять испытания, выполняемые для каждого компьютерного блока или для каждого требования к интерфейсу подсистемы.

f) План интеграционных испытаний системы должен быть проанализирован командой по верификации, обладающей достаточными знаниями спецификации системы.

6.3.5 План по валидации системы

План по валидации системы определяет процедурные и технические меры, осуществляемые с целью демонстрации, что система соответствует своей спецификации системы и своей спецификации требований к системе. Валидацию требований к прикладным функциям рассматривают на этапе функциональной валидации (см. 6.2.4.2.1).

a) План по валидации системы следует разрабатывать, описывая конфигурацию(и) системы для валидации, выполняемые испытания и анализы, а также выпускаемые отчеты.

1) Документы по испытаниям для валидации должны определять конфигурацию системы, подлежащую испытаниям, входные данные, методы, используемые инструментальные средства и калибровки, а также соответствующие критерии приемки. В соответствующих случаях следует оценивать точность и влияние инструментальных средств наблюдения на поведение системы.

2) Документы по анализу валидации должны определять, что следует продемонстрировать при испытаниях, а также ожидаемые результаты и соответствующие критерии приемки.

Примечание 1 — Хорошей практикой считается, если подготовка плана валидации системы и спецификация испытаний начинаются с завершением подготовки первой версии спецификации требований к системе для того, чтобы сведения, полученные во время подготовки спецификации испытаний, можно было применять как раннюю обратную связь при подготовке спецификации требований.

b) Для функций категории A должен быть разработан план по валидации системы, должны быть выполнены работы по валидации и проанализированы результаты командами, независимыми от тех, кто осуществлял проектирование, реализацию или модификацию системы (см. раздел 10 МЭК 60880:2006).

Примечание 2 — Независимость друг от друга лиц, привлеченных к выполнению плана валидации и подготовке отчета по ее итогам, не требуется.

c) Для функций категории B в разработку плана по валидации системы должны быть включены ответственные лица, которые не принимали участие в проектировании, реализации и/или модификации системы.

d) Для функций категорий A и B план по валидации системы должен обеспечивать прослеживаемость между спецификацией и соответствующими испытаниями и верификациями.

e) Для функций категории C в плане по валидации системы следует обеспечивать прослеживаемость между спецификацией и соответствующими испытаниями и верификациями.

Считается хорошей практикой проводить валидационное испытание в несколько этапов на заводе и на площадке. Стратегия поэтапного валидационного испытания (см. также 5.5.4) может включать следующие шаги:

- имитационные/эмуляционные испытания для валидации прикладного программного обеспечения;
- первая серия валидационных испытаний в течение интеграционных испытаний на заводе;
- повторная серия валидационных испытаний во время интеграционных испытаний на площадке;
- окончательные валидационные испытания в рамках общей программы ввода станции в эксплуатацию.

6.3.6 План по монтажу системы

План по монтажу системы определяет процедурные и технические меры, осуществляемые по монтажу системы на площадке и для проверки, необходимой для подтверждения готовности системы к эксплуатации. План дополняется общими планами по интеграции и вводу в эксплуатацию (см. 5.5.4).

a) План по монтажу системы следует разрабатывать и описывать меры, которые будут гарантировать и верифицировать, что конфигурация системы и любых изменяемых параметров является верной, что система целостная, правильно смонтирована, собрана, соединена и может эксплуатироваться как требуется в соответствии со спецификацией.

b) Для систем класса 1 план по монтажу должен соответствовать требованиям раздела 10 МЭК 60987:2007.

c) Для функций категории А для каждого канала безопасности должна быть продемонстрирована корректная работа на площадке.

6.3.7 План по эксплуатации системы

План по эксплуатации системы описывает, каким образом система должна эксплуатироваться, и требования, применимые в течение эксплуатации системы.

a) План по эксплуатации системы должен определять, как система должна функционировать во всех режимах эксплуатации. План должен соответствовать плану по техническому обслуживанию системы (см. 6.3.8) и общим планам эксплуатации и технического обслуживания (см. 5.5.5 и 5.5.6).

b) В плане эксплуатации следует определять условия, которым система должна соответствовать, прежде чем ее начнут эксплуатировать. В частности:

- система должна быть полностью смонтирована, интегрирована и введена в эксплуатацию (см. 5.5.4);
- план по техническому обслуживанию системы (см. 6.3.8) и пользовательская документация должны быть доступны.

c) Если требуются периодические испытания (см. 6.2.2.3.5), то план по эксплуатации системы должен определять:

- частоту и продолжительность каждого испытания, условия, которые следует выполнять, прежде чем начать испытание, и влияние, при наличии, на эксплуатацию системы и станции;
- шаги, необходимые для выполнения каждого испытания, применяемые инструментальные средства и средства калибровки, анализ корректности результатов;
- верификацию полного восстановления нормального состояния, если требуются временные изменения в системе.

Примечание — Периодические испытания проводят совместно персоналом, осуществляющим эксплуатацию и техническое обслуживание. Эта деятельность может рассматриваться как часть регламентного технического обслуживания (см. 6.3.8).

d) План по эксплуатации системы должен определять порядок ведения записей при ее эксплуатации. Записи должны включать в себя детали отказов, записи о проведенных испытаниях системы и записи требований к системе.

e) План по эксплуатации системы следует рассматривать с точки зрения его влияния на безопасность станции.

f) План по эксплуатации системы должен определять требования по периодическим испытаниям системы в соответствии с требованиями, определенными в соответствии с 6.2.2.3.5.

6.3.8 План по техническому обслуживанию системы

Техническое обслуживание системы включает процедурные и технические меры, необходимые для поддержания функциональности эксплуатируемой системы. План по техническому обслуживанию системы разрабатывают таким образом, чтоб он соответствовал плану по эксплуатации системы и общему плану эксплуатации и технического обслуживания (см. 5.5.5 и 5.5.6).

a) План по техническому обслуживанию системы должен быть разработан и должен определять:

- регламентные действия и процедуры, которые будут применять для выявления неявных отказов системы, поддержания функциональности эксплуатации «как спроектировано» и надежности системы (профилактическое техническое обслуживание);

- действия и процедуры, которые необходимо выполнять для восстановления системы в полностью рабочее состояние (корректирующее техническое обслуживание).

b) Объем профилактического технического обслуживания следует определять на основе метода систематического анализа, например анализ характера отказа и его влияния на работу системы, или на основе применения модели обслуживания, ориентированной на обеспечение надежности, или на основе анализа деревьев отказа для функций системы.

c) Процедуры замены компонентов должны гарантировать следующее:

- установленные компоненты функционально идентичны замененным и соответствуют требованиям по качеству;

- если замену проводят в горячем режиме, то ее воздействие на функциональность системы оценивают и документально оформляют до проведения замены;

- делают записи о всех заменах, что позволяет выполнить любые требования по прослеживаемости.

d) Процедуры по повторной калибровке должны гарантировать следующее:

- новую калибровку выполняют в заданных пределах (если такие пределы устанавливаются системой, то нет необходимости предъявлять формальные ограничения к действиям обслуживающего персонала);

- если повторную калибровку проводят в горячем режиме, то ее воздействие на работоспособность системы оценивают и документально оформляют до проведения операции;

- делают записи обо всех операциях повторной калибровки, что позволяет выполнить любые требования по прослеживаемости.

6.4 Выходная документация

6.4.1 Общие положения

Настоящий подраздел определяет выходную документацию на этапах жизненного цикла системы: содержание, характеристики и основные разделы, которые необходимо верифицировать.

Требования к выходной документации должны представлять собой ряд соответствующим образом ссылающихся друг на друга взаимосогласованных документов, которые гарантируют прослеживаемость финальной версии проекта к входным требованиям.

6.4.2 Документация спецификации требований к системе

6.4.2.1 Содержание

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

6.4.2.2 Характеристики

Характеристики документа спецификации требований к системе:

a) требования должны быть однозначными и верифицируемыми;

b) основными пользователями спецификации требований являются эксперты и лица, ответственные за спецификацию системы и функциональную валидацию. Требования должны быть ясными, краткими, полными, связанными и корректными, а также подготовленными с учетом работы с ними указанных ранее лиц;

c) требования к прикладным функциям следует излагать в функциональных терминах, а не в терминах компьютерной технологии, чтобы позволить выполнять их верификацию инженерам-технологам СКУ и персоналу, осуществляющему эксплуатацию, которые могут иметь ограниченные знания в области компьютерной технологии;

d) Требования следует разрабатывать с использованием документированных методов системной инженерии, инструментальных средств и руководств.

Примечание — Детальные требования относительно программных инструментальных средств, для систем класса 1, приведены в разделе 14 МЭК 60880:2006;

e) для облегчения выполнения оценки соответствия спецификации на систему и обеспечения связи с планом квалификации системы требования следует записывать и структурировать.

6.4.2.3 Верификация

Должны быть верифицированы следующие требования:

a) требования должны быть прослеживаемыми и связанными с требованиями к системе, установленными в проекте архитектуры и функциональном назначении (см. 5.6);

b) требования к интерфейсам должны быть согласованы с требованиями к взаимодействующим системам и оборудованию;

c) следует определять требования, которые необоснованно увеличивают сложность системы (сложность может привести к увеличению риска ошибок в спецификации требований к системе и/или в самой системе).

6.4.3 Документация спецификации системы

6.4.3.1 Содержание

a) Документация спецификации системы должна быть полной и однозначной и должна представлять всю информацию, необходимую для последующих действий в рамках жизненного цикла безопасности системы, особенно на этапах проектирования и валидации системы.

b) Документация спецификации системы должна определять, какое оборудование будет использоваться: ранее существующее оборудование или вновь разработанное. Пригодность выбранного оборудования должна быть подтверждена.

c) Документация спецификации системы должна описывать архитектуру системы:

- декомпозицию системы на подсистемы и/или на компоненты аппаратного и программного обеспечения;
- внутреннее функционирование системы (см. 6.2.2.3.3), включая описание основных постулированных событий, внутренних по отношению к системе, и ее защиту от этих событий (см. 6.2.3.3.4);
- границы, условия окружающей среды, ожидаемую надежность аппаратного обеспечения, функционирование, функции, работу и интерфейсы каждой подсистемы;
- классификацию каждой подсистемы; следует представлять обоснование, если класс подсистемы ниже, чем класс системы или подсистемы, в которую она входит;
- условия эксплуатации и связь идентифицированных подсистем с системой.

Примечание — Описание подсистем может выполняться в соответствии с иерархией, чтобы облегчить восприятие от общего описания вниз до элементарных подсистем (т. е. подсистем, которые далее не декомпозируются в документации проекта системы). «Горизонтальная» информация может быть также полезна.

d) Документация спецификации системы должна включать спецификацию программного обеспечения (см. 6.2.3.4).

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

6.4.3.2 Характеристики

Характеристики документации спецификации системы:

a) основными пользователями документации спецификации системы являются эксперты и лица, ответственные за проектирование системы и выполнение комплексной интеграции и валидации. Документация должна быть ясной, краткой, полной, систематизированной и актуальной, и написана соответствующим для понимания персоналом образом;

b) спецификацию прикладных функций следует выполнять в терминах, которые облегчают верификацию и понимание со стороны инженеров-технологов СКУ и эксплуатационного персонала станции;

c) спецификацию системы следует разрабатывать с использованием документированных методов системной инженерии, инструментальных средств и руководств. Это следует делать так, чтобы указанные методы, средства и руководства минимизировали отличия от методов, инструментальных средств и руководств, используемых при создании спецификации требований к системе.

Примечание — Методы программной инженерии и инструментальные средства могут улучшить качество окончательной спецификации проекта системы, даже по сравнению со спецификацией проекта аппаратной системы;

d) спецификацию системы следует оформлять и структурировать, чтобы облегчить оценку целостности спецификации требований к системе и обеспечить наличие эффективных ссылок для валидации системы, т. е. следует облегчить полную идентификацию спецификаций (вместо объяснений и другой информации).

6.4.3.3 Верификация

a) Верификацию спецификации системы на соответствие спецификации требований к системе следует проводить до завершения разработки детального проекта. Это позволит осуществить корректирующие действия до реализации и интеграции системы.

b) Чтобы верифицировать пригодность выбранного оборудования, следует устанавливать эффективную коммуникацию между ответственными за спецификацию системы и поставщиками.

c) Верификация должна документировать соответствие и регистрировать любое несоответствие спецификации системы по отношению к спецификации требований к системе.

d) Преобразование спецификации требований к прикладной функции в спецификацию прикладного программного обеспечения должно быть верифицировано на корректность.

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

f) Для систем классов 1 и 2 оборудование, увеличивающее сложность системы, но не требующееся спецификацией требований к системе, должно быть выявлено, а его наличие обосновано с точки зрения безопасности.

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

6.4.4 Документация детального (технорабочего) проекта СКУ

6.4.4.1 Общие положения

Детальный проект может быть реализован в несколько итераций. Требования настоящего подраздела относятся к документации на систему, когда детальный проект, интеграция и валидация системы завершены и система готова к поставке и монтажу на площадке станции.

Документация детального проекта, как правило, может быть разделена на четыре группы документов:

- документы проекта системы;
- требуемый анализ (см. 6.2.4.2);
- документы проекта прикладного программного обеспечения;
- документы проекта компонентов аппаратного обеспечения и системного программного обеспечения.

Примечание 1 — Если система реализована с применением ранее существующего оборудования, то документы проекта на аппаратное обеспечение и системное программное обеспечение являются частью документации на ранее существующее оборудование.

Рассматриваются только первые две группы, поскольку проекты программного обеспечения и аппаратного обеспечения не входят в область применения настоящего стандарта (см. 6.2.4).

Примечание 2 — Для систем класса 1 и классов 2/3 требования к документации на программное обеспечение установлены в МЭК 60880 и МЭК 62138, а требования к документации на аппаратное обеспечение — в МЭК 60987.

6.4.4.2 Содержание

a) Документация проекта системы должна быть полной, однозначной и должна представлять всю информацию, необходимую для последующих деятельностей в жизненном цикле системы, включая интеграцию, валидацию, установку, эксплуатацию и техническое обслуживание.

b) Документация проекта системы дополняет документы спецификации и должна представлять детальное описание внутренней структуры и функционирования системы. Уровень детализации описания может быть соотнесен с классом безопасности системы.

c) Документация проекта системы должна включать в себя описание монтажа оборудования на станции и положения по испытаниям системы.

d) Документы проекта системы должны включать описание валидированной функциональности и работы системы, в частности, ожидаемое время отклика при различных условиях работы станции, номинальные параметры безопасности установок и алгоритмам управления, а также диапазоны параметров безопасности.

6.4.4.3 Характеристики

Характеристики проектной документации системы:

a) основными адресатами документации проекта системы являются эксперты и разработчики планов по интеграции системы, квалификации системы, монтажа и ввода в эксплуатацию системы и

плана технического обслуживания системы, а также обслуживающий персонал, разработчики и эксперты модификаций проекта. Документацию следует разрабатывать в форме, доступной для понимания персоналом;

b) актуальность документации детального проекта должна быть поддержана в течение разработки системы, чтобы гарантировать, что финальная версия документов соответствует реализованному проекту.

6.4.4.4 Верификация

a) Верификацию детального проекта системы и его документации следует выполнять до реализации нового аппаратного обеспечения и программного обеспечения; следует предусматривать достаточное время, чтобы гарантировать реализацию любых корректирующих действий по результатам верификации.

b) Требования к надежности, определяемой для прикладных функций системы (см. 6.2.4.2.1), следует верифицировать 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 решений по выбору общей архитектуры СКУ.

c) Возможность сервисных функций системы подвергать опасности выполнение прикладных функций должна быть неукоснительно проанализирована посредством определения роли безопасности прикладных функций.

d) Допущения, внесенные при верификации детального проекта, должны быть сформулированы и задокументированы.

6.4.5 Документация по интеграции системы

6.4.5.1 Содержание

Документация по интеграции системы должна включать документацию (план) интеграции, отчеты об интеграционных испытаниях и всю информацию, необходимую для последующих этапов валидации.

6.4.5.2 Характеристики

Отчеты об интеграционных испытаниях должны содержать следующую информацию:

- версии модулей аппаратного обеспечения и программного обеспечения, используемую спецификацию испытаний, используемые инструментальные средства и оборудование вместе со всеми выполненными калибровками и данными по настройке оборудования, любое использованное оборудование или любые симуляции интерфейса;
- результаты каждого испытания с перечислением всех несоответствий полученных результатов ожидаемым и для каждого несоответствия — запись по проведенному анализу и принятым решениям о продолжении испытания или о реализации изменения;
- решения по всем зафиксированным дефектам и результаты последующей оценки должны быть задокументированы достаточно подробно и таким образом, чтобы мог быть проведен их аудит лицами, напрямую не вовлеченными в процесс разработки системы и плана верификации.

6.4.5.3 Верификация

a) Верификацию отчетов об интеграции системы на соответствие плану по интеграции следует выполнять до проведения валидации.

b) Для систем классов 1 и 2 должна быть обеспечена прослеживаемость от документации проекта к соответствующим компоненту и интеграционным испытаниям и анализам, чтобы облегчить оценку испытаний и анализов с точки зрения объема испытаний.

c) Для систем класса 3 следует обеспечивать прослеживаемость от документации проекта к соответствующим компоненту и интеграционным испытаниям и анализам, чтобы облегчить оценку испытаний и анализов с точки зрения объема испытаний.

6.4.6 Документация по валидации системы

6.4.6.1 Содержание

Документация по валидации системы должна включать план по валидации и отчеты о валидационных испытаниях, а также всю информацию, необходимую для квалификации системы.

6.4.6.2 Характеристики

a) В отчете по валидации системы должны быть отражены характеристики программного обеспечения валидации системы.

b) В отчете должны быть указаны аппаратные средства, программное обеспечение, другие программируемые и конфигурационные данные и используемая конфигурация системы, используемое оборудование и его калибровка, а также используемые имитационные модели.

c) В отчете также должны быть указаны все выявленные несоответствия между ожидаемыми и полученными результатами и для каждого несоответствия выполнена запись о проведенном анализе и принятом решении о том, проводить ли испытания далее или реализовать изменение.

d) В отчете должны быть обобщены результаты валидации системы.

e) В отчете должна быть дана оценка соответствия системы всем требованиям.

f) Результаты валидации и результаты последующего анализа должны сохраняться в таком виде и с такой степенью детализации, которая позволит провести их аудит лицам, непосредственно не участвовавшим в валидации.

g) Использованные в процессе валидации программные инструментальные средства следует указывать в соответствующем разделе отчета. Симуляции станции и ее систем, используемые для валидации, должны быть задокументированы.

6.4.6.3 Верификация

Результаты валидационных испытаний и их анализ должны быть задокументированы и рассмотрены на соответствие требованиям, представленным в плане по валидации системы, чтобы подтвердить, что функциональная работа системы удовлетворяет этим требованиям.

Примечание — Документация по валидации вместе с документацией по функциональной валидации (см. перечисление d) в 6.4.4.2) подтверждает соответствие системы как спецификации системы, так и спецификации требований к системе.

6.4.7 Документация по модернизации и модификации системы

6.4.7.1 Содержание

a) Запрос на модификацию

Этот документ должен устанавливать:

- обоснование изменений и влияние (при наличии) на безопасность АС;
- функциональное описание изменения (с чертежами с разметкой, блок-схемами, структурными схемами и пр.) и предполагаемые средства реализации изменения;
- связь данного изменения с любыми другими связанными изменениями на станции.

b) Пакет модификации

Когда изменение проекта завершено, т. е. внесены изменения в компоненты программного обеспечения, компоненты аппаратного обеспечения и документацию, отражающую изменение проекта, следует подготовить пакет изменений на внесение изменений в работающую систему. Пакет документации должен описывать модули аппаратного обеспечения, модули программного обеспечения и средства реализации изменения, т. е. какое оборудование следует выключить, какая процедура должна быть выполнена для загрузки нового программного обеспечения, или может быть предоставлена ссылка на утвержденную существующую процедуру.

6.4.7.2 Характеристики

Запрос на модификацию должен быть однозначно идентифицирован и должен быть оценен и принят или отклонен компетентными лицами. Результат рассмотрения (принят или отклонен) должен быть оформлен документально.

6.4.7.3 Верификация

a) Для систем класса 1 весь пакет документов по реализации модификации должен быть рассмотрен на полноту и правильность технического решения специалистами, не принимавшими непосредственного участия в модификации проекта, но являющимися технически компетентными для оценки изменения.

b) Пакет модификации не должен быть включен в систему без оценки вносимого изменения.

6.5 Квалификация системы

6.5.1 Общие положения

Данный подраздел устанавливает требования к квалификации классифицированных СКУ (см. 6.2.2.7). Этот процесс обеспечивает подтверждение, что СКУ способна удовлетворять на постоянной основе функциональным и эксплуатационным требованиям проектных основ, необходимым для обеспечения выполнения функций, важных для безопасности, в определенных условиях окружающей среды и при определенных ограничениях (см. 6.2.2.2—6.2.2.6).

Примечание — Серия стандартов МЭК 61508 может быть использована в качестве дополнительного руководства при квалификации и оценке компонентов.

6.5.2 Общая и прикладная квалификация

Хорошей практикой является использование доказательств квалификации компонентов аппаратного обеспечения и программного обеспечения, проведенной вне рамок проекта станции или в контексте специального приложения (например, предварительная квалификация или общая квалификация коммерческих продуктов или комплекса оборудования), чтобы разделить трудозатраты по квалификации между несколькими проектами (см. 6.2.3.2). Общая квалификация может быть проведена как единая работа для нескольких проектов АС или может быть проведена поставщиком операционной системы, используемой для обеспечения безопасности. Предварительная квалификация также может быть проведена для продуктов, первоначально предназначенных для областей, не связанных с проектированием АС, необязательно в полном соответствии методам и процедурам, требующимся в проекте.

Примечание 1 — Сертификация готовых коммерческих продуктов на соответствие уровням полноты безопасности 1, 2 или 3 согласно стандартам серии МЭК 61508, осуществляемая независимым и аккредитованным экспертом, является одним из примеров предварительной квалификации коммерческого оборудования. Поскольку стандарты серии МЭК 61508 являются обобщающими стандартами для МЭК 61513, то такая сертификация обеспечивает хорошую базу для прикладной квалификации коммерческих продуктов и для демонстрации соответствия требованиям МЭК 61513 и его дочерних стандартов.

При использовании результатов предварительной квалификации ранее существующего оборудования необходимо выполнять прикладную квалификацию, чтобы подтвердить соответствие доказательств, полученных в ходе предварительной квалификации, требованиям к СКУ или устранить выявленные пробелы. Такая прикладная квалификация может предполагать разнообразные виды деятельности, такие как приемка результатов существующей квалификации на основе анализа существующей документации, проведение аудитов, дополнительных функциональных, климатических и сейсмических испытаний и оценка опыта эксплуатации.

a) В зависимости от объема существующей документации и доказательств в рамках предварительной квалификации, соответствующая программа квалификации должна быть определена и включена в план квалификации (см. 6.5.3).

b) Прикладная квалификация должна касаться свойств и характеристик, не охваченных предварительной квалификацией.

c) Прикладная квалификация должна касаться различий между методологией и процедурами, использованными при предварительной квалификации, и методологией и процедурами, указанными в спецификации требований к системе (см. 6.2.2.7).

Примечание 2 — В прикладной квалификации, как правило, учитывается следующее:

- доказательства предварительной квалификации применимы и соответствуют требованиям к СКУ;
- любые пробелы в доказательствах выявлены и устранены;
- в случае замены оборудования любые различия проекта по отношению к существующему оборудованию или к системе проверены и подтверждено отсутствие неблагоприятных воздействий;
- приемочные и эксплуатационные критерии, использованные при проведении предквалификационных испытаний, соответствуют данному приложению.

Процесс квалификации системы может быть разбит на стадии: сначала квалификация отдельных компонентов аппаратного и программного обеспечения СКУ, а затем — квалификация интегрированной СКУ (т. е. законченного реализованного проекта).

d) Квалификация аппаратного и программного обеспечений системы, построенной путем конфигурации комплекса оборудования или путем соединения существующих компонентов, может быть получена из квалификации, проведенной для отдельных компонентов и конфигураций соединенных компонентов. В таких случаях должен быть проведен анализ для демонстрации того, что квалификация охватывает финальную конфигурацию системы, используемую на станции, включая монтажное расположение, распределение нагрузки и температуры внутри шкафов.

e) На основании предыдущего анализа в плане квалификации следует определить все новые особенности проекта системы и установить необходимость проведения дополнительных квалификационных испытаний и оценок.

6.5.3 Документация (план) по квалификации

6.5.3.1 Общие положения

Необходимо разработать план по квалификации, который определяет все темы, подлежащие анализу и оценке, для целей квалификации системы и функций, важных для безопасности, и реализует и поддерживает статус квалификации.

План по квалификации включает аппаратные, программные и системные аспекты. Даже если используемые аппаратные и программные компоненты прошли предварительную квалификацию в соответствии со стандартами по квалификации, как минимум, доступная квалификационная документация должна быть проанализирована на соответствие требованиям к системе и для подтверждения ее пригодности, а аспекты системной интеграции должны быть оценены (анализ пригодности).

На рисунке 6 приведен обзор видов деятельности.

Примечание — Квалификация существующих компонентов или коммерческих продуктов всегда специфична для конкретной версии этого продукта. Любые модификации проекта — это изменение версии, и квалификация при этом будет нуждаться в переоценке.

6.5.3.2 Функциональная и климатическая квалификация

Примечание 1 — Функциональную квалификацию и квалификацию в отношении условий окружающей среды также называют «квалификацией аппаратного обеспечения».

Для реализации функциональной квалификации и квалификации по условиям окружающей среды допускается применять несколько методик. Как правило, такая квалификация выполняется поэтапно, сначала на уровне отдельных компонентов или частей подсистем, а затем на уровне целой системы. Квалификация компонентов и частей подсистем включает типовые испытания, функциональные испытания, оценки и экспертизы проекта и опыт эксплуатации в подобных приложениях. Предпочтительным является метод, основанный на проведении типовых испытаний (см. 4.1 МЭК 60780:1998).

Примечание 2 — Обычно функциональная квалификация включает работу оборудования, интегрированного с его фирменным или системным программным обеспечением, работающего в характерном для него режиме использования. Как правило, она составляет последний этап интеграционных испытаний фирменного средства/аппаратного средства в цикле разработки оборудования СВ.

a) Системы классов 1 и 2 должны быть квалифицированы по условиям окружающей среды в соответствии с требованиями МЭК 60780 и МЭК 60980. Условия окружающей среды должны включать условия, указанные в 6.2.2.6.

b) Системы класса 3, для которых требуется специальная квалификация по условиям окружающей среды (например, сейсмостойкость или работа в особых условиях окружающей среды), могут быть квалифицированы по общепромышленным стандартам. Требования к работе в особых условиях окружающей среды, к квалификации по сейсмическим воздействиям в соответствии с общепромышленными стандартами или к другим функциональным характеристикам должны быть подтверждены документальными доказательствами. В тех случаях, когда существуют факторы существенного старения и когда квалификация срока службы не может быть продемонстрирована в соответствии с определением по МЭК 60780, должна быть предоставлена и обоснована проводимая программа квалификации в соответствии с МЭК 60780.

c) Квалификация по электромагнитной совместимости должна быть выполнена в соответствии с требованиями стандартов серии МЭК 61000-4. Условия окружающей среды должны включать требования, определенные в 6.2.2.6.

d) Последовательность испытаний, включая приемочные критерии, следует устанавливать для испытаний компонентов или конфигураций компонентов, или всей системы таким образом, чтобы:

- проверить функциональные характеристики при нормальных условиях окружения и при всех указанных предельных рабочих условиях;
- проверить указанную самодиагностику, характеристики безотказности и режимы ограниченной функциональности;
- продемонстрировать устойчивость к соответствующим климатическим условиям (включая сейсмические и электромагнитные внешние условия).

e) Анализ следует выполнять при необходимости обоснования характеристик системы, которые не могут быть адекватно подтверждены другими способами. Такой анализ может включать:

- анализ надежности для представления или обоснования данных по надежности;
- анализ режима отказа и последствий, подтверждающий специфицированные виды отказов и представляющий набор данных для функций самодиагностики;
- анализ схем, подтверждающий указанные функциональность, точность и пределы.

6.5.3.3 Анализ и оценка программного обеспечения

Примечание 1 — Анализ и оценка программного обеспечения также называется «квалификация программного обеспечения».

При анализе и оценке программного обеспечения учитывают, насколько строго соблюдался процесс разработки программного обеспечения, а также объем тестирования и валидации, проведенных на интегрированной системе. Для ранее разработанного программного обеспечения опыт его эксплуатации может при определенных условиях компенсировать недостаток информации о процессе разработки.

Программное обеспечение компьютеризированных систем, подлежащее квалификации, должно включать:

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

a) Квалификация должна проводить анализ и оценку как для системного, так и для прикладного программного обеспечения для предоставления достаточной гарантии, что качество программного обеспечения является соответствующим для достижения требуемой надежности функций, выполняемых системой.

b) Для систем класса 1 вновь разработанное программное обеспечение должно быть проанализировано и оценено в соответствии с требованиями МЭК 60880.

c) Программное обеспечение существующего оборудования, выбранного для систем класса 1, следует разрабатывать в соответствии с известными руководствами и стандартами, обеспечивающими высокое качество, требуемое для функций категории А (см. 7.2.2.1 МЭК 61226:2009). В частности, требования МЭК 60880 к ранее разработанному программному обеспечению и инструментальным средствам и требования МЭК 60987 должны быть выполнены.

Примечание 2 — Пункт 15.3.3 МЭК 60880:2006 определяет критерии приемки и ограничения на использование документированного опыта эксплуатации в процессе квалификации.

d) Программное обеспечение существующего оборудования, выбранного для систем класса 2, должно быть разработано в соответствии с общепризнанными руководствами и стандартами. В противном случае программное обеспечение может быть квалифицировано в соответствии с критериями МЭК 62138, принимая во внимание задокументированный опыт удовлетворительной работы программного обеспечения в аналогичных приложениях.

e) Критерии по анализу, оценке и приемке программного обеспечения для систем класса 3 приведены в МЭК 62138.

6.5.4 Дополнительная квалификация взаимосвязанных систем

a) Должен быть разработан план для дополнительного испытания, которое может потребоваться на уровне взаимосвязанных СКУ для завершения их индивидуальной квалификации, например испытания на электромагнитную совместимость отдельных линий связи и заземления, устойчивость поведения системы в случае перегрузки и некорректного поведения сети.

b) Выполнимость и последовательность дополнительного испытания должны быть верифицированы как часть верификации проекта архитектуры СКУ.

6.5.5 Поддержание квалификации

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

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

Примечание — Дополнительный план может быть изложен в специальном разделе плана квалификации (см. 6.5.2), определяющем модификацию, либо в специальном отдельном документе. Рекомендуется составлять дополнительный план как можно раньше. Также рекомендуется утвердить руководство по квалификации модификаций уже на начальном этапе проектирования, чтобы иметь возможность пользоваться им при вводе в эксплуатацию.

6.5.6 Документация

a) Следует перечислять информацию, которая будет предоставляться лицензирующему органу.

Примечание — Как правило, отчеты о квалификации СКУ классов 1 и 2 и отдельных систем класса 3 (например, систем, связанных с блочным и дополнительными пунктами управления) будут представлены регулятору в процессе лицензирования.

b) В перечне документации следует различать информацию, необходимую до монтажа системы, и информацию, которую следует предоставлять лицензирующему органу в процессе монтажа и ввода системы в эксплуатацию, например отчеты об испытаниях. Типы информации, которые могут потребоваться, включают в себя следующее:

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

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

- отчет о предварительном анализе безопасности и обобщающие документы для оценки концептуального и технического проектов 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 независимых процессов по верификации и валидации;
- информацию, касающуюся монтажа, интеграции, ввода в эксплуатацию, приемочных испытаний на заводе изготовителя (поставщика) и на площадке станции, для того чтобы обеспечить верификацию тех этапов жизненного цикла безопасности, которые находятся между этапами проектирования и эксплуатации;
- документацию с информацией, необходимой для эксплуатации системы, чтобы верифицировать процедуры поддержки качества системы в течение длительного времени.

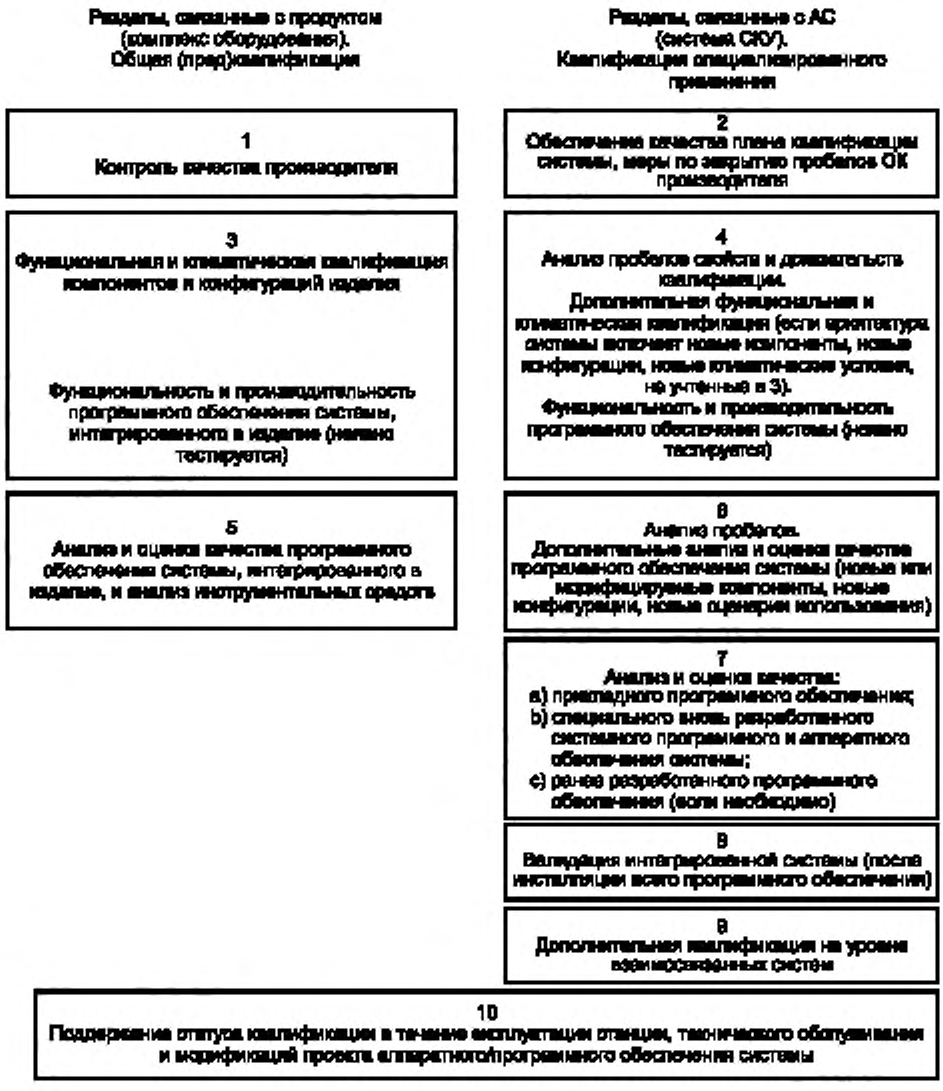


Рисунок 6 — Разделы плана квалификации системы, связанные с квалификацией продукта и с прикладной квалификацией АС

7 Общая интеграция и ввод в эксплуатацию

7.1 Общие положения

Целью данного этапа является интеграция СКУ на площадке и гарантия того, что все функции СКУ, важные для безопасности, выполняются, как и ожидалось, во время приемо-сдаточных испытаний станции. План ввода в эксплуатацию СКУ включают в программу ввода в эксплуатацию систем станции (см. 4.4 МАГАТЭ 75-INSAG-3:1999).

7.2 Цели, которые должны быть достигнуты

а) Деятельность необходимо проводить систематически на основе стратегии, разработанной в соответствии с планами по монтажу системы, интеграции и вводу в эксплуатацию, защищенности, определенными в 5.5 и 6.3.

b) Работы по общей интеграции СКУ следует выполнять со всеми связанными СКУ, смонтированными и отдельно испытанными (см. 6.2.7).

c) Программное обеспечение и базы данных с параметрами должны быть загружены, а сохраненные значения должны быть обоснованы и протестированы.

d) Аппаратное и программное обеспечение компьютеризированных систем должно находиться под управлением конфигурацией.

e) Верификация и валидация всех функций, важных для безопасности, должны быть завершены до введения этих функций в эксплуатацию.

7.3 Выходная документация

a) Документация по интеграции СКУ с записями о хронологии деятельностей по верификации и валидации на площадке должна быть представлена до начала эксплуатации.

b) Отчет о деятельности по общему вводу в эксплуатацию должен подтвердить, что СКУ удовлетворяют всем ожиданиям по их использованию и функции, важные для безопасности, соответствуют общим спецификациям требований (см. 5.3).

c) Обнаруженные отклонения от проекта оценивают, корректируют или доводят до сведения эксплуатирующей организации, чтобы любое влияние на работу станции не было оставлено без внимания.

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

8 Общая эксплуатация и техническое обслуживание

8.1 Общие положения

Общая эксплуатация СКУ может быть начата после экспертизы отчетов о вводе в эксплуатацию, которая покажет, что данная деятельность успешно завершена. Эксплуатация может продолжаться до тех пор, пока записи данных об эксплуатации не будут свидетельствовать о необходимости ремонта или модификации. Эксплуатация может быть продолжена после успешного завершения ремонта или модификации и рассмотрения соответствующих отчетов.

С эксплуатирующей организацией до начала эксплуатации при переходе из фазы ввода в эксплуатацию следует согласовывать условия начала эксплуатации. Следующие требования являются независимыми от указанного согласования:

- должны быть завершены необходимые испытания систем, чтобы подтвердить их соответствие функциональности спецификации. Если при испытаниях выявлены дефекты, то они должны быть задокументированы и, если возможно, исправлены перед передачей системы в эксплуатацию;
- должны быть доступны соответствующая документация пользователя и планы технического обслуживания.

8.2 Цели, которые должны быть достигнуты

СКУ эксплуатируют и обслуживают таким образом, чтобы требования к функциям СКУ, важным для безопасности, были удовлетворены.

a) Планы по эксплуатации, техническому обслуживанию и защищенности, указанные в 5.5 и 6.3, должны быть реализованы.

b) Процедуры, предназначенные для операторов станции или обслуживающего персонала в нормальных условиях эксплуатации и при возникновении аварии, должны находиться в помещении блочного пункта управления или в ближайшем помещении. Следует обеспечивать, чтобы их форма и содержание соответствовали международным или национальным нормативным актам.

c) Процедуры технического обслуживания, испытаний и модификации аппаратных и программных средств должны быть реализованы в соответствии с МЭК 62138, МЭК 60880 и МЭК 60987.

8.3 Выходная документация

Должна быть сохранена вся хронология документации по эксплуатации, ремонту и техническому обслуживанию. Оперативные записи следует регулярно рассматривать с целью оценки негативных эксплуатационных трендов и в случае выявления любых тенденций, указывающих на неприемлемое ухудшение оборудования СКУ, следует выполнять корректирующие мероприятия.

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

Приложение А
(справочное)

Основные вопросы безопасности атомных станций

А.1 Общие положения

Настоящее приложение определяет общие положения концепций безопасности, которые рассмотрены в настоящем стандарте в проекте СКУ АС. В приложении приведен обзор содержания документов МАГАТЭ, но при этом оно не ставит перед собой задачу расширить требования, изложенные в этих документах.

А.2 Цели безопасности станции

Любая промышленная деятельность, которая влечет за собой риски для персонала, населения и окружающей среды, требует от оператора принятия всех мер, необходимых для минимизации этих рисков. Одним из характерных рисков ядерной энергетики является потенциальная угроза ионизирующего излучения [см. раздел 2 МАГАТЭ SSR-2/1 (Rev.1)].

Основной целью ядерной безопасности является защита людей, общества и окружающей среды посредством установления и поддержания эффективной защиты от радиационного воздействия АС.

Технической целью безопасности действующих АС является «целевая вероятность» возникновения тяжелого повреждения активной зоны менее 10^{-4} событий в год на энергоблок. Реализация всех принципов безопасности для будущих станций должна привести к улучшению показателя вероятности до значения не более 10^{-5} событий в год на энергоблок. Управление тяжелой аварией и меры смягчения последствия аварий должны привести к уменьшению вероятности повышенного выброса с АС, требующего контроля за ее пределами не менее чем в 10 раз (см. 2.3 МАГАТЭ 75-INSAG-3:1999).

А.3 Анализ безопасности станции

А.3.1 Общие положения

Анализ безопасности проекта АС выполняют с целью установления и подтверждения проектных основ для элементов, важных для безопасности, и гарантии, что общий проект АС способен обеспечить соблюдение пределов и контрольных уровней доз облучения, а также выбросов, установленных регулирующим органом, для каждой категории состояния АС [см. раздел 5 МАГАТЭ SSR-2/1 (Rev.1)].

Анализ безопасности может включать:

- демонстрацию того, что эксплуатационные пределы и условия соответствуют требованиям нормальной эксплуатации АС;
- характеристики ПИС, соответствующие проекту АС, и места их возникновения;
- анализ и оценку последовательностей событий, возникающих вследствие ПИС;
- сравнение результатов анализов с радиационными критериями приемлемости и проектными пределами;
- установление и подтверждение проектных основ;
- демонстрацию того, что управление при отклонениях от нормальной эксплуатации и в условиях аварии является возможным с помощью автоматических систем безопасности в комбинации с предписанными действиями оператора.

Такой процесс анализа безопасности АС выполняется итеративно, начиная с концептуального проекта и до окончательной оценки безопасности АС, и учитывает все детали конфигурации АС, которые могут иметь влияние на безопасность. Анализ безопасности АС учитывает вероятные ошибки персонала в процессе эксплуатации и условиях аварии.

Целью анализа является демонстрация того, что действия, которые выполняются автоматическими системами и операторами, повлияют на поведение АС таким образом, что доза облучения персонала и населения останется ниже установленных пределов при нормальной эксплуатации, ожидаемых эксплуатационных событиях и в условиях аварии.

А.3.2 Анализ последовательности событий

Целью анализа последовательности событий является систематическое и подробное выявление всех возможных последствий ПИС на АС, включая те из них, которые возникают из-за отказов вспомогательных и обеспечивающих систем и из-за возможной ошибки оператора. Результаты такого анализа последовательности событий могут затем использоваться для определения соответствия требованиям безопасности станции, правилам проектирования, установленным МАГАТЭ [см. приложения к МАГАТЭ SSR-2/1 (Rev.1)].

Пригодным аналитическим инструментальным средством для определения возможных состояний АС после ПИС являются анализ дерева событий (качественный анализ) и анализ 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 ПИС и последовательность событий, которые соответствуют граничным случаям проекта безопасности. При выборе последовательности событий следует учитывать опыт на существующих АС.

Даже ограничиваясь рассмотрением последовательности событий, приводящих к граничным случаям, как указано выше, применение методологии дерева событий во многих практических случаях приводит для каждого ПИС к выявлению гораздо большего числа конфигураций АС, чем в действительности может быть рассмотрено детально. Поэтому допустимо ограничивать детальный анализ определенным числом репрезентативных последовательностей событий.

А.3.3 Оценка проектных основ: детерминистический/вероятностный методы

Для оценки степени достижения целей безопасности разработаны соответствующие методы (см. МАГАТЭ 75-INSAG-3).

При детерминистическом подходе проектные события выбирают так, чтобы ограничить круг связанных возможных исходных событий, которые могли бы повлиять на безопасность станции.

Вероятностный анализ используют для оценки вероятности любой конкретной последовательности и ее последствий. При проведении оценки допустимо принимать в расчет меры по смягчению последствий как на самой станции, так и за ее пределами.

Сравнение детерминистического и вероятностного подходов: нехватка достаточных данных о компонентах или о поведении системы или невозможность определить подходящий режим может привести к невозможности применения строгого количественного вероятностного подхода. Однако частичный вероятностный подход может зачастую дополняться качественной инженерной оценкой. С другой стороны, детерминистический подход требует такую инженерную оценку, которая в неявной форме содержит некоторые качественные вероятностные критерии.

В сущности, текущая практика состоит в использовании детерминистического подхода при проектировании систем и вероятностного подхода для оптимизации отдельных частей проекта и оценки общей безопасности.

А.4 Глубокоэшелонированная защита

Основным вкладом в философию безопасности является концепция глубокоэшелонированной защиты. Эта концепция должна применяться ко всей деятельности по безопасности: организационной, поведенческой или связанной с проектированием, для обеспечения взаимного наложения мер безопасности, чтобы в случае, когда отказ произошел, он был бы скомпенсирован или скорректирован [см. МАГАТЭ SSR-2/1 (Rev.1); МАГАТЭ 75-INSAG-3; МАГАТЭ INSAG-10 и МАГАТЭ NS-G-1.3].

Первое применение концепции глубокоэшелонированной защиты к процессу проектирования заключается в создании независимых, но дополняющих друг друга комплектов оборудования и процедур для предотвращения аварий или для обеспечения надлежащей защиты в случае, если меры предотвращения не сработали.

Примеры многоуровневой защиты:

- создание многократно резервированных средств, гарантирующих выполнение каждой основной функции безопасности, т. е. управление реактивностью, отвод тепла и удержание радиоактивности;
- использование надежных защитных устройств в дополнение к внутренним средствам безопасности;
- дополнение управления станции с помощью автоматики и действий оператора;
- наличие оборудования и процедур для смягчения последствий аварии.

В общем, все уровни защиты должны быть доступными в течение всего времени, как определено для различных эксплуатационных режимов.

Цель первого уровня защиты — предотвратить отклонение от нормальной эксплуатации. Для этого необходимо, чтобы АС была надежно и консервативно спроектирована, сооружена и эксплуатировалась при надлежащих уровнях качества и инженерных практиках.

Цель второго уровня защиты — выявить и перехватить отклонения от условий нормальной эксплуатации, чтобы предотвратить переход предусмотренных проектом эксплуатационных событий в аварию.

Для третьего уровня защиты предполагается (хотя очень маловероятно), что развитие предусмотренных событий не могло быть предотвращено предыдущими уровнями защиты, поэтому для управления последствиями возникающих аварийных условий предусматривается дополнительное оборудование и процедуры. Еще одной из главных задач этой линии защиты является достижение стабильных и приемлемых условий после аварии.

После третьего уровня защиты дополнительная защита населения обеспечивается за счет дополнительных свойств станции (которые не являются важными для безопасности) и планов аварийной готовности, которые, по большей части, не зависят от проекта реакторной установки.

Второе применение концепции глубокоэшелонированной защиты состоит в сооружении и эксплуатации АС так, чтобы радиоактивные материалы удерживались группой физических барьеров. Эти физические барьеры являются пассивными и чаще всего включают в себя топливо, оболочку топливного элемента, границу контура ох-

лаждения реактора и защитную оболочку. Проект должен обеспечить необходимую эффективность и защитные свойства каждого из указанных выше физических барьеров.

Дополнительное применение концепции глубокоэшелонированной защиты заключается в осуществлении однократного или многократного резервирования СКУ. Для того чтобы уменьшить масштаб нарушения и достичь глубокоэшелонированной защиты, допускается применение более одной СКУ, которые срабатывают по мере того как контролируемая переменная отклоняется от требуемого значения. В первую очередь, если переменная отклоняется от значений, соответствующих нормальным условиям, срабатывают 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 или значительно 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 Описание схемы категоризации/классификации

МАГАТЭ NS-R-1 устанавливает перечень функций безопасности, которые позволяют проекту станции удовлетворять общим требованиям безопасности, от средств безопасного останова реактора до отвода остаточного тепла от активной зоны и снижения вероятности выброса радиоактивных веществ. Данный документ устанавливает принцип классификации компонентов, содержащих жидкости, необходимых для выполнения функций безопасности, в соответствии с их важностью для безопасности. Данный документ вводит методологию ранжирования функций безопасности и назначения требований к проекту, основанную на последствии отказа функции безопасности, вероятности того, что функция может потребоваться, и вероятности того, что функция может не выполняться, когда потребуется.

МАГАТЭ NS-G-1.3 распространяет принцип классификации на системы контроля и управления. Данный документ подразделяет СКУ на «системы, важные для безопасности», и «системы, не важные для безопасности». Далее системы, важные для безопасности, подразделяют на «системы безопасности» и «системы, связанные с безопасностью» и устанавливают требования к проекту.

МЭК 61226 классифицирует функции, важные для безопасности, на три категории: А, В и С. Данный стандарт устанавливает критерии назначения категорий функциям СКУ и требования к проекту для соответствующих систем и оборудования.

Количество классов, определенных МАГАТЭ, отличается от установленных в МЭК 61226 (системы, безопасности и системы, связанные с безопасностью, в отличие от категорий А, В и С). Более того, МАГАТЭ и МЭК не всегда используют идентичные определения и концепции (система классификации МАГАТЭ отличается от категоризации функций/классификаций систем в МЭК), и эти расхождения могут быть источником различных интерпретаций.

Настоящий стандарт следует положениям МЭК 61226 в отношении деления на три класса, данный подход типичен для различных уровней обеспечения требуемой работоспособности и надежности, достигаемой при использовании существующих методологий и продуктов СКУ (например, разработанные в соответствии со стандартами атомной отрасли, отобранное и классифицированное коммерческое или серийное оборудование, отобранное коммерческое или серийное оборудование). Однако во избежание неоднозначной трактовки требований стандарта приняты отдельные схемы градации функций и систем.

Ниже изложены основные положения настоящего стандарта по категоризации и классификации.

В.2 Обоснование принципов категоризации и классификации, принятых в настоящем стандарте

В.2.1 Общие положения

Функции, системы и оборудование АС можно рассматривать с двух точек зрения (см. рисунок В.1):

- функциональная точка зрения

С этой точки зрения рассматривают только выполняемые функции. Хотя известно, что датчики, устройства обработки, устройства интерфейса и т. д. необходимы для реализации функции, функциональная точка зрения не учитывает эти элементы, т. к. они могут быть интегрированы в состав более крупной сборки оборудования, которая также выполняет и другие функции (см. «системная точка зрения»). Средства, необходимые для реализации функции, называются системами и оборудованием, связанными с данной функцией;

- системная точка зрения

Данная точка зрения рассматривает системы как организованный набор оборудования, который реализует множество функций/подфункций; например система защиты, система автоматизации и управления, система ЧМИ. Отдельные функции, выполняемые системой, могут относиться к разным категориям.

В.2.2 Этап проектирования технологии АС

Проектировщики технологических процессов АС анализируют станцию и связанные системы с функциональной точки зрения. Они определяют характерные ПИС для АС и реактора и функции, важные для безопасности, необходимые для обеспечения управления этими исходными событиями с целью предотвращения их развития в аварию. Несколько независимых функций (или подфункций) может потребоваться для каждого ПИС в соответствии с принципом глубокоэшелонированной защиты. Функции (или подфункции) относят к категориям А, В или С в зависимости от того, играют ли они принципиальную, дополнительную, вспомогательную или косвенную роль в обеспечении безопасности АС.

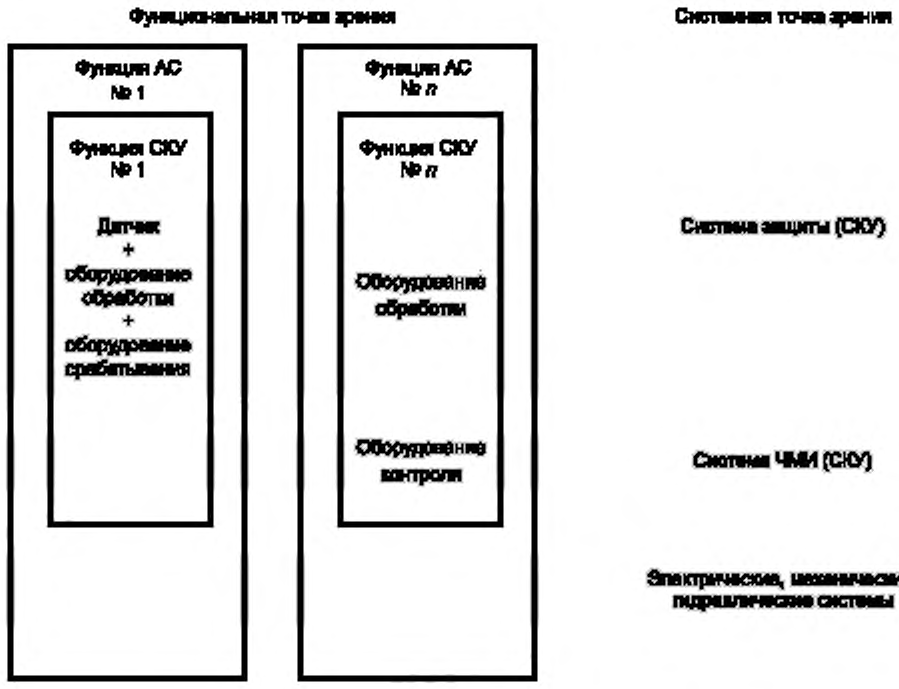


Рисунок В.1 — Взаимосвязь между функциями СКУ и СКУ системами

Методы категоризации, как правило, основаны на детерминистическом, вероятностном соображении и соображении с позиции снижения риска. Они принимают во внимание различные факторы, такие как вероятность и возможная тяжесть последствий ПИС при сбоях в СКУ, отрезок времени, в течение которого функция требуется после ее инициации, временные границы и надежность, с которыми могут быть выполнены альтернативные действия или устранен любой отказ в СКУ.

Процесс категоризации допускает, что функции СКУ группы безопасности могут быть распределены по различным категориям, например может потребоваться альтернативная автоматическая остановка реактора, которая запускается только при маловероятных условиях предусмотренного переходного процесса, сопровождающегося отказом основной защитной функции. В этом случае вместо присвоения функции СКУ категории А (должна быть реализована в системе класса 1) ей может быть присвоена категория В или С.

Категории определяют уровень требований к проекту, а также минимальный требуемый класс соответствующих систем и оборудования, необходимых для реализации функции.

В.2.3 Этап проектирования СКУ АС

Проектировщики СКУ АС анализируют функции СКУ, соответствующие системы и оборудование, используя системный подход. Их задача состоит в определении количества СКУ, необходимых для реализации функций СКУ, с требуемым для проектирования технологического процесса уровнем качества и независимости. Системам назначают классы в зависимости от достижимого уровня качества.

Процесс классификации и назначения функций для компьютеризированных систем отличается от подхода, применяемого для аппаратной технологии, поскольку:

- при аппаратной технологии функции, как правило, реализуются по одной в цепи отдельных электронных компонентов или реле, а компьютеризированные системы с использованием одних и тех же компонентов оборудования позволяют выполнять несколько функций;
- компьютеризированная система включает в себя ряд вспомогательных функций, например функции самоконтроля и диагностики, которым не присваивается категория при проектировании станции. Этим функциям может потребоваться более низкий уровень квалификации, но требуется функциональная изоляция;
- выбор архитектуры системы может быть ограничен с целью ограничения сложности и для упрощения выполнения функций высшей категории безопасности;
- для проектировщика существует возможность формировать требования к архитектуре систем, например функциональное разделение, внутреннее поведение, сложность, защита от ООП, которые не связаны с отдель-

ными функциями, но связаны с СКУ, и свойствами комплекса оборудования, используемого для реализации этих систем и квалификации таких систем.

Это приводит к очевидной необходимости устанавливать систему классификации для СКУ в зависимости от функции, обладающей наивысшей категорией из выполняемых системой функций.

В.3 Категоризация функций СКУ, важных для безопасности

В настоящем стандарте предполагается, что проект безопасности станции, разрабатываемый проектировщиками технологии, определяет категоризацию отдельных функций СКУ, важных для безопасности, по трем категориям: A, B, C. Определение требований к категоризации по сути определяет степень качества элементов, которые используют для реализации функции.

Категоризация функций СКУ завершается на уровне подфункций (см. примечание), так что дополнительный анализ для завершения категоризации на уровне процесса инженерам СКУ 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 станции определяет требования к независимости и разнообразию отдельных функций для обеспечения глубокоэшелонированной защиты. Независимость требуется между функциями, поддерживающими различные уровни защиты в одной и той же группе безопасности, между функцией защиты и функцией снижения риска.

Требования к независимости и разнообразию являются входами в процесс назначения функций СКУ. Функции СКУ могут быть распределены по различным СКУ так, чтобы они имели одну и ту же классификацию безопасности (см. раздел В.2).

В.4 Классификация систем контроля и управления

СКУ, которые образуют общую архитектуру СКУ, обычно объединяют ряд функций или подфункций, которые выполняют схожие задачи на станции. Системы, как правило, могут быть охарактеризованы функциональностью, которую они выполняют. Количество СКУ и их функциональность зависят от типа станции. Характерные примеры СКУ, важных для безопасности, приведены ниже.

a) Системы автоматизации и контроля

Системы контролируют параметры энергоблока или оборудования:

- для поддержания показателей технологического процесса в пределах в соответствии с анализом безопасности станции;
- поддержания безопасной эксплуатации систем станции и оборудования, важных для безопасности;
- снижения до минимума размеров и частоты возможных нарушений;
- снижения до минимума частоты возникновения событий, которые требуют срабатывания систем защиты. Это может достигаться за счет обеспечения высокого качества, резервирования диверсных систем автоматизации и контроля или реализации более чем одного уровня воздействия. Например, это достигается комбинацией автоматического и ручного управления, если имеется достаточное время для правильной реакции, или комбинацией двух и более из указанных выше мер.

Системы автоматизации и контроля могут влиять на безопасность, т. к. их эксплуатационные характеристики, надежность, а также последствия отказа составляют часть проектных основ для системы защиты. Системы автоматизации и контроля могут быть также основным средством выполнения функций, важных для безопасности, например, если имеется достаточно длительный период времени для осуществления корректирующих действий.

Типичная функциональность этих систем включает управление в разомкнутом контуре, управление в замкнутом контуре и выполнение действий вручную.

b) Системы ЧМИ

Системы представляют информацию оператору станции и другим лицам о состоянии станции и ее систем, важных для безопасности. Они также используются для поддержки принятия решения оператором и выполнения вручную действий по поддержанию безопасности станции.

Типичная функциональность таких систем заключается в следующем:

- преобразовании информации от датчиков или сигналов других систем в информацию, пригодную для отображения или регистрации на индикаторах, электронно-лучевых трубках, принтерах и т. д. Система предоставляет такую информацию, как обзор, сокращение числа аварийных сигналов, а также поддержка эксплуатации;
- отображении аварийных и предупредительных сигналов и другой информации;
- обеспечении интерфейса для запуска ручного управления.

c) Системы активации защиты и безопасности

Эти системы гарантируют, что определенные проектом пределы не превышаются в результате предусмотренных эксплуатационных событий и что последствия аварий находятся в пределах основы проекта.

Типичная функциональность этих систем:

- определение аварийных условий и автоматическое инициирование работы соответствующих систем, включая остановку реактора;
- обеспечение приоритетности выполнения функций различных категорий (например, прерывание работы системы контроля).

d) Система аварийного энергоснабжения

Типичная функциональность:

- аварийная разгрузка;
- последовательная нагрузка дизель-генераторов и других источников энергоснабжения.

СКУ, выполняющие функции, важные для безопасности, относятся к одному из трех классов, которые соответствуют определенному проекту, производству и требованиям к квалификации, которые позволяют этим системам выполнять функции, относящиеся к одной категории или более: A, B или C, или неклассифицированные функции (см. В.2). Пример типовой классификации СКУ приведен в таблице В.1.

Таблица В.1 — Типовая классификация СКУ

	Класс 1	Класс 2	Класс 3	Неклассифицированные
Системы автоматизации и контроля АС		X	X	X
Системы ЧМИ (класс 1 может быть ограничен несколькими критическими индикаторами и кнопками)	X	X	X	X
Системы активации защиты безопасности	X			
Система аварийного энергоснабжения	X			

Требования к функции самой высокой категории безопасности определяют класс системы.

Приложение С
(справочное)

Качественный анализ мер защиты от отказов по общей причине

С.1 Примеры распределения функций группы безопасности по системам

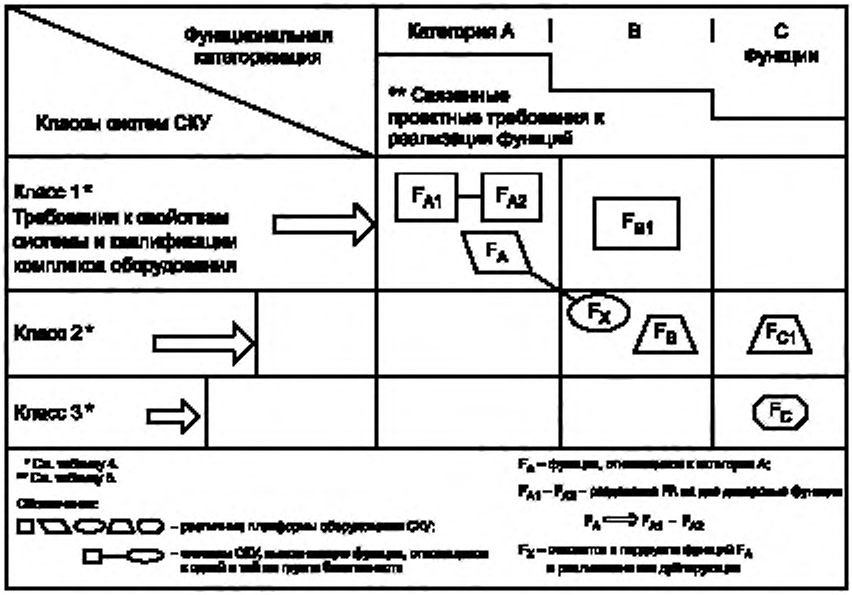


Рисунок С.1 — Примеры распределения функций группы безопасности по СКУ

Требования к свойствам оборудования и квалификации, как, например, требования к внешней среде и надежности программного обеспечения, могут быть получены из подходящего выбранного комплекса оборудования. Требования к системам сфокусированы на особенностях проекта, как, например, допустимый дефект архитектуры системы и адекватность процедур верификации и валидации проекта, принятых для обеспечения корректного функционирования.

На рисунке С.1 показаны некоторые примеры распределения функций по группам безопасности СКУ[1)], которые отражают различные проектные стратегии для достижения требуемой надежности. Стратегии основаны на анализе эффективности различных мер против ООП.

F_{A1}—F_{A2}: состав группы безопасности включает две функционально различные функции: F_{A1} и F_{A2} категории А. Оценка анализа ООП должна показать, что для этого случая использование функционального разнообразия способствует эффективной защите от ООП. Затем обе функции реализуются в независимых системах класса 1, выполненных на том же самом комплексе оборудования.

F_A—F_X: состав группы безопасности включает основную функцию F_{A1} категории А и дополнительную функцию категории В или С, функция F_X как резервная. Анализ ООП должен в этом случае показать, что применение разнообразия оборудования обеспечивает достаточную защиту от ООП. Функция F_A назначается одной системе класса 1, а функция F_X реализуется в системе класса 2, выполненной на другом комплексе оборудования для того, чтобы обеспечить разнообразие оборудования.

F_{B1}—F_B: состав группы безопасности включает две функционально разнообразные функции категории В—F_{B1} и F_B. Анализ ООП должен показать, что применение разнообразия оборудования и функционального разнообразия обеспечивает достаточную защиту от ООП. Функцию F_{B1} назначают одной системе класса 1, а функ-

[1)] *В НП-026-16 «Требования к управляющим системам, важным для безопасности атомных станций» определено понятие «функциональная группа» — совокупность элементов управляющей системы, важной для безопасности, выполняющая управляющую или информационную функцию в установленном проектом АС объеме».*

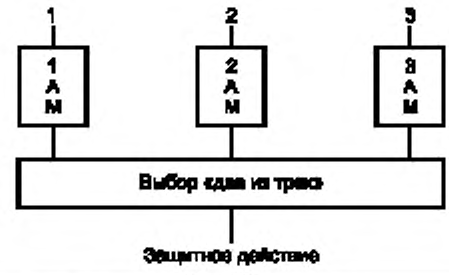
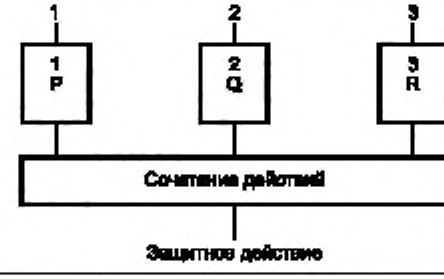
цию F_B реализуют в системе класса 2, выполненной на другом комплексе оборудования для того, чтобы обеспечить разнообразие оборудования.

Случай с функциями F_{C1} и F_C аналогичен предыдущему случаю.

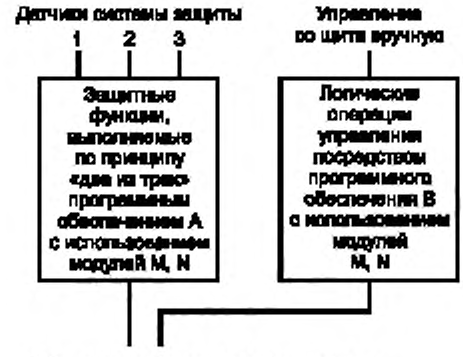
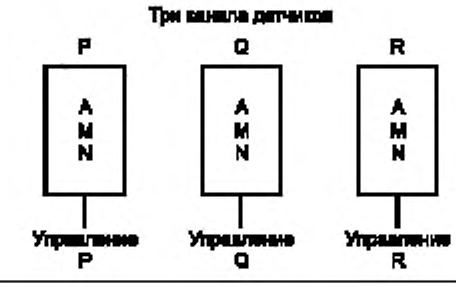
С.2 Примеры чувствительности к ООП в группах безопасности

Могут возникнуть следующие типичные ситуации.

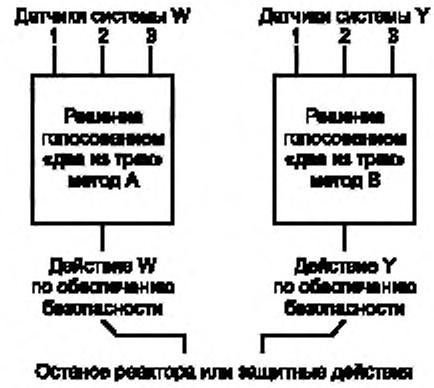
Таблица С.1 — Примеры чувствительности ООП в группе безопасности

Пример 1 Группа безопасности, содержащая систему с тремя идентичными резервированными каналами, выполняющими единственную защитную функцию А	
Возможные причины ООП Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка в спецификации требований к прикладной функции А (H)	Независимая верификация спецификации (M)
Дефект в спецификации или в разработке прикладного программного обеспечения или дефект в модуле системного программного обеспечения (M). Отказ может возникнуть как следствие прохождения одинаковых сигналов по трем каналам [(L) — для систем класса 1)]	Разработка системы, соответствующей классу 1 (H)
Одновременный отказ аппаратного обеспечения трех каналов вследствие опасного воздействия на станцию	Физическая и электрическая независимость (H)
Отказ при срабатывании двух из трех (или при других действиях каналов)	Разработка системы класса 1 (H); надежные, проверенные на практике решения (стандартный модуль) (H)
Пример 2 Группа безопасности, содержащая систему с резервированными каналами, реализующими одиночную функцию защиты А с общей спецификацией требований и разным программным обеспечением (блоки P, Q, R)	
Возможные причины ООП Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка в спецификации требования к прикладной функции А (H)	То же, что в примере 1

Продолжение таблицы С.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). Недостаток: разнообразное программное обеспечение
Одновременный отказ оборудования трех каналов вследствие опасного воздействия на станцию	То же, что в примере 1
Отказ при срабатывании двух из трех каналов (или при других действиях каналов)	То же, что в примере 1
Пример 3 Группа безопасности, содержащая систему с двумя каналами, выполняющими независимо одну и ту же защитную операцию* * Предполагается, что оператор имеет достаточное время и информацию для реагирования.	
Возможные причины ООП Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка при спецификации требования к обеим функциям (L)	Защита обеспечивается функциональным разнообразием (автоматически; вручную) (H)
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)
Одновременный отказ оборудования каналов системы вследствие опасного воздействия на станцию	То же, что в примере 1
Ошибка при голосовании «два из трех» (или при других действиях каналов)	Ручное управляющее действие по управлению приоритетом голосования (H)
Пример 4 Группа безопасности, содержащая распределенные диверсные защитные функции P, Q, R, использующие различные датчики и исполнительные устройства и одинаковое аппаратное обеспечение в каждом канале управления	

Окончание таблицы С.1

Возможные причины ООП Вероятность: (H) = высокая; (M) = средняя; (L) = низкая	**Возможная защита** Эффективность: (H) = высокая; (M) = средняя; (L) = низкая
Ошибка в спецификации требований к трем функциям (L)	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 (L)	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 Группа безопасности, содержащая 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 (H)
Одновременный отказ аппаратного обеспечения каналов системы вследствие опасного воздействия на станции	То же, что в примере 1
Ошибка в обоих исполнительных действиях по обеспечению безопасности (L)	Различные (дублированные) системы исполнительных устройств (H)

Приложение D
(справочное)

Взаимосвязь настоящего стандарта с серией стандартов МЭК 61508 и стандартами атомной отрасли

D.1 Общие положения

В данном приложении приведено сравнение настоящего стандарта со стандартами МЭК 61508-1:2010, МЭК 61508-2:2010 и МЭК 61508-4:2010.

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 и МЭК 62138.

Настоящее приложение состоит из четырех разделов:

- Раздел D.2 рассматривает основные отличия в областях действия и концепциях двух стандартов;
- Раздел D.3 сравнивает положения настоящего стандарта с МЭК 61508-1 (основные требования);
- Раздел D.4 сравнивает положения настоящего стандарта с МЭК 61508-2 (системные аспекты);
- Раздел D.5 сравнивает положения настоящего стандарта с МЭК 61508-4 (определения).

Сокращения:

E/E/PES — электрическая/электронная/программируемая электронная система;

EUC — контролируемое оборудование;

SIL — уровень полноты безопасности

D.2 Сравнение областей действия и концепций

При сравнении прежде всего рассматриваются некоторые важные отличия областей применения двух стандартов.

Рассматриваемые в серии стандартов МЭК 61508 системы могут быть любыми — электрическими, электронными или программируемыми электронными технологиями и, хотя настоящий стандарт содержит основные требования к архитектуре для всех этих технологий, его основной объект — компьютеризированные системы.

Серия стандартов МЭК 61508 относится к «системам, связанным с безопасностью», тогда как настоящий стандарт следует положениям МАГАТЭ и распространяется на «системы, важные для безопасности» (т. е. важные для ядерной безопасности)[1)].

Примечание — Предполагается, что при проектировании СКУ для АС, которые реализуют традиционные функции безопасности (например, защищенность персонала, защиты объекта, защита от химически опасных факторов и опасных факторов, связанных с производством энергии), будут применяться международные или национальные стандарты, которые основаны на требованиях серии стандартов МЭК 61508.

a) Область общего жизненного цикла безопасности

Общий жизненный цикл по серии стандартов МЭК 61508 включает в себя все системы, предусмотренные проектом безопасности, и контролируемое оборудование, включая СКУ (E/E/PE), системы на основе других технологий, а также устройства, снижающие риск внешнего воздействия.

Настоящий стандарт специально не рассматривает ни анализ безопасности станции, ни средства оценки соответствия требованиям к эксплуатации и надежности, возникающие при анализе. Практики атомной отрасли предназначены для проекта АС, который выполняют в соответствии со специальными принципами МАГАТЭ, правилами МЭК и требованиями национальных регулирующих органов, которые находятся вне области настоящего стандарта. Проектные основы АС определяют ПИС, их последствия, концепцию глубокоэшелонированной защиты АС, категоризацию функций, необходимых для обеспечения защиты. Однако настоящий стандарт описывает требуемую исходную информацию из проектных основ АС и анализа безопасности, которая должна быть доступна разработчикам СКУ для последующей работы над проектом СКУ.

b) Общая валидация/оценка безопасности

В соответствии с требованиями настоящего стандарта общая верификация и валидация каждой распределенной функции, важной для безопасности, описываются в отчете об общей интеграции и вводе в эксплуатацию.

В атомной отрасли экспертиза этого отчета по вопросам безопасности рассматривается в рамках процедуры лицензирования.

c) СКУ и архитектура СКУ

СКУ, рассматриваемые в настоящем стандарте, эквивалентны E/E/PE системам в соответствии с серией стандартов МЭК 61508. В настоящем стандарте архитектура СКУ (см. раздел 5) определяет набор отдельных си-

---

[1)] *В НП-001-15 определено деление систем, важных для безопасности, на системы безопасности и системы нормальной эксплуатации, важные для безопасности.*

стем с определенными классами и требованиями к независимости, которые выполняют функции, важные для безопасности. Для каждой из этих систем раздел 6 настоящего стандарта определяет отдельный жизненный цикл системы. В серии стандартов МЭК 61508 любое разделение на несколько систем рассмотрено в части 2.

Данное различие следует учитывать, чтобы избежать недоразумений.

d) Уровень полноты безопасности и классификация

Серия стандартов МЭК 61508 устанавливает уровень полноты безопасности, требующийся для компьютеризированной системы, в соответствии со степенью снижения риска, которую система должна обеспечить. Это достигается определением серьезности риска, связанного с опасностью, оценкой частоты опасных событий и с защитой, которую должна обеспечить система с целью снижения риска от опасности до допустимого уровня.

Атомная отрасль традиционно использовала детерминистический метод определения значимости системы для безопасности и ее влияние на величину риска, связанного с возможным выходом радиоактивных веществ (см. Руководства по безопасности МАГАТЭ и МЭК 61226).

Самый высокий реальный уровень полноты безопасности обычно необходим для той системы, которая предотвращает или смягчает последствия радиоактивных выбросов. Низкий уровень полноты безопасности может быть приемлемым лишь для вспомогательных систем, которые непосредственно не решают задачи предотвращения или ограничения выбросов. Поэтому не существует эквивалентной схемы с позиций надежности/снижения риска уровней SIL, предложенных в серии стандартов МЭК 61508, для широкого применения в атомном секторе. Такой детерминистический подход в атомной отрасли признается, как правило, 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 цели по обеспечению надежности компьютерных систем.

Назначение функциям безопасности «уровней полноты» по серии стандартов МЭК 61508 практически полностью соответствует категоризации функции ядерной безопасности, применимой в атомной отрасли. Однако имеются существенные различия в процедурных вопросах:

- в серии стандартов МЭК 61508 присвоение уровней полноты безопасности основано на вероятностном анализе опасностей и риска;
- в МЭК 61226 присвоение функциям ядерной безопасности категорий основано на детерминистическом критерии и инженерном опыте оценки последствий в случае отказа.

D.3 Соответствие настоящего стандарта и МЭК 61508-1

МЭК 61508-1	Настоящий стандарт
5 Документация	5.6 Выходная документация
6 Управление функциональной безопасностью	5.5.2 В соответствии с МАГАТЭ GSR (часть 2) и МАГАТЭ GS-G-3.1 вся деятельность, связанная с АС, описывается в программе обеспечения качества или предпочтительно интегрированной системой управления
7 Требования к общему жизненному циклу безопасности	5 Общий жизненный цикл безопасности СКУ
7.1 Общие положения	
Полный жизненный цикл безопасности охватывает E/E/PES, другие технологии, снижение внешнего риска	Общий жизненный цикл систем контроля и управления (жизненный цикл СКУ) охватывает функции СКУ, системы и оборудование, важные для безопасности, и общую архитектуру СКУ [см. пункт а) раздела D.2]
7.2 Концепция	
Описание объектов управления, требуемых функций управления и физического окружения	Рассмотрение проекта АС (5.2): - установление условий окружающей среды (5.2.4); - функции СКУ, важные для безопасности; - действия автоматики и оператора
Определение источников опасности	Внутренние и внешние источники опасности устанавливаются при разработке проекта АС и являются входами для СКУ (5.2.4) (см. пункт а) раздела D.2)
7.3 Определение области действия	
Определение границы EUC	Определить установленные границы станция/СКУ (см. 5.2.4)

Продолжение

МЭК 61508-1	Настоящий стандарт
Определение области опасности и анализа риска, а также событий, приводящих к аварии	События (ПИС) определяются основой проекта АС и являются входами для разработки СКУ [(см. 5.2) [(см. пункт а) раздела D.2]
7.4 Анализ источников опасности и риска	
Определение опасности для EUC...	Не рассматривается настоящим стандартом, является частью основы проекта станции [см. пункт а) раздела D.2]
... и системы управления EUC	Детерминированные ограничения СКУ, например критерий единичного отказа для функций категории А, функциональное разделение, накладываются основой проекта станции
Определение последовательности следствий опасных событий	Последовательности ПИС определяются в проекте АС и являются входом для СКУ (см. 5.2) [см. пункт) раздела D.2]
Определение риска EUC	Категоризация функций СКУ (см. 5.2.3) является входом для СКУ [см. пункт а) раздела D.2]
7.5 Общие требования безопасности	5.3 Общий план защищенности систем и оборудования СКУ
Необходимые функции безопасности являются установленными. Они включают в себя: - спецификацию требований к функциям безопасности; - спецификацию требований к полноте безопасности	Общие спецификации требований к функциям, важным для безопасности, вытекают из основы проекта станции. Они включают в себя: спецификацию требований к функциональности и производительности [см. а) 1) и а) 2) в 5.3]; категоризация функций СКУ [см. а) 3) в 5.3] спецификация требований к независимости [см. b) в 5.3]
Общая спецификация требований к безопасности, охватывающей СКУ (системы E/E/PE), с использованием других технологий, а также к устройствам снижения риска	Другие технология и меры по снижению риска определяются в основе проекта АС в соответствии с принципами глубокоэшелонированной защиты. Они находятся вне области настоящего стандарта [см. пункт а) раздела D.2]
7.6 Распределение требований безопасности	5.4.2 Проектная документация по архитектуре СКУ 5.4.3 Назначение функций системам
Распределение функций безопасности по системам и присвоение уровня полноты безопасности каждой функции. Рассматривается возможность ООП (см. 7.6.2.7) и целевая безопасность для полноты отдельной E/E/PE ограничивается (см. 7.6.2.11)	Разделение общих СКУ на отдельные СКУ соответствующего класса. Распределение функций СКУ по СКУ в соответствии с классификацией, глубокоэшелонированной защитой, принимая во внимание ООП
Общее планирование	5.5 Общее планирование
6 Управление функциональной безопасностью	5.5.2 Общая программа обеспечения качества
7.8 Общее планирование валидации безопасности	5.5.4 Общие планы интеграции и ввода в эксплуатацию
	5.5.3 Общий план защищенности
7.9 Общее планирование установки и ввода в действие	5.5.4 Общие планы интеграции и ввода в эксплуатацию
7.7 Общее планирование эксплуатации и технического обслуживания	5.5.5 Общий план эксплуатации
	5.5.6 Общий план технического обслуживания
7.10 Спецификация требований к безопасности	6.2.2 Спецификация требований к системе
7.11 Реализация: E/E/PES	6 Жизненный цикл безопасности системы
См. МЭК 61508-2 (системные аспекты)	См. раздел 6 (жизненный цикл системы)

Окончание

МЭК 61508-1	Настоящий стандарт
См. МЭК 61508-3 (требования к программному обеспечению)	Программное обеспечение не входит в область данного стандарта
7.12 Другие меры по снижению риска. Спецификация и реализация	Не входит в область данного стандарта [см. пункт а) раздела D.2]
7.13 Общие установка и ввод в эксплуатацию	7 Общая интеграция и ввод в эксплуатацию
7.14 Общая валидация безопасности Валидировать, что E/E/PE удовлетворяет общим спецификациям требований в соответствии с распределением	7.2 Общие требования, необходимые для достижения целей Верифицировать и валидировать функции, важные для безопасности, распределенные более чем по одной системе. 6.5 Квалификация системы
7.15 Общие эксплуатация, техническое обслуживание и ремонт	8 Общая эксплуатация и техническое обслуживание
7.16 Общие модификация и модернизация	1 Область применения Настоящий стандарт (или его часть) применим к СКУ на новых АС так же, как и к реконструируемым и модернизируемым системам на существующих станциях. 6.2.8 Модификация проекта системы
7.17 Снятие с эксплуатации или утилизация	Настоящим стандартом не рассматривается
7.18 Верификация	5.4.1 Общие программы обеспечения качества
8 Оценка функциональной безопасности Исследовать и привести обоснование по функциональной безопасности, достигнутой системами E/E/PE	В атомной отрасли эта оценка связывается с лицензированием и зависит от национальных регулирующих органов

D.4 Соответствие настоящего стандарта и МЭК 61508-2

МЭК 61508-2	Настоящий стандарт
5 Документация	6.4 Выходная документация
6 Управление функциональной безопасностью	5.5.2 Общая программа обеспечения качества
7 Требования к жизненному циклу безопасности систем E/E/PE Структура жизненного цикла безопасности E/E/PE охватывает цели и требования к системам E/E/PE	6 Жизненный цикл безопасности СКУ Структура жизненного цикла безопасности системы включает цели и требования к отдельным СКУ, входящим в архитектуру СКУ [см. пункт с) раздела D.2]
7.1 Общие положения В таблице 1 для каждого этапа приведены цели и требования, области действия этапа, требуемые входы к каждому этапу и требуемые выходы	В таблице 3 для каждого этапа приведены цели и требования, требуемые входы к каждому этапу и требуемые выходы
7.2 Спецификация требований к проекту E/E/PES включает в себя: - требования к функциям безопасности; - требования к полноте безопасности	6.2.2 Спецификация требований к системе включает в себя: - спецификацию требований к прикладным функциям; - спецификацию требований к сервисным функциям; - условия окружающей среды (см. 6.2.2.6); - категоризацию функций СКУ (вход от 5.3); - требования к ограничениям проекта системы (см. 6.2.2.3); - классификацию системы
Примечание — Указанные выше разделы серии стандартов МЭК 61508 и настоящего стандарта охватывают общие положения, но в настоящем стандарте различают требования к функциям СКУ и требования к СКУ, осуществляющим эти функции.	

Окончание

МЭК 61508-2	Настоящий стандарт
7.3 Планирование валидации безопасности E/E/PES	6.3 Разработка документации (планирование) СКУ
	План валидации системы (см. 6.3.5). Функциональная валидация спецификации требований к прикладным функциям (см. 6.2.4.2.1). Квалификация системы (см. 6.5)
7.4 Проектирование и разработка E/E/PES	6.2.3 Спецификация системы 6.2.4 Детальное проектирование и реализация системы
7.4.2 Общие требования	Ограничения проекта (см. 6.2.2.3). Структура системы (см. 6.2.2.3). Документация по спецификации системы (см. 6.4.3)
7.4.3 Синтез элементов для обеспечения требуемой стойкости к систематическим отказам	Цикл безопасности системы (см. раздел 6). Требования к ограничениям проекта (см. 6.2.2.3)
7.4.4 Архитектурные ограничения полноты безопасности аппаратных средств	Требования к ограничениям проекта (см. 6.2.2.3)
7.4.5 Требования к количественной оценке случайных отказов аппаратных средств	Оценка надежности (см. 6.2.4.2.2)
7.4.6 Требования по предотвращению систематических отказов 7.4.7 Требования по управлению систематическими сбоями	Разработка архитектуры СКУ (см. 5.4.2), относительно принципа глубокоэшелонированной защиты. Оценка надежности и защиты от ООП (см. 5.4.4.2). Оценка человеческих факторов (см. 5.4.4.3). Распределение подсистем по помещениям (см. 6.2.3.3.2). Независимость (см. 6.2.3.3.3). Защита от развития отказов и их побочных эффектов (см. 6.2.3.3.4)
7.4.8 Требования к поведению системы при обнаружении отказов	- структура системы (см. 6.2.2.3.2); - самотестирование и устойчивость к отказам (см. 6.2.2.3.4)
7.4.9 Требования к реализации E/E/PES	- выбор существующих компонентов (см. 6.2.3.2)
7.4.10 Требования к проверенным в эксплуатации элементам	- выбор существующих компонентов (см. 6.2.3.2) с ссылками на отдельные стандарты МЭК 60880, МЭК 62138, МЭК 60987
7.4.11 Дополнительные требования к передаче данных	- средства передачи данных (см. 5.4.2.4), связано с МЭК 61500; - внутреннее поведение системы (см. 6.2.2.3.3)
7.5 Интеграция E/E/PES	6.2.5 Интеграция системы
7.6 Процедуры эксплуатации и технического обслуживания E/E/PES	6.3.7 План эксплуатации системы
7.7 Валидация функциональной безопасности E/E/PES	6.2.6 Валидация системы
7.8 Модификация E/E/PES	6.2.8 Модификация системы
7.9 Верификация E/E/PES	6.3.2.2 План верификации системы
8 Оценка функциональной безопасности (см. МЭК 61508-1)	См. раздел D.3

D.5 Соответствия между некоторыми важными терминами и определениями в области ядерных технологий, приведенными в настоящем стандарте и МЭК 61508-4

Тема: анализ риска	
МЭК 61508-4	Настоящий стандарт
3.1.2 **опасность:** Потенциальный источник причинения вреда (ИСО/МЭК Руководство 51) [19]. 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)	3.25 **опасность**

Тема: глубокоэшелонированная защита	
МЭК 61508-4	Настоящий стандарт
3.4.2 **другое устройство снижения риска:** Средство снижения и ослабления риска, отдельное и отличное от E/E/PE систем, связанных с безопасностью, и не использующее E/E/PE системы, связанные с безопасностью	**концепция глубокоэшелонированной защиты** (см. раздел А.4) Концепция снижения риска обязательно реализуется при анализе безопасности атомной станции с концепцией глубокоэшелонированной защиты и линий (барьеров) защиты

Тема: системы, важные для безопасности	
МЭК 61508-4	Настоящий стандарт
3.4.1 **система, связанная с безопасностью:** Система, которая: - реализует необходимые функции безопасности, требующиеся для достижения и поддержки безопасного состояния управляемого оборудования, и - предназначена для достижения своими средствами или в сочетании с другими E/E/PE системами, связанными с безопасностью, и другими средствами снижения риска необходимой полноты безопасности для требуемых функций безопасности	3.33 **узел, важный для безопасности**

Тема: СКУ	
МЭК 61508-4	Настоящий стандарт
3.2.13 **электрическая/электронная/программируемая электронная система (E/E/PE):** Система, основанная на электрической (Э) и/или электронной (Э) и/или программируемой электронной (ПЭ) технологии	3.29 **СКУ**

Тема: надежность	
МЭК 61508-4	Настоящий стандарт
3.5.4 **полнота безопасности:** Вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности при всех оговоренных условиях в течение заданного интервала времени. Примечание 3 — При определении полноты безопасности должны учитываться все причины отказов (случайных отказов аппаратных средств и систематических отказов), которые приводят к небезопасному состоянию, например отказы аппаратных средств, отказы, вызванные программным обеспечением, и отказы, вызванные электрическими помехами. Некоторые из этих типов отказов, например случайные отказы аппаратных средств, могут быть охарактеризованы количественно, с использованием таких параметров, как интенсивность отказов в опасном режиме или вероятность того, что система защиты, связанная с безопасностью, не сможет выполнить запрос. Однако полнота безопасности системы также зависит и от многих факторов, которым невозможно дать точную количественную оценку и которые могут быть оценены только качественно	3.43 **надежность:** В настоящем стандарте надежность оценивается обычно на основе качественных представлений (см. 6.2.2.2 и 6.2.4.2.2)

Тема: классификация систем, важных для безопасности	
МЭК 61508-4	Настоящий стандарт
3.5.8 **уровень полноты безопасности:** Дискретный уровень (принимающий одно из четырех возможных значений), соответствующий диапазону значений полноты безопасности, при котором уровень полноты безопасности, равный 4, является наивысшим уровнем полноты безопасности, а уровень полноты безопасности, равный 1, соответствует наименьшей полноте безопасности	3.6 **класс СКУ:** Все компоненты, конструкции 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 78 МАГАТЭ 75-INSAG-3:1999). 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. разделы 174—176 МАГАТЭ 75-INSAG-3:1999)

Тема: отказ по общей причине	
МЭК 61508-4	Настоящий стандарт
3.6.10 **отказ по общей причине:** Отказ, являющийся результатом одного или нескольких событий, вызвавших одновременные отказы двух и более отдельных каналов в многоканальной системе, ведущих к отказу системы. Примечание — В подразделах 7.6.2.7 и 7.6.2.8 МЭК 61508-1:2010 приводятся требования к независимости двух систем	3.8 **отказ по общей причине:** См. 5.4.2.6

Приложение Е
(справочное)

Изменения, которые следует внести в последующие издания стандартов подкомитета ПК 45 А для их адаптации с настоящей версией МЭК 61513

МЭК 60880:2006	Изменение, которое должно быть внесено
3 Термины и определения	Определения необходимо привести в соответствие
6.3 Тестирование	Удалить все, кроме 6.3.1 и 6.3.2. Заменяется 6.2.2.3.5 МЭК 61513
9.3 Верификация интегрированной системы	Удалить подраздел. Заменяется 6.2.5 и 6.3.4 МЭК 61513
9.4 Процедура устранения дефектов	Удалить подраздел. Заменяется 6.3.2.4 МЭК 61513
9.5 Программные аспекты отчета о верификации интегрированной системы	Удалить подраздел. Заменяется 6.4.5 МЭК 61513
10.1 Программные аспекты плана валидации системы	Удалить подраздел. Заменяется 6.2.6 и 6.3.5 МЭК 61513
10.3 Программные аспекты отчета о валидации системы	Удалить подраздел. Заменяется 6.4.6 МЭК 61513
10.4 Процедура устранения дефектов	Удалить подраздел. Заменяется 6.3.2.4 МЭК 61513
12.4 Обучение оператора	Удалить подраздел. Заменяется 5.5.7 МЭК 61513

МЭК 62138.2004	Изменение, которое должно быть внесено
3 Термины и определения	Определения необходимо привести в соответствие
5.6 и 6.6 Программные аспекты интеграции системы	Предполагается удаление раздела. Заменяется 6.2.5 и 6.3.4 МЭК 61513
5.7 и 6.7 Программные аспекты валидации системы	Предполагается удаление. Заменяется 6.2.6 и 6.3.5 МЭК 61513

МЭК 61226.2009	Изменение, которое должно быть внесено
3 Термины и определения	Определения необходимо привести в соответствие
Новое приложение	Принять содержание приложения В

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 60671	—	*
IEC 60709	IDT	ГОСТ Р МЭК 60709—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
IEC 60780	—	*
IEC 60880:2006	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
IEC 60964:2009	IDT	ГОСТ Р МЭК 60964—2012 «Атомные станции. Пункты управления. Проектирование»
IEC 60965	IDT	ГОСТ Р МЭК 60965—2020 «Резервный пункт управления атомной станции, используемый при отказе блочного пункта управления. Общие требования»
IEC 60980	—	*
IEC 60987:2007	—	*
IEC 61000-4-1	IDT	ГОСТ Р 51317.4.1—2000 (МЭК 61000-4-1—2000) «Совместимость технических средств электромагнитная. Испытания на помехоустойчивость. Виды испытаний»
IEC 61000-4-2	MOD	ГОСТ 30804.4.2—2013 (IEC 61000-4-2:2008) «Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний»
IEC 61000-4-3	MOD	ГОСТ 30804.4.3—2013 (IEC 61000-4-3:2006) «Совместимость технических средств электромагнитная. Устойчивость к радиочастотному электромагнитному полю. Требования и методы испытаний»
IEC 61000-4-4	MOD	ГОСТ 30804.4.4—2013 (IEC 61000-4-4:2004) «Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Требования и методы испытаний»
IEC 61000-4-5	IDT	ГОСТ Р 51317.4.5—99 (МЭК 61000-4-5—95) «Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Требования и методы испытаний»
IEC 61000-4-6	IDT	ГОСТ Р 51317.4.6—99 (МЭК 61000-4-6—96) «Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам, наведенным радиочастотными электромагнитными полями. Требования и методы испытаний»
IEC 61226:2009	IDT	ГОСТ Р МЭК 61226—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 61500	IDT	ГОСТ Р МЭК 61500—2012 «Атомные станции. Системы контроля и управления, важные для безопасности. Передача данных в системах, выполняющих функции категории А»
IEC 61508-2:2010	IDT	ГОСТ Р МЭК 61508-2—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам»
IEC 61508-4:2010	IDT	ГОСТ Р МЭК 61508-4—2012 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения»
IEC 62138:2004	IDT	ГОСТ Р МЭК 62138—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С»
IEC 62340	—	*
ISO 9001:2008	IDT	ГОСТ Р ИСО 9001—2008 «Системы менеджмента качества. Требования»[1)]
IAEA INSAG-10:1996[2)]	—	*
IAEA NS-R-1:2000[2)]	—	*
IAEA GS-R-3:2006[2)]	—	*
IAEA GS-G-3.1:2006[2)]	—	*
IAEA NS-G-1.3:2002[2)]	—	*
IAEA 75-INSAG-3 Rev.1 — INSAG 12:1999[2)]	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:
- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

[1)] Действует ГОСТ Р ИСО 9001—2015, идентичный ИСО 9001:2015.

[2)] Перевод документа на русском языке доступен на gost.e-ecolog.ru

Библиография

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

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

[3] IAEA Safety Glossary — Terminology used in Nuclear Energy and Radiation Protection — 2007 Edition

[4] IEEE 610:1992, IEEE standard Computer Dictionary, Compilation of IEEE Standard Computer Glossaries

[5] 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

[6] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary

[7] ISO 8402:1994, Quality management and quality assurance — Vocabulary

[8] ISO/IEC Directives, Part 2, 2004, Part 2: Rules for the structure and drafting of International Standards

[9] ISO/IEC 12207:2008, Systems and software engineering — Software life cycle processes

[10] IEC 60050-394:2007, International Electrotechnical Vocabulary — Part 394: Nuclear instrumentation — Instruments, systems, equipment and detectors

[11] IEC 62381, Automation systems in the process industry — Factory acceptance test (FAT), Site acceptance test (SAT), and Site integration test (SIT)

[12] IEC 62342, Nuclear power plants — Instrumentation and control systems important to safety — Management of ageing

[13] IEC 61000-6-2, Electromagnetic compatibility (EMC) — Part 6-2: Generic Standards — Immunity for industrial environments

[14] IEC 61000-6-4, Electromagnetic compatibility (EMC) — Part 6-4: Generic Standards — Emission standard for industrial environments

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

[16] IEC 61225, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for electrical supplies

[17] ISO 10007, Quality management systems — Guidelines for configuration management

[18] IEEE 828, IEEE Standard for Software Configuration Management Plans

[19] ISO/IEC Guide 51:1990, Guidelines for the inclusion of safety aspects in standards

УДК 774:002:006.354 ОКС 27.120.20

Ключевые слова: автоматизированные системы управления

БЗ 1—2020/62

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 20.02.2020. Подписано в печать 06.03.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 10,23. Уч.-изд. л. 8,70.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru