ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 60744—2023

Атомные станции

ЛОГИЧЕСКИЕ УСТРОЙСТВА, ИСПОЛЬЗУЕМЫЕ В СИСТЕМАХ БЕЗОПАСНОСТИ, ВЫПОЛНЯЮЩИХ ФУНКЦИИ КАТЕГОРИИ А

Характеристики и методы испытаний

(IEC 60744:2018, Nuclear power plants — Instrumentation and control systems important to safety — Safety logic assemblies used in systems performing category A functions: Characteristics and test methods, IDT)

Издание официальное

Москва
Российский институт стандартизации
2023

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 9 октября 2023 г. № 1086-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 60744:2018 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Логические устройства обеспечения безопасности в системах, выполняющих функции категории А. Характеристики и методы испытаний» (IEC 60744:2018 «Nuclear power plants — Instrumentation and control systems important to safety — Safety logic assemblies used in systems performing category A functions: Characteristics and test methods», 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 стандарты, сведения о которых приведены в дополнительном приложении ДА.

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

5 ВВЕДЕН ВПЕРВЫЕ

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

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

© IEC, 2018
© Оформление. ФГБУ «Институт стандартизации», 2023

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
2 Нормативные ссылки . . . 2
3 Термины и определения . . . 3
4 Обозначения и сокращения . . . 6
5 Принципы и описание логических устройств . . . 7
5.1 Логическое устройство . . . 7
5.2 Технология проектирования логического устройства . . . 7
5.3 Интерфейсы логического устройства . . . 8
5.4 Показатели надежности . . . 10
5.5 Режимы функционирования . . . 10
5.6 Принципы достижения целей безопасности . . . 10
5.7 Принципы достижения готовности . . . 11
6 Проектные требования к логическим устройствам . . . 12
6.1 Общие положения . . . 12
6.2 Функции . . . 12
6.3 Архитектура и резервирование . . . 13
6.4 Технология . . . 13
6.5 Квалификация . . . 13
6.6 Обслуживание . . . 14
6.7 Разделение . . . 14
6.8 Энергообеспечение . . . 15
7 Испытания логических устройств . . . 15
7.1 Общие положения . . . 15
7.2 Типовые испытания . . . 15
7.3 Производственные испытания . . . 16
7.4 Испытания на месте эксплуатации . . . 17
8 Обеспечение качества . . . 17
Приложение А (справочное) Примеры применения логического устройства . . . 18
Приложение В (обязательное) Логическое устройство как аппаратно-реализованное технологическое решение . . . 19
Приложение С (справочное) Надежность и ее характеристики . . . 22
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов межгосударственным и национальным стандартам . . . 24
Библиография . . . 29

Введение

a) Техническая справка, основные вопросы и организация настоящего стандарта

Настоящий стандарт посвящен логическим устройствам безопасности, используемым на атомных станциях (АС). Логические устройства первоначально были встроены в системы защиты, использовавшиеся, в основном, для управления исполнительными механизмами. В МЭК 60744 основное внимание уделяется проектированию, а также техническим решениям, интерфейсам с блочным пунктом управления (БПУ) и резервным пунктом управления (РПУ), испытаниям и квалификации. Также изложены требования к отображению входных данных и состояния систем безопасности.

МЭК 60744 является документом, в котором рассматриваются функции и рабочие характеристики логического устройства безопасности.

Применение компьютеризированного оборудования или программного обеспечения всесторонне освещено в других стандартах. Из технических средств при проектировании логических устройств (SLA) используют главным образом аппаратно реализуемые технологии и субмикронные высокоинтегрированные компоненты (HPD), применение которых ограничено из-за очень высоких требований безопасности.

Стандарт рассматривает проектные и испытательные характеристики логических устройств безопасности, уделяя особое внимание функциональным требованиям, вопросам надежности и сопряженным с логическими устройствами средствам управления, в том числе средствам сигнализации, индикации и контроля. Стандарт также содержит требования к функционированию, испытаниям и квалификации логических устройств и требования к интерфейсам для взаимодействия между устройствами.

Настоящий стандарт предназначен для использования операторами АС (энергетическими компаниями), экспертами-системотехниками и лицензирующими органами.

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

Среди документов, находящихся в ведении ПК 45А, МЭК 60744 является документом третьего уровня, посвященным конкретному вопросу проектируемых и контролируемых характеристик логических устройств безопасности.

МЭК 60744 следует рассматривать совместно с МЭК 61513, также находящимся в ведении МЭК ПК 45А, содержащим требования к системам контроля и управления (СКУ), важным для безопасности АС, а также с МЭК 60964, содержащим требования к пунктам управления АС, поскольку система безопасности тесно сопряжена с БПУ и РПУ.

Более подробная информация о структуре серий стандартов МЭК ПК 45А представлена в пункте d) настоящего введения.

c) Рекомендации и ограничения, касающиеся применения настоящего стандарта

Следует отметить, что настоящий стандарт не устанавливает дополнительные функциональные требования на уровне систем безопасности.

Настоящий стандарт содержит конкретные рекомендации по следующим аспектам:

- принятие решения по частичным отключениям для выявления каждого срабатывания системы безопасности;
- выходные устройства, подающие сигналы отключения и срабатывания;
- проектные и подлежащие испытаниям параметры функциональных требований;
- надежность логических устройств безопасности;
- функциональные характеристики логических устройств;
- требования к испытаниям, квалификации и интерфейсам логических устройств безопасности.

Чтобы настоящий стандарт и далее оставался актуальным, его положения акцентированы на принципиальных вопросах, а не на конкретных технологиях.

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

Стандартами самого высокого уровня серии стандартов ПК 45А МЭК являются МЭК 61513 и МЭК 63046. МЭК 61513 содержит общие требования к СКУ и оборудованию, используемым для выполнения важных для безопасности АС функций. МЭК 63046 содержит общие требования к электроэнергетическим системам АС и распространяется на системы электроснабжения, включая системы питания СКУ. МЭК 61513 и МЭК 63046 следует рассматривать вместе и на одном уровне. МЭК 61513 и МЭК 63046 формируют структуру серии стандартов ПК 45А МЭК и устанавливают полный набор общих требований к системам контроля и управления и к электротехническим системам атомных станций.

МЭК 61513 и МЭК 63046 содержат прямые ссылки на другие стандарты ПК 45А МЭК по общим вопросам, связанным с категоризацией функций и классификацией систем, квалификацией, разделением, защитой от отказов по общим причинам, проектированием пунктов управления, электромагнитной совместимостью, кибербезопасностью, программными и аппаратными аспектами программируемых цифровых систем, согласованием требований безопасности и защиты информации и управлением старением. Стандарты, на которые напрямую ссылаются МЭК 61513 и МЭК 63046, являющиеся стандартами второго уровня, следует рассматривать вместе с МЭК 61513 и МЭК 63046, как единый комплект документов.

Третий уровень стандартов ПК 45А МЭК составляют стандарты, на которые отсутствуют прямые ссылки в МЭК 61513 или МЭК 63046, относящиеся к конкретному оборудованию, техническим методам или определенным видам деятельности. Как правило, эти стандарты, содержащие ссылки на стандарты второго уровня по общим темам, могут быть использованы самостоятельно.

Четвертый уровень документов ПК 45А МЭК представлен техническими отчетами, которые не являются нормативными документами.

Серия стандартов ПК 45А МЭК постоянно реализует и детализирует принципы безопасности и защиты информации, а также базовые аспекты, содержащиеся в соответствующих стандартах безопасности МАГАТЭ и соответствующей серии документов МАГАТЭ по ядерной безопасности (NSS). В частности, к этим документам относятся нормы безопасности МАГАТЭ SSR-2/1, устанавливающие требования безопасности, связанные с проектированием АС, руководство по безопасности МАГАТЭ SSG-30, в котором рассмотрена классификация безопасности конструкций, систем и компонентов АС, руководство по безопасности МАГАТЭ SSG-39, относящееся к проектированию систем контроля и управления АС, руководство по безопасности МАГАТЭ SSG-34, рассматривающее проектирование электроэнергетических систем для АС, а также внедряемое руководство NSS17 по компьютерной безопасности оборудования атомных станций. Термины и определения, используемые в стандартах ПК 45А по безопасности и защите информации, соответствуют терминам и определениям, используемым в документах МАГАТЭ.

МЭК 61513 и МЭК 63046 представлены в том же формате, что и основной стандарт по безопасности МЭК 61508, с той же схемой жизненного цикла в целом и схемой жизненного цикла системы. В отношении ядерной безопасности МЭК 61513 и МЭК 63046 содержат толкование основных требований, действующих в атомной энергетике и изложенных в МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4. В этой структуре МЭК 60880, МЭК 62138 и МЭК 62566 соответствуют МЭК 61508-3 для атомной энергетики. МЭК 61513 и МЭК 63046 содержат ссылки на документы ИСО, а также на документы МАГАТЭ GS-R-3, МАГАТЭ GS-G-3.1 и МАГАТЭ GS-G-3.5 по вопросам, связанным с обеспечением качества (ОК). На втором уровне по вопросам ядерной безопасности вводным документом для серии стандартов по безопасности ПК 45А МЭК является МЭК 62645. Он основан на действующих принципах высокого уровня и главных концепциях стандартов по безопасности, в частности ИСО/МЭК 27001 и ИСО/МЭК 27002. МЭК 62645 адаптирует и дополняет их применительно к атомной отрасли и приводит в соответствие с серией стандартов МЭК 62443. По пунктам управления на втором уровне первичным документом среди стандартов ПК 45А МЭК является МЭК 60964, а по вопросам управления старением — МЭК 62342.

Примечания

1 Предполагается, что при проектировании систем контроля и управления АС, реализующих стандартные функции безопасности (например, обеспечение безопасности работников, защита объекта, химическая безопасность, энергетическая безопасность технологических процессов), будут применяться международные или национальные стандарты.

2 В 2013 г. расширена сфера ответственности ПК 45А МЭК, которая распространилась также на электрические системы. В 2014 и 2015 гг. в ПК 45А МЭК проведены дискуссии с целью принятия решения о том, каким образом и где следует учитывать общие требования к проектированию электрических систем. Эксперты ПК 45А МЭК рекомендовали разработать независимый стандарт такого же уровня, как и МЭК 61513, устанавливающий общие требования к электрическим системам. В настоящее время для решения этой задачи начата работа над проектом МЭК 63046, и когда он будет опубликован, примечание 2 во введении стандартов подкомитета ПК 45А МЭК будет исключено.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Атомные станции

ЛОГИЧЕСКИЕ УСТРОЙСТВА, ИСПОЛЬЗУЕМЫЕ В СИСТЕМАХ БЕЗОПАСНОСТИ, ВЫПОЛНЯЮЩИХ ФУНКЦИИ КАТЕГОРИИ А

Характеристики и методы испытаний

Nuclear power plants.
Logic assemblies used in safety systems performing category A functions.
Characteristics and test methods

Дата введения — 2023—12—01

1 Область применения

Настоящий стандарт устанавливает требования и рекомендации к проектированию, конструкции и испытаниям логических устройств, используемых в системах безопасности для выполнения функций безопасности категории А (в соответствии с МЭК 61226). Логические устройства безопасности представляют собой логические схемы, такие как аппаратно-реализованный логический узел, обеспечивающий взаимодействие компьютеризированных систем с распределительными устройствами, исполнительными механизмами или контакторами для осуществления отключений или срабатывания технических средств безопасности. Логические устройства являются значимой частью систем безопасности, способной применять мажоритарную логику при обработке сигналов резервных каналов.

Настоящий стандарт содержит общее описание логических устройств безопасности для управления исполнительными механизмами защиты. В стандарте представлены принципы достижения целей надежности, описаны и разъяснены основные особенности, относящиеся к проектным требованиям.

Представлены различные испытания и их требования, позволяющие оценивать правильность проекта (в том числе квалификационные испытания), изготовления, а также корректность установки на месте.

В приложении А представлен перечень возможных применений логических устройств.

В приложении В приведен перечень возможных аппаратно-реализуемых технологий с соответствующими требованиями к проектированию логических устройств.

Приложение С содержит пояснение понятия надежности и ее характеристик с целью повышения работоспособности и снижения конечного риска, ставящего под угрозу безопасность и готовность АС.

В область применения настоящего стандарта не входит проектирование системы защиты, здесь рассмотрены только технологические и архитектурные решения, необходимые для проектирования логического устройства. Проектирование систем безопасности с использованием логических устройств рассматривают в МЭК 61513.

Отдельные детали и конкретные функции, реализуемые логическим устройством, сильно зависят от проекта каждого отдельного ядерного реактора и в настоящем стандарте не рассматриваются.

Поскольку положения настоящего стандарта относятся к части системы, осуществляющей контроль и управление, конечная мажоритарная логика в отношении выключателей питания исключена из области применения настоящего стандарта.

Издание официальное

2 Нормативные ссылки

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

IEC 60255 (all parts), Measuring relays and protection equipment [Реле измерительные и защитное оборудование (все части)]

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

IEC 60709, Nuclear power plants — Instrumentation and control systems important to safety — Separation (Атомные станции. Системы контроля и управления, важные для безопасности. Разделение)[1)]

IEC/IEEE 60780-323, Nuclear facilities — Electrical equipment important to safety — Qualification (Объекты использования атомной энергии. Электрооборудование, важное для безопасности. Квалификация)

IEC 60812, Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA) (Методы анализа надежности систем. Метод анализа видов и последствий отказа)[2)]

IEC 60964, Nuclear power plants — Control rooms — Design (Атомные станции. Пункты управления. Проектирование)

IEC 60965, Nuclear power plants — Control rooms — Supplementary control room for reactor shutdown without access to the main control room (Атомные станции. Пункты управления. Резервный пункт управления для останова 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 (Рекомендуемая практика проведения сейсмической квалификации электрооборудования системы безопасности для атомных электростанций)[3)]

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

IEC 61225, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for electrical supplies (Атомные станции. Системы контроля и управления, важные для безопасности. Требования к электроснабжению)[4)]

IEC 61226, Nuclear power plants — Instrumentation and control systems important to safety — Classification of instrumentation and control functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления)[5)]

IEC 61227, Nuclear power plants — Control rooms — Operator controls (Атомные станции. Пункты управления. Органы управления оператора)

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

IEC 62003, Nuclear power plants — Instrumentation and control important to safety — Requirements for electromagnetic compatibility testing (Атомные станции. Системы контроля и управления, важные для безопасности. Требования к испытаниям на электромагнитную совместимость)[6)]

IEC 62241, Nuclear power plants — Main control room — Alarm functions and presentation (Атомные электростанции. Блочный пункт управления. Функции и представление сигнализации)

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

---

[1)] Заменен на IEC 60709:2018 «Nuclear power plants — Instrumentation, control and electrical power systems important to safety — Separation».

[2)] Заменен на IEC 60812:2018 «Failure modes and effects analysid (FMEA and FMECA)».

[3)] Заменен на IEC/IEEE 60980-344:2020 «Nuclear facilities — Equipment important to safety — Seismic qualification».

[4)] Заменен на IEC 61225:2019 «Nuclear power plants — Instrumentation, control and electrical power systems — Requirements for static uninterruptible DC and AC power supply systems».

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

[6)] Заменен на IEC 62003:2020 «Nuclear power plants — Instrumentation, control and electrical power systems — Requirements for electromagnetic compatibility testing».

ции. Системы контроля и управления, важные для безопасности. Разработка HDL-программируемых интегральных схем для систем, выполняющих функции категории А)

IAEA-GSR Part 2, Leadership and Management for Safety (Общие требования МАГАТЭ по безопасности. Часть 2. Руководство и управление в целях обеспечения безопасности)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **готовность** (availability): Способность объекта или системы выполнять требуемые функции в заданных условиях, в заданный момент или период времени при условии, что все необходимые внешние ресурсы обеспечены.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.2 **канал** (channel): Совокупность взаимосвязанных элементов в системе, которая выдает один выходной сигнал.

Примечание — Канал теряет свою идентичность, когда одиночные выходные сигналы объединяются с сигналами, поступающими от других каналов (например, от контрольно-измерительного канала или канала исполнительного средства защиты).

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.3 **надежность** (dependability): Общий термин, применяемый для обозначения всесторонней надежности системы; т. е. степень, в которой этой системе можно оправданно доверять.

Примечания

1 Работоспособность, готовность и безопасность являются характеристиками надежности.

2 Разъяснения, касающиеся данного определения, приведены в приложении С.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.4 **оборудование с динамическими логическими схемами** (dynamic logic equipment): Системный узел или подузел, использующий динамические логические сигналы.

3.5 **динамический логический сигнал** (dynamic logic signal): Периодически изменяющееся напряжение или ток при частоте, согласующейся с требуемым временем отклика системы.

Примечания

1 Одно логическое состояние может быть связано с отсутствием периодического изменения такого сигнала.

2 Различные логические состояния связаны с различными значениями одного или более параметров периодического изменения, например амплитуды, крутизны, частоты повторения импульсов, направления изменений или импульсного кодирования.

3.6 **техническое средство безопасности** (engineered safety feature): Исполнительная часть системы безопасности (исполнительный механизм, связанный с ее электрической и приводной частью).

Примечание — Техническим средствам безопасности необходима энергия для функционирования (клапаны, приводы и т. д.). Обычно их противопоставляют выключателям аварийной защиты ядерного реактора, которым не нужна энергия для функционирования.

3.7 **отказ** (failure): Потеря способности конструкции, системы или компонента функционировать в соответствии с критериями приемлемости[1)].

Примечания

1 Отказ конструкции, системы или компонента признают в случае, если они оказываются неспособными функционировать независимо от того, есть ли в этом необходимость в данный момент времени. Отказ, например, резервной системы, может не проявиться до тех пор, пока не возникнет необходимость в ее функционировании во время испытаний или при отказе системы, которую она дублирует.

2 Отказ конструкции, системы или компонента является событием, приводящим к ошибке конструкции, системы или компонента.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

---

1) *Согласно ГОСТ Р 27.102—2021, статья 36: «отказ: Событие, заключающееся в нарушении работоспособного состояния объекта. Примечания: Отказ может быть полным или частичным. Полный отказ характеризуется переходом объекта в неработоспособное состояние. Частичный отказ характеризуется переходом объекта в частично неработоспособное состояние».*

3.8 **программируемая логическая интегральная схема;** ПЛИС (Field Programmable Gate Array, FPGA): Интегральная схема, которую может запрограммировать на месте производитель СКУ.

Примечания

1 ПЛИС включает в себя программируемые логические блоки (комбинаторные или последовательностные), программируемые схемы соединения между ними и программируемые блоки для входных и/или выходных сигналов. Его функцию определяет проектировщик СКУ, а не поставщик интегральных схем[1)].

2 Хотя ПЛИС по существу являются цифровыми устройствами, некоторые из них могут включать в состав преобразователи аналоговых входных/выходных сигналов и аналого-цифровые преобразователи. ПЛИС могут включать такие усовершенствованные цифровые функции, как функции аппаратных умножителей, выделенную память, память встраиваемых процессоров.

[МЭК 62566:2012, пункт 3.5]

3.9 **язык описания аппаратных средств;** HDL (hardware description language, HDL): Язык, используемый для формального описания функций и/или конструкции электронного элемента с целью документирования, моделирования или синтеза.

[МЭК 62566:2012, пункт 3.6]

3.10 **HDL-программируемое устройство;** HPD (HDL-Programmed Device, HPD): Интегральная схема, конфигурированная (для систем контроля и управления АС) с использованием языков описания аппаратных средств и сопутствующих программных инструментов.

[МЭК 62566:2012, пункт 3.7]

3.11 **эксплуатационные состояния** (operational states): Состояния АС, определяемые в условиях нормальной эксплуатации и в условиях ожидаемых нарушений нормальной эксплуатации.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.12 **сигнал частичного отключения** (partial trip signal): Двоичный сигнал канала системы безопасности, полученный после обработки сигналов от датчиков этого канала, до его конечной обработки с применением мажоритарной логики и выдачи требования аварийного останова ядерного реактора или срабатывания технических средств безопасности.

3.13 **программируемое логическое устройство;** ПЛУ (programmable logic device, PLD): Интегральная микросхема, состоящая из логических элементов с рисунком межсоединений, части которой программирует пользователь.

Примечания

1 Существуют различные виды ПЛУ, например ПЛУ с возможностью стирания или сложные ПЛУ (СПЛУ).

2 Различия между ПЛИС и ПЛУ определены нечетко, но ПЛУ обычно относят к более простым устройствам, чем ПЛИС.

[МЭК 62566:2012, пункт 3.13]

3.14 **аттестованный ресурс** (qualified life): Период, в течение которого конструкция, система или компонент демонстрируют посредством испытаний, анализа или на основе опыта способность функционировать в пределах критериев приемлемости при возникновении особых условий эксплуатации, сохраняя при этом способность выполнять свои функции безопасности в случае проектной аварии или проектного землетрясения[2), 3)].

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

---

1) *ПЛИС обладают всеми достоинствами специализированных интегральных схем, но не требуют значительных затрат времени на разработку и изготовление. Однако без надлежащих средств проектирования все указанные преимущества ПЛИС ничего не значат. Эти средства проектирования не только должны быть простыми в применении, надежными и эффективными, но им нельзя также отставать в своем развитии от развития и совершенствования различных приборов данного класса. Особенно важную роль играет то обстоятельство, что средства проектирования схем на ПЛИС должны быть хорошо объединены и состыкованы со всеми остальными средствами проектирования и конструирования схемных плат. Например, важную роль при выявлении проектных ошибок играет совместное функциональное моделирование ПЛИС со всеми остальными компонентами схемной платы.*

2) *Согласно ГОСТ Р 27.102—2021, статья 27: «ресурс: Суммарная наработка объекта от начала его эксплуатации или ее возобновления после ремонта до момента достижения объектом предельного состояния».*

3) *Согласно НП-096-15, приложение № 1, пункт 1: «Выработанный ресурс — изменение значений ресурсных характеристик оборудования и трубопроводов от начала их эксплуатации до текущего момента эксплуатации (или контроля их технического состояния)»; пункт 7: «Остаточный ресурс — разность между установленным и выработанным ресурсом».*

3.15 **резервирование** (redundancy): Обеспечение альтернативных (идентичных или отличающихся) конструкций, систем и компонентов для того, чтобы любая отдельная конструкция, система или компонент могли выполнять требуемую функцию независимо от эксплуатационного состояния или отказа любых других[1].

Примечание — В контексте настоящего стандарта это определение нуждается в пояснениях:
- не отличающееся резервирование учитывает риск одиночного (случайного) отказа;
- отличающееся резервирование учитывает риск случайного отказа или отказа по общим причинам.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.16 **работоспособность** (reliability): Вероятность того, что устройство, система, компонент или техническое средство будет удовлетворять минимальным эксплуатационным требованиям, когда возникнет такая необходимость[2].

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.17 **безопасность (ядерная)** [safety (nuclear)]: Защита людей и окружающей среды от радиационных рисков и обеспечение безопасности установок и деятельности, связанных с радиационными рисками[3], [4].

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.18 **функция безопасности** (safety function): Конкретная цель, которая должна быть достигнута для обеспечения безопасности, заключающаяся в предотвращении или уменьшении последствий радиоактивных выбросов от оборудования или видов деятельности в условиях нормальной эксплуатации, ожидаемых нарушений нормальной эксплуатации или аварийных ситуаций[5], [6].

Примечания

1 Нормы безопасности МАГАТЭ SSR-2/1 устанавливают требования к функциям безопасности, которые должны быть удовлетворены при проектировании АС, чтобы проект соответствовал трем основным требованиям безопасности:

a) возможность безопасного останова ядерного реактора и поддержания его в безопасном остановленном состоянии во время соответствующих эксплуатационных состояний и аварийных условий, а также после них;

b) возможность отводить остаточное тепло из активной зоны реактора, от реакторной установки и ядерного топлива в хранилищах после останова ядерного реактора, во время соответствующих эксплуатационных состояний и аварийных условий, а также после них;

c) способность снижать потенциальную возможность выброса радиоактивных материалов и обеспечивать удерживание любых выбросов в предписанных пределах во время эксплуатационных состояний и после них, а также в допустимых пределах во время проектных аварий и после них.

2 В МЭК 61226 даны рекомендации, связанные с категориями функций безопасности.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

---

[1] *Согласно НП-001-15, приложение № 2: «Принцип резервирования (избыточности) — 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».*

[2] *Согласно ГОСТ Р 27.102—2021, статья 5: «надежность (объекта): Свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность объекта выполнять требуемые функции в заданных режимах, условиях применения, стратегиях технического обслуживания, хранения и транспортирования».*

[3] *Согласно ГОСТ 26392—84, статья 1: «ядерная безопасность — Свойство ядерного объекта, обусловливающее с определенной вероятностью невозможность ядерной аварии».*

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

[5] *Согласно НП-001-15, приложение № 2: «Функция безопасности — конкретная цель и действия, обеспечивающие ее достижение, направленные на предотвращение аварий и (или) ограничение их последствий».*

[6] *Согласно НП-001-15, приложение № 2: «Авария на АС (авария) — нарушение нормальной эксплуатации АС, при котором произошел выход радиоактивных веществ и (или) ионизирующего излучения за границы, предусмотренные проектной документацией АС для нормальной эксплуатации в количествах, превышающих установленные пределы безопасной эксплуатации; авария характеризуется исходным событием, путями протекания и последствиями».*

3.19 **логическое устройство** (safety logic assembly): Оборудование, являющееся частью системы защиты, выполняющее простые логические функции категории А, с очень высоким уровнем надежности и обычно используемое для отправки команд исполнительным механизмам защиты или сигналов другому логическому устройству.

Примечание — Простая логическая функция бывает комбинаторной и/или последовательностной. Соответственно, такая функция полностью пригодна для тестирования.

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

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.21 **аварийный останов** (scram): Быстрое прекращение работы ядерного реактора при возникновении чрезвычайной ситуации.

Примечание — Термин «аварийный останов» связан с устройством отключения, которое является частью автоматического выключателя, размыкающего цепь. Поэтому аварийный останов часто называют отключением ядерного реактора.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.22 **единичный отказ** (single failure): Отказ, который приводит к потере способности отдельной системы или компонента выполнять назначенные им функции безопасности, а также любые последующие отказы, являющиеся его результатом[2)].

Примечания

1 Единичный отказ обычно вызывают такие факторы, как коррозия, термическое напряжение и полный износ, относящиеся к аппаратным средствам системы.

2 Единичный отказ также называют случайным отказом.

3 По причине случайного характера статистическую информацию можно получить из результатов испытаний или из накопленного со временем опыта. Таким образом, можно рассчитать среднюю вероятность и, соответственно, риск, связанный с возникновением случайного отказа.

[Словарь терминов МАГАТЭ по безопасности, 2016 г.]

3.23 **отключение** (trip): Быстрое снижение мощности ядерного реактора.

Примечание — Отключение ядерного реактора также называют аварийным остановом.

[МЭК 60050-395:2014, статья 395-07-91]

4 Обозначения и сокращения

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

БПУ — блочный пункт управления (main control room, MCR);

МАГАТЭ — международное агентство по атомной энергии (international atomic energy agency, IAEA);

ОК — обеспечение качества (quality assurance, QA);

ООП — отказ по общей причине (common cause failure, CCF);

ПИС — постулируемое исходное событие (postulated initiating event, PIE);

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

ПЛУ — программируемое логическое устройство (programmable logic device, PLD);

---

1) *Согласно НП-001-15, приложение № 2: «Локализующие системы (элементы) безопасности — системы (элементы) безопасности, предназначенные для предотвращения или ограничения распространения выделяющихся при авариях радиоактивных веществ и ионизирующего излучения за предусмотренные проектом АС границы и выхода их в окружающую среду».*

2) *Согласно НП-001-15, приложение № 2: «Исходное событие — единичный отказ в системе (элементе) АС, внутреннее или внешнее воздействие, или ошибка персонала, либо сочетания указанных событий, которые приводят к нарушению нормальной эксплуатации АС и могут привести к нарушению пределов и (или) условий безопасной эксплуатации».*

РПУ — резервный пункт управления (safety control room/emergency control room, SCR);
СКУ — система контроля и управления (instrumentation and control system, I&C system);
СПЛУ — сложное программируемое логическое устройство (complex programmable logic device, CPLD);
ЭМС — электромагнитная совместимость (electromagnetic compatibility, EMC);
EMI/RFI — электромагнитные помехи/радиочастотные помехи (electromagnetic interference/radiofrequency interference);
EMR — электромагнитное реле (electromagnetic relay);
ESF — технические средства безопасности (а также действия и последовательности после их срабатывания) (engineered safety feature);
FMEA — анализ типов и последствий отказов (failure mode and effect analysis);
HDL — язык описания аппаратных средств (hardware description language);
HPD — HDL-программируемое устройство (HDL-programmed device);
SCP — дополнительные точки управления (supplementary control points);
SLA — логическое устройство безопасности (safety logic assembly);
SSR — твердотельное реле (solid state relay);
2oo3 — элемент мажоритарной логики 2 из 3;
2oo4 — элемент мажоритарной логики 2 из 4.

5 Принципы и описание логических устройств

5.1 Логическое устройство

Систему защиты для выполнения функций безопасности цифровыми средствами проектируют с применением программно-реализуемой технологии.

Как правило, такая система имеет несколько, подчас разнообразных дублирующих каналов, обеспечивающих, среди прочего, соответствие системы критериям единичного отказа, достижение заданного уровня работоспособности, а также возможность функционального диагностирования и технического обслуживания системы в режиме реального времени.

Выходные сигналы от различных каналов до отправки конечного сигнала команды исполнительному механизму проходят дополнительную обработку логическим устройством. Процедура обработки зависит от проекта, но обычно включает некоторую форму мажоритарной логики в отношении каналов, в результате чего выходной сигнал канала может быть проигнорирован или направлен в обход для периодической проверки.

В приложении А приведены и другие примеры возможных функций, выполняемых логическим устройством.

Поскольку конечная обработка является простой (последовательная и/или комбинаторная) и важной для безопасности (прямая команда исполнительным механизмам защиты), технология проектирования логического устройства должна быть высоконадежной, т. е. обеспечивать достоверность и безопасность. В приложении С приведены сведения, поясняющие понятие надежности.

Настоящий стандарт не рассматривает логические устройства, использующие программно-реализуемую технологию, поскольку компьютеризированные системы и разработка программного обеспечения надлежащим образом изложены в других стандартах.

Таким образом, логическое устройство, описанное в настоящем стандарте, выполняет логические функции категории А для отправки прямых команд исполнительным механизмам без применения программно-реализуемой технологии.

Проектирование логического устройства, являющегося частью системы защиты, должно осуществляться в соответствии с требованиями МЭК 61513.

5.2 Технология проектирования логического устройства

Логическое устройство может быть спроектировано с применением технологии любого типа, если характеристики надежности соответствуют требованиям. В настоящем стандарте рассмотрены два типа технологий: аппаратно-реализуемая технология и технология с применением HPD.

a) Аппаратно-реализуемая технология подразумевает определение функции логического устройства характеристиками входящих в него компонентов и связями между ними. Данная технология использовалась в первых электронных системах, выполняющих функции безопасности.

Рассмотрено несколько типов технических компонентов, таких как реле, твердотельные компоненты, динамические логические схемы. Иногда вместо термина «аппаратно-реализуемая технология» используют термин «аналоговая технология», чтобы подчеркнуть тот факт, что сигналы являются аналоговыми (напряжение, ток, частота и др.). Но сигналы не обязательно являются аналоговыми, поскольку более ранние цифровые компоненты не были программируемыми. Аппаратно-реализуемая технология является простой, устойчивой к сбоям и быстрой. Функция устройства, спроектированного по такой технологии, постоянна и стабильна.

После валидации и испытаний остающийся риск отказа может быть связан только со случайными отказами по причинам старения, износа, условий окружающей среды, которые могут вызывать отклонения.

Поскольку вероятность отказа можно оценить, поведение системы более или менее предсказуемо.

При применении аппаратно-реализуемой технологии безопасность обеспечивают за счет принятия мер против случайных отказов, что достигается использованием конкретного проекта и неразнообразным резервированием.

b) Технология с применением HPD

Значительное уменьшение размеров электронных компонентов за последнее время способствовало созданию нового вида технологии, основанной на логических схемах с высокой плотностью упаковки, способных выполнять сложные функции с использованием языка описания аппаратных средств (HDL). Такие устройства называют «HDL-программируемыми устройствами» (HPD), к которым относятся ПЛИС, ПЛУ, СПЛУ или специализированные интегральные схемы. Их проектирование основано на принципах аппаратно-реализуемой технологии, поскольку функции аппаратно фиксированы соединениями между логическими элементами. Тем не менее применение данной технологии имеет много сходства с программно-реализуемой технологией, в частности в том, что на проект могут влиять ошибки. Для снижения риска ошибки, обусловленной сложностью устройств, необходимо следовать рекомендациям МЭК 62566.

В связи с очень высокими требованиями к работоспособности и характеристикам безопасности SLA при их проектировании следует тщательно контролировать и выбирать HPD, соответствующие требованиям.

Рекомендации и ограничения, относящиеся к HPD, приведены в В.4.3 приложения В.

5.3 Интерфейсы логического устройства

На рисунке 1 показана типовая организация канала контроля и управления в системе защиты с использованием логического устройства для управления исполнительными механизмами защиты.

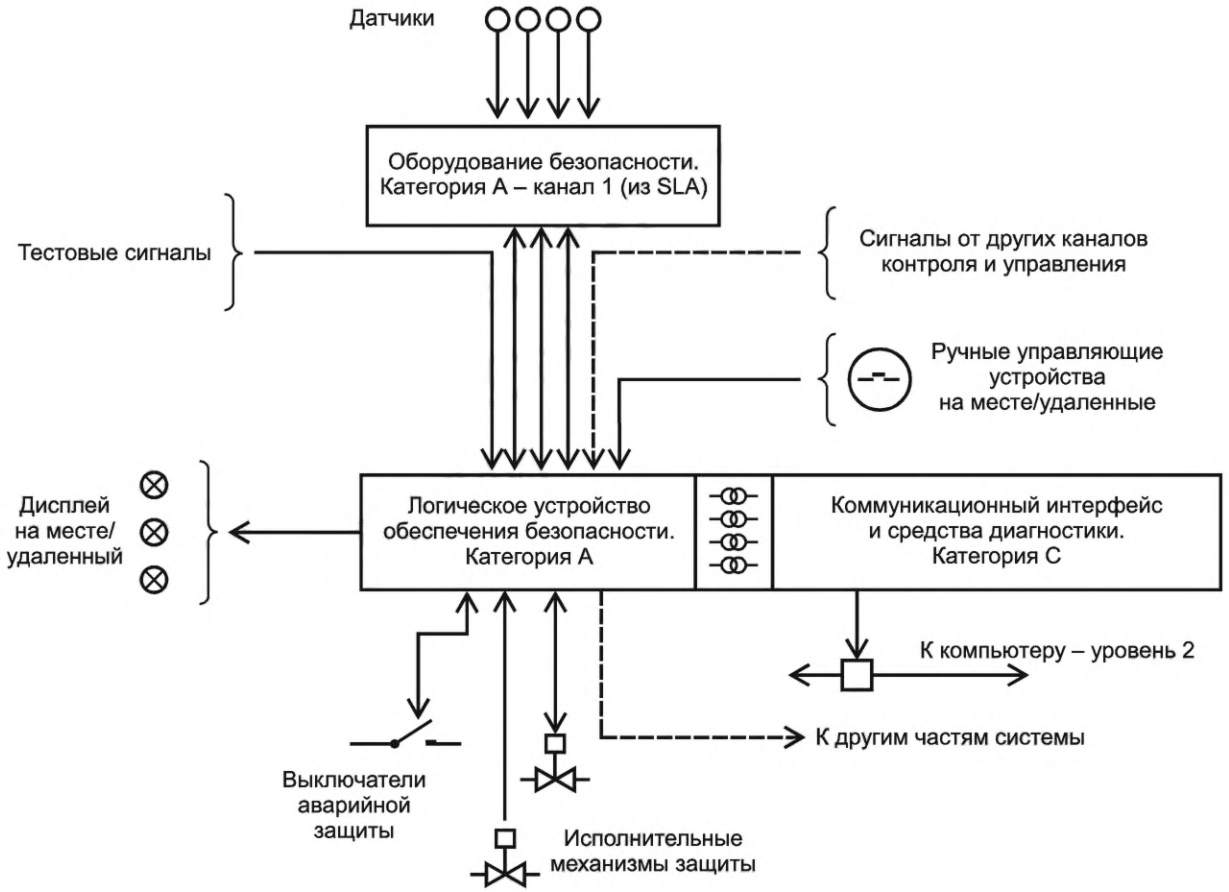

Рисунок 1 — Типовые интерфейсы системы защиты, использующей логическое устройство

Как правило, в системе защиты с использованием логического устройства выделяют три части:

a) оборудование безопасности

Например, резервный канал контроля и управления в системе защиты. Канал 1 на рисунке 1, выполняющий функции категории А, в том числе обработку аналоговых сигналов и сравнение уставки с сигналами от датчиков. Это оборудование генерирует двоичные сигналы, являющиеся входными сигналами для логического устройства;

b) логическое устройство (аппаратно-реализуемое или с применением HPD)

Устройство выполняет функции категории А с использованием двоичных сигналов, получаемых от цифрового оборудования безопасности, и других сигналов, в том числе от ручных управляющих устройств, тестовых сигналов и сигналов от других каналов контроля и управления, если востребована мажоритарная логика. В некоторых проектах логические устройства используют для отправки конечных и прямых управляющих сигналов выключателям аварийной защиты или исполнительным механизмам защиты.

Возможно использование дисплеев для индикации данных о безопасности (удаленно или на месте). Некоторые сигналы от коммуникационного и диагностического оборудования (поступающие в логическое устройство системы защиты извне) подключают к интерфейсу системы защиты для улучшения мониторинга системы при поддержке компьютерной системы станции.

Сигналы также могут быть соединены с другими частями системы защиты (например, с другим логическим устройством) в зависимости от функций и архитектуры системы защиты.

Функции, выполняемые логическим устройством, зависят от каждого конкретного проекта и могут существенно отличаться. В некоторых случаях логическое устройство может получать сигналы от исполнительных механизмов, несущие информацию о статусе или месте расположения;

c) интерфейс коммуникационного и диагностического оборудования

Это оборудование связано с логическим устройством системы защиты и выполняет функции категории С, получая сигналы от логического устройства. Сигналы от диагностических устройств с ре-

зультатами проверки могут быть переданы на компьютеры и в пункты управления при условии, что это оборудование надлежащим образом изолировано от логического устройства.

5.4 Показатели надежности

Рассматривая вопрос о важности логического устройства, направляющего сигнал прямого управления исполнительным механизмам защиты, а также о его надежности, необходимо обратить внимание на его функционирование в случае отказа. Вероятность отказа следует подразделять на вероятность отказа в безопасном состоянии (ложное аварийное отключение) и в небезопасном состоянии (блокирование действия).

Наиболее подходящим параметром, характеризующим безопасность и готовность АС, является надежность (см. приложение С). Функциональная надежность включает два главных показателя работы АС: безопасность и готовность станции.

Назначение логического устройства в системе безопасности АС заключается в гарантированной отправке команды исполнительному механизму безопасности, если требуется выключение.

Лучшего уровня безопасности и готовности можно достичь путем повышения надежности (вероятности надлежащего функционирования без отказов).

В случае отказа SLA рассматривают два варианта:

- отказ с выходным сигналом в состоянии срабатывания (ложное срабатывание механизмов безопасности). Реакторная установка будет остановлена и поэтому будет находиться в состоянии меньшей готовности, но большей безопасности. Для повышения готовности необходимо снизить вероятность отказа в безопасном состоянии;
- отказ с выходным сигналом, заблокированным в небезопасном состоянии. Энергоблок продолжает функционировать, но безопасность под угрозой. Для повышения безопасности необходимо снизить вероятность отказа в состоянии ненахождения в действии.

Безопасность и готовность — показатели, которые могут быть выражены двумя вероятностями:

- вероятность отказа отправки команды, когда такая команда необходима (вероятность отказа по запросу);
- вероятность отказа путем отправления ложного сигнала срабатывания (вероятность отказа в год).

Эти вероятности следует предусмотреть для логического устройства во время проектирования системы защиты, как предписано в МЭК 61513.

Фактические вероятности рассчитывают при анализе работоспособности, выполняемом в соответствии с процедурой, приведенной в МЭК 60812.

Данные вероятности можно корректировать в ходе разработки проекта, обращая внимание на такие аспекты, как внутренняя архитектура, технология, выявление отказа.

5.5 Режимы функционирования

Для подтверждения того, что функционирование логического устройства не нарушено, следует подвергнуть анализу указанные ниже различные режимы функционирования устройства.

Нормальные условия эксплуатации:

- отсутствие отказа, нормальные условия окружающей среды;
- режим отказа;
- тестовый режим;
- пусковой режим для технологии HDL.

Нештатные условия эксплуатации:

- предусмотренные аномальные условия окружающей среды;
- человеческая ошибка: следует учитывать риск человеческой ошибки при реализации некоторых профилактических функций.

5.6 Принципы достижения целей безопасности

5.6.1 Безопасное функционирование в нормальных условиях

Надлежащее функционирование логического устройства возможно при выполнении следующих указаний:

а) корректность функций, реализуемых логическим устройством. Это достигается качеством составления спецификаций и их валидацией, а также качеством проектирования;

b) проведение периодических испытаний для обнаружения отказа, который нельзя выявить с помощью постоянной схемы обнаружения. Если при проведении периодического испытания испытуемая часть оборудования должна быть выведена из эксплуатации, но при этом ее функционирование при испытании необходимо, в проекте следует предусмотреть соответствующее резервирование;

c) работоспособность компонентов для снижения частоты отказов при их функционировании в заданных условиях. Это достигается выбором соответствующих компонентов при проектировании системы защиты;

d) прогнозирование поведения в случае отказа. Даже если все компоненты имеют низкую частоту отказа, поведение в случае отказа логического устройства должно быть понятно. Для этого следует реализовать несколько функций:

- отказоустойчивая конструкция: в случае отказа логического устройства контрольные сигналы автоматически приводят компонент к выключенному или безопасному состоянию;
- проектирование с учетом ограничения времени функционирования с компонентом или частью оборудования, находящимися в состоянии отказа. Это означает, что в проект оборудования закладывают постоянную схему обнаружения отказов, аварийное сигнальное устройство для оповещения операторов технического обслуживания, а также план быстро и легко выполнимого ремонта отказавших модулей;
- внутреннее резервирование логического устройства, чтобы реагировать на риск неотключения в случае отказа.

5.6.2 Безопасное функционирование в нештатных условиях

Логическое устройство должно быть способно функционировать в заданных условиях окружающей среды. Проект должен учитывать все функциональные особенности путем соответствующего выбора компонентов, чтобы оборудование было устойчивым к сбоям. Безопасное функционирование в нештатных условиях достигается посредством квалификации, проводимой в соответствии с 6.5.

5.6.3 Защита от человеческой ошибки

Согласно функциональным спецификациям логическое устройство получает ручные управляющие сигналы, например, для того, чтобы перевести оборудование в тестовый режим или начать вручную управлять исполнительными механизмами безопасности.

Проект должен учитывать риск возможного ненадлежащего управления оператором. Например, запрещено одновременно переводить две зарезервированные части системы в тестовый режим. Необходимо внедрить схему блокировки для изменения логики в зависимости от количества объектов, находящихся в тестовом режиме. Данные особенности важны, и их следует тщательно анализировать при проектировании оборудования.

5.7 Принципы достижения готовности

5.7.1 Требования к готовности АС

Требования к готовности АС понятны и не ограничиваются требованиями к SLA. Так как SLA направляют команды непосредственно исполнительным механизмам, в случае отказа последствия сказываются на функционировании АС, и этот аспект является принципиальным.

5.7.2 Готовность АС при нормальных условиях эксплуатации

При проектировании необходимо обеспечить минимизацию риска ложного срабатывания по причине аппаратного отказа, проектной ошибки или недопустимой команды оператора. Принципы схожи с теми, которые применяют для достижения целей безопасности, но некоторые решения (особенно внутренняя архитектура с мажоритарной логикой) следует тщательно продумывать, чтобы не ставить под угрозу состояние безопасности.

Вероятность того, что единичный случайный отказ вызовет автоматическое срабатывание, должна соответствовать значению, присвоенному логическому устройству.

Мажоритарная логика и после резервирования частей логического устройства должна быть простой и высоконадежной.

5.7.3 Готовность АС в нештатных условиях эксплуатации

Принципы достижения целей безопасности в нештатных условиях эксплуатации применимы также для достижения готовности АС в нештатном режиме эксплуатации.

5.7.4 Защита от человеческой ошибки

Во избежание ложных срабатываний по причине ошибки оператора необходимо реализовать определенные решения, например:

- осуществлять индикацию состояния других резервных каналов с целью четкого информирования оператора о риске срабатывания в случае ручного управления, например, когда канал уже находится в тестовом режиме;

- реализовать схему блокировки во избежание ложного срабатывания. Если проектировщик решает реализовать такую схему, проект следует подвергнуть тщательному анализу, чтобы не ставить под угрозу безопасное функционирование.

6 Проектные требования к логическим устройствам

6.1 Общие положения

Проект логического устройства должен быть разработан таким образом, чтобы:

- обеспечить надлежащее функционирование устройства во всех предусмотренных условиях;
- были достигнуты показатели надежности;
- устройство соответствовало всем требованиям, применимым к системам безопасности.

6.2 Функции

6.2.1 Спецификация функций

Функции безопасности логического устройства специфичны для каждого проекта и должны быть установлены и подвергнуты валидации в соответствии с требованиями МЭК 61513.

Функции с двоичными сигналами являются, в основном, комбинаторными или последовательностными. Выходные сигналы подаются на исполнительные механизмы или другие устройства системы безопасности.

Поскольку функции логического устройства в соответствии с МЭК 61226 относятся к категории А, их необходимо подвергать периодическим испытаниям в соответствии с рекомендациями, изложенными в МЭК 60671.

По возможности в логическое устройство следует внедрить постоянную аппаратно-реализуемую диагностическую схему для обнаружения постулированного отказа или неправильного положения ручных управляющих средств.

Если положение соответствует небезопасному состоянию, должны быть обеспечены индикация сигнала опасности и генерация управляющего сигнала для автоматического срабатывания исполнительного механизма безопасности (проектирование отказоустойчивой системы).

При проектировании логического устройства должны быть тщательно продуманы, а затем внедрены принципы постоянной аппаратно-реализуемой диагностики. Для определения функций схемы постоянной аппаратно-реализуемой диагностики проводят анализ работоспособности и безопасности. Следует определить полноту охвата отказов этой схемой мониторинга.

Постоянная аппаратно-реализуемая диагностика не должна негативно влиять на безопасное функционирование системы.

В качестве примеров функций постоянной аппаратно-реализуемой диагностики можно привести проверку корректного соединения платы, наблюдение за подачей электропитания или корректным положением переключателей.

При возникновении отказа схема аппаратно-реализуемой диагностики передает соответствующие сигналы:

- в систему безопасности, если необходимо отменить любые сигналы, передаваемые неисправным каналом. Это требование следует обосновать посредством анализа;
- оператору на устройство отображения, расположенное по месту, или на удаленный пункт управления через интерфейс и оборудование связи.

6.2.2 Средства ручного управления

Ручными управляющими средствами являются двоичные сигналы, передаваемые непосредственно от оборудования или дистанционно от пунктов управления. Такие управляющие сигналы применяют:

- для ручной активации конкретного исполнительного механизма или всей исполнительной системы безопасности с несколькими исполнительными механизмами;
- переведения части оборудования в состояние для испытания.

В МЭК 60965 установлены требования к средствам ручного управления, применяемым в случае невозможности использования блочного пункта управления.

Ручные управляющие средства оператора проектируют в соответствии с МЭК 61227.

6.2.3 Время срабатывания

Время срабатывания логического устройства должно быть определено и установлено таким образом, чтобы его значение соответствовало требованиям системы безопасности.

Временные характеристики включают два аспекта:

- временная последовательность срабатывания (все управляющие средства не могут быть активированы одновременно);
- время отклика между входным и выходным сигналом каждого модуля.

Временную последовательность срабатываний и время отклика логического устройства подвергают валидации и используют для расчета времени срабатывания системы безопасности в целом.

6.2.4 Отображение аварийных сигналов на дисплее

Состояние выходного сигнала (нормальное или инициирующее срабатывание защиты) от каждого логического устройства должно быть отображено на дисплее (или следует обеспечить средства оповещения). На дисплее также должна быть отображена степень важности входных сигналов.

Рекомендации и требования, относящиеся к функциям аварийной сигнализации в блочном пункте управления, приведены в МЭК 62241.

Требования к реализации функций сигнализации в пунктах управления приведены в МЭК 60964.

Необходимо обеспечить индикацию информации об извлечении модуля для замены.

Следует также отображать (или обеспечить средства оповещения) изменение функции мажоритарной логики логического устройства (например, замену логики 2оо4 на 2оо3), чтобы сократить время, необходимое для обнаружения этого обстоятельства и для ремонта неисправных компонентов.

6.2.5 Интерфейс

Логическое устройство может быть соединено с интерфейсом, диагностическим и коммуникационным оборудованием для предоставления компьютерной системе АС и операторам пункта управления всех важных сигналов от логического устройства. Эти сигналы должны быть изолированы в соответствии с 6.7.

6.3 Архитектура и резервирование

Архитектуру логического устройства, закрепленного за определенным набором исполнительных механизмов в канале системы защиты, проектируют в соответствии с параметрами надежности, как указано в 5.4.

Для достижения необходимого уровня надежности и безопасности в логическом устройстве предусматривают внутреннюю резервную архитектуру, причем резервные части должны обеспечивать высоконадежную мажоритарную логику.

Основные требования к проекту архитектуры логического устройства изложены в МЭК 61513.

6.4 Технология

При проектировании логического устройства возможны различные технологические решения.

В приложении В представлены несколько возможных типов аппаратно-реализуемых технологий и условия их применения при проектировании логических устройств.

Основные критерии при выборе технологии включают способность выполнять функцию, достижение заданной надежности (см. 5.4) и соблюдение условий квалификации (см. 6.5).

6.5 Квалификация

Логические устройства должны быть спроектированы и квалифицированы как важное для безопасности оборудование, устойчивое к окружающим условиям, являющимся следствием нормальных и постулированных исходных событий. Необходимо учитывать влияние следующих параметров[1)]:

- температура;
- давление;
- влажность;

[1)] *В НП-026-16, пункт 70 к условиям окружающей среды, при которых должно обеспечиваться сохранение работоспособности важного для безопасности оборудования, помимо указанных параметров включены также скорость изменения температуры окружающей среды, предельные значения концентрации коррозионно-активных и иных химических агентов, предельные значения концентрации пыли.*

- механическая вибрация;
- землетрясение;
- радиация;
- электромагнитная совместимость (ЭМС);
- электрическая изоляция.

Квалификационные испытания и соответствующие применяемые стандарты указаны в 7.2.4.

Спецификация логических устройств должна устанавливать аттестованный срок службы устройств и продолжительность выполнения целевого задания при заданных условиях эксплуатации.

Аттестованный срок службы логического устройства должен соответствовать заданным условиям эксплуатации и продолжительности выполнения целевого задания системы безопасности.

6.6 Обслуживание

Логическое устройство должно позволять проводить простой и быстрый ремонт после обнаружения отказа и при профилактическом обслуживании. Данное положение подразумевает две особенности:

- обнаружение отказов осуществляют с применением специальной детекторной схемы с оповещением оператора о том, какой именно компонент или плата вышли из строя;
- необходимо обеспечивать быструю замену и ограниченную потребность наладки или регулировки. Замена неисправного компонента должна быть быстрой и несложной. Она возможна только после обнаружения и получения сигнала о неисправном компоненте, что возможно, например, путем использования печатных плат, реализованных в стандартных электронных панелях.

Для облегчения обслуживания и быстрой идентификации логического состояния логического устройства и заменяемых модулей необходимо предоставить внутренние и внешние средства.

Запасную часть (модуль, плату) необходимо верифицировать и испытать, прежде чем устанавливать вместо неисправного компонента. Требования к испытаниям всех заменяющих компонентов приведены в 7.3.3.

После извлечения заменяемого модуля вероятность безопасного функционирования соответствующей системы должна поддерживаться на приемлемом уровне безопасности и готовности.

Поскольку для каждого из описанных в приложении В видов технологического решения требуется специфическое обслуживание, оно должно быть тщательно проработано на этапе проектирования.

6.7 Разделение

Проект логического устройства должен быть таким, чтобы все независимые критерии, применимые к системе безопасности в целом, были удовлетворены. Требования к разделению между резервными и другими частями системы должны соответствовать рекомендациям, изложенным в МЭК 60709.

Логические устройства резервных каналов должны быть спроектированы с учетом достаточной степени электрической независимости и физического разделения. Это необходимое, но не достаточное условие для снижения вероятности множественных отказов до приемлемого уровня, соответствующего требованиям к работоспособности, заложенным в проекте системы защиты.

Логическое устройство должно функционировать надлежащим образом при заданном уровне помех. Также необходимо обеспечить защиту в целях соблюдения требований к ЭМС логического устройства с другими устройствами. Принципы проведения квалификации приведены в 6.5, а квалификационных испытаний — в 7.2.4.

Входные и выходные цепи должны быть защищены от возникновения электрического напряжения под воздействием внешних источников и от возможного электрического контакта с ними вследствие неисправности.

При необходимости применения средств для предотвращения образования электрической дуги эти средства не должны отрицательно влиять ни на скорость переключений, ни на работоспособность логического устройства и выводить значения соответствующих показателей за пределы допустимых.

Сигналы ручного управления, получаемые логическим устройством (на месте или от БПУ), должны быть аппаратно реализованы, защищены от влияния ЭМС и разделены изоляционным модулем во избежание отклонений, вызванных непредусмотренным напряжением, аккумулированным на кабелях.

Логическое устройство может быть соединено с другими устройствами, относящимися к другим каналам. Все сигналы соединяют через изоляционные модули других каналов.

Требования к функциональному и коммуникационному разделению архитектуры СКУ на АС должны быть соблюдены во внутренних и внешних соединениях логических устройств.

6.8 Энергообеспечение

К логическим устройствам резервного канала должно подаваться электропитание от резервного канала электроснабжения.

Для поддержания требуемых функций логического устройства, действующего в системе, важной для безопасности, необходимо обеспечивать источник электропитания достаточной независимости и мощности.

Систему энергообеспечения проектируют в соответствии с МЭК 61225.

7 Испытания логических устройств

7.1 Общие положения

Для логического устройства предусмотрено четыре вида испытаний:

- типовые испытания для валидации проекта;
- производственные испытания для валидации изготовления;
- испытания на месте эксплуатации для валидации установки;
- периодические испытания для обнаружения отказов при функционировании логических устройств.

7.2 Типовые испытания

7.2.1 Общие положения

Типовые испытания проводят с целью валидации проекта логического устройства и для подтверждения того, что наблюдаемые рабочие характеристики логического устройства соответствуют или превосходят заданные рабочие характеристики для общего и/или специального проектного условия.

Допускается заменять некоторые типовые испытания теоретическим анализом. Однако, такой анализ должен быть обоснован и зафиксирован документально в квалификационной программе.

7.2.2 Последовательность испытаний

Типовые испытания логического устройства следует выполнять в установленной последовательности, письменно зафиксированной в процедуре испытаний.

Рекомендуются две последовательности испытаний:

a) функциональные и эксплуатационные валидационные испытания — для валидации функций и их выполнения в нормальных условиях эксплуатации;

b) квалификационные испытания — для валидации функционирования оборудования в нештатных и экстремальных внешних условиях.

7.2.3 Функциональные и эксплуатационные валидационные испытания

Логические устройства являются частями систем безопасности, и их функциональные валидационные испытания следует включать в валидационные испытания этих систем безопасности.

Валидационные испытания должны быть выполнены по программе обеспечения качества (ОК) и задокументированы.

Логические устройства испытывают для верификации следующих эксплуатационных характеристик:

- диапазон входных сигналов (допущение для элементов мажоритарной логики 0 и 1);
- диапазон выходных сигналов (допущение для элементов мажоритарной логики 0 и 1);
- логическая функция;
- время реагирования (логическое устройство должно выдавать выходной сигнал в течение установленного времени после инициации конфигурации входных сигналов);
- ограничения выхода за пределы диапазона входных сигналов;
- входное и выходное сопротивление;
- допустимая нагрузки;
- допустимые характеристики входного сигнала;
- допустимые характеристики выходного сигнала, где применимо;

- характеристики изолирования и разделения (для любого входа и выхода от любого входа и выхода);
- номинальная нагрузка (переменный ток, постоянный ток индуцирующий и резистивный);
- соотношение сигнал/шум (измеряемое в децибелах и указываемое в качестве меньшего значения, соответствующего элементу мажоритарной логики 1).

7.2.4 Квалификационные испытания

Необходимо провести верификацию того, что оборудование выполняет предписанные ему функции до, в процессе и после постулируемого исходного события. Типовое испытание состоит из процедур, осуществляемых в заданной последовательности:

- квалификационные испытания на влияние условий внешней среды в соответствии с IEC/IEEE 60780-323;
- квалификационные испытания на сейсмостойкость в соответствии с МЭК 60980;
- квалификационные испытания на ЭМС в соответствии с серией стандартов МЭК 61000 и МЭК 62003;
- квалификационные испытания на облучение, где применимо, в соответствии с IEC/IEEE 60780-323.

7.3 Производственные испытания

7.3.1 Общие положения

Для верификации того, что логические устройства, изготовленные на заводе, находятся в полном соответствии с устройствами, прошедшими типовые испытания, выполняют нижеуказанные испытания на соответствующем количестве образцов.

Условия и процедуры производственных испытаний устанавливают в программе обеспечения качества, составляемой производителем.

7.3.2 Испытания запасных частей

Запасные части предоставляют в виде электронных модулей или печатных плат. Они могут быть изготовлены в любое время в течение жизненного цикла оборудования и испытаны в соответствии с технологическими процедурами.

Для проверки функционирования запасных частей рекомендуется использовать специальный испытательный стенд, представляющий все интерфейсы в реальных условиях.

На протяжении жизненного цикла АС необходимо обращать внимание на возможное моральное устаревание, в связи с чем может потребоваться разработка новой конструкции запасной части. Квалификацию новой запасной части следует проводить в соответствии с требованиями, изложенными в 7.2.4.

Функциональную квалификацию и квалификацию на соответствие условиям окружающей среды необходимо анализировать, чтобы определить последовательность выполнения испытаний для обеспечения действительности квалификации.

7.3.3 Производственные испытания изготовленных логических устройств

Производственные испытания логических устройств должны включать:

- визуальный осмотр;
- проверку сварки, пайки, накрутки проводов и других методов соединения;
- проверку механических допусков;
- электрические испытания (испытание изоляции на сопротивление и пробой);
- испытания источников электропитания;
- функциональные испытания. Может быть указана необходимость предварительной приработки оборудования.

Вышеуказанные испытания выполняют в отношении всего объема выпущенных логических устройств.

7.3.4 Испытания замещающих компонентов/модулей

Все приобретаемые компоненты должны быть такого же типа, как и в квалифицированном оборудовании. Однако, когда возникает необходимость применения замещающих компонентов, они должны иметь соответствующее подтверждение в виде квалификационной документации, в которой должны быть отражены процесс изготовления, процедуры обеспечения качества и отличия ожидаемых характеристик, имеющие отношение к работе оборудования.

Если программа обеспечения качества включает испытания образцов, число компонентов или модулей, отбираемых в качестве образцов, должно соответствовать указанному уровню обеспечения качества, уровню отбора образцов и уровню контроля.

7.3.5 Испытания сборных шкафов

В отношении каждого сборного шкафа должны быть выполнены следующие испытания:

- функциональные испытания, по возможности наряду с аппаратурой автоматики, по крайней мере в отношении всех конфигураций входных и выходных сигналов, необходимые для выявления отказоопасных дефектов;
- проверка корректности функционирования вентиляции и других средств охлаждения;
- испытания статистической выборки для верификации изоляции между входными и выходными терминалами, а также между клеммными колодками и корпусами. Число испытаний может быть выбрано в соответствии со спецификацией.

7.4 Испытания на месте эксплуатации

7.4.1 Проверки технического состояния оборудования перед установкой

Перед установкой на месте логическое устройство необходимо проверить для подтверждения того, что оно не было повреждено во время транспортирования.

Проверку проводят в соответствии с прописанной процедурой и составляют отчет, подтверждающий, что все компоненты логического устройства перед установкой находятся в надлежащем состоянии.

7.4.2 Валидационные испытания установки

После установки на месте необходимо провести испытания, подтверждающие, что логическое устройство установлено должным образом и функционирует корректно.

Испытания проводят в соответствии с прописанной процедурой, учитывающей все возможные влияния на функционирование логического устройства условий места установки, например:

- адресация и соединение кабелей;
- закрепление шкафа;
- заземление.

После испытаний установки выполняют приемочные испытания в рамках приемочных испытаний системы защиты.

Возможность проведения диэлектрических испытаний изоляции или EMI/RFI испытаний следует рассматривать особо, учитывая ограничения во избежание нарушений в работе других систем.

7.4.3 Периодические испытания

Периодические испытания необходимо проводить в нормальных эксплуатационных условиях с целью выявления отказа, который нельзя обнаружить с помощью постоянных диагностических схем.

Согласно МЭК 61226 логические устройства выполняют функции категории А, они являются частью системы защиты и функционируют на протяжении многих лет. Их необходимо подвергать испытанию, которое должно подтверждать соответствие логического устройства критерию единичного отказа.

Промежутки времени между периодическими испытаниями определяют при анализе надежности в соответствии с вероятностными требованиями безопасности.

Рекомендуется использовать автоматический тестер, формирующий отчет об испытании.

Методы и процедуры контрольных испытаний должны соответствовать требованиям МЭК 60671.

8 Обеспечение качества

Для логического устройства обеспечения безопасности должен быть составлен план обеспечения качества с учетом специфики атомной отрасли и в соответствии с требованиями IAEA-GSR, часть 2.

В МЭК 61513 приведен большой перечень рекомендаций, относящихся к проектированию и реализации систем, в том числе к обеспечению качества.

Приложение А
(справочное)

Примеры применения логического устройства

Применение логических устройств разнообразно и возможно в более или менее важных частях систем безопасности. Там, где важно соблюдать требования безопасности и готовности, выбор аппаратно-реализованной технологии принципиален для обеспечения необходимого уровня эксплуатационной готовности и безопасности.

Ниже приведены примеры использования логических устройств:

a) останов ядерного реактора при регистрации определенного значения конкретного параметра в канале системы аварийной защиты;

b) логика в канале, т. е. осуществление логических операций со многими параметрами отключения реактора, обычно присутствующими в канале; логика подгруппы обработки входных сигналов канала для подтверждения того, что значение параметра находится в соответствующем диапазоне. Примеры включают действующие байпасы с измеряемыми потоком и температурой на выходе из активной зоны. В некоторых ядерных реакторах логика в байпасном канале необходима для подтверждения того, что главные насосы охладителя функционируют в границах рабочего режима, а не находятся в состоянии перехода к остановке или в кавитационном режиме;

c) логика приоритетности: логический интерфейс между канальным выходом и распределительным устройством или контакторами, между канальным выходом и исполнительными механизмами ESF. Сюда необходимо включить определение приоритета между элементами управления систем различных категорий безопасности;

d) логика для последовательности действий после отключения и для функционирования ESF;

e) логика при ручном отключении и обеспечении соединения между данным элементом управления и распределительным устройством, исполнительными механизмами или контакторами;

f) логика при ручных управляющих операциях системы безопасности для соблюдения последовательности действий после отключения и для функционирования ESF;

g) при ручной активации останова от SCP и осуществлении соединений с другими устройствами срабатывания;

h) в допустимых или необходимых случаях для соединения между двумя разными системами безопасности, обеспечивающего срабатывание обеих систем в случае срабатывания любой из них;

i) выходные действия для подачи или отключения питания системы, инициирующей аварийный останов реактора, для приведения в действие технических средств безопасности или для определения последовательности действий после аварийного останова;

j) при работе устройств, обеспечивающих применение или устранение технологических байпасов, разрешающих или запрещающих;

k) использование байпаса для технического обслуживания;

l) использование байпаса останова для реагирования на показания датчиков или на параметры останова;

m) при действии систем индикации и аварийных сигналов, необходимых для системы безопасности;

n) мажоритарная логика между резервированными каналами.

Приложение В
(обязательное)

Логическое устройство как аппаратно-реализованное технологическое решение

В.1 Краткий обзор

В.1.1 Общие положения

Ни на одну электронную технологию нельзя положиться на 100 %. У любого решения есть показатель частоты отказов. Для удовлетворения достаточно жестких требований, предъявляемых к системе безопасности, следует особенно тщательно подходить к выбору технологии и конечной логики, применяемых к резервным управляющим сигналам.

Логические устройства могут быть реализованы посредством различных технологических решений в целях достижения заданного уровня безопасности. Выбор логических систем (статических или динамических) должен соответствовать требованиям к работоспособности системы защиты в целом.

Наивысших уровней защиты обычно достигают при использовании систем, спроектированных с учетом заданного вида отказа (параметрами отказоустойчивости). Когда для этой цели применяют динамические полупроводниковые или магнитные логические устройства, их виды отказов должны быть изучены, чтобы убедиться, что все они соответствуют характеру безопасных отказов (обычно отсутствуют динамические логические сигналы).

Для повышения безопасности и/или готовности можно использовать резервирование как для статических, так и для динамических логических систем.

Испытания статических логических систем повышают надежность благодаря сокращению средней продолжительности отказа и, следовательно, времени, в течение которого опасный невыявленный отказ остается в системе. Рекомендации приведены в МЭК 60671.

Электронная технология использует компоненты с низким энергопотреблением для выполнения функций контроля и управления.

Проектирование логического устройства может предусматривать использование компонентов различных технологий. В следующих разделах представлены возможные аппаратно-реализуемые технологические решения, их основные особенности и требования к проектированию логического устройства.

В.1.2 Реле

Логическое устройство, генерирующее сигнал останова или срабатывание ESF, может быть реализовано в виде реле.

Реле являются простыми и надежными компонентами, которые применяют для исполнения логических функций посредством соответствующих соединений между контактами и катушками. Для реле существует два основных технологических решения:

- электромагнитные реле (EMR);
- твердотельные реле (SSR).

Для применения в качестве логических устройств здесь рассмотрены только реле, работающие на низком напряжении и низких токах.

В.1.3 Электромагнитные реле

Электромагнитное реле (EMR) представляет собой переключатель с электрическим приводом, контакты которого перемещаются силой магнитного поля, регулируемой электрическим током.

Реле, используемые в системе безопасности, должны быть рассчитаны на непрерывную работу в соответствии с серией стандартов МЭК 60255. Необходимо учитывать следующие аспекты:

- необходимо установить напряжение для испытания изоляции катушки реле;
- необходимо установить номинальное напряжение изоляции контактов;
- размер контактов реле должен быть обеспечен с запасом.

Особый интерес представляют специфические особенности EMR в конструкции логического устройства:

- разделение управляющего сигнала и управляемых цепей и разделение контактов. Важно соблюдать электроизоляцию между сигналами, поступающими от нескольких резервных каналов, даже в случае отказа. По этой причине электромагнитные реле предпочтительнее использовать для выполнения простых логических функций с изолированными двоичными сигналами;
- полное сопротивление катушки позволяет реализовать в конструкции контроль целостности цепи. Для этого целесообразно использовать низкий ток, меньший чем рабочий ток, или импульсные токи продолжительностью менее времени работы цепи. В тех исключительных случаях, когда подача питания вызывает останов, тестовый ток должен составлять порядка одной десятой минимального тока, который может подаваться для питания реле. Последнюю рекомендацию не обязательно применять к испытанию или контролю непрерывности импульса;
- время переключения EMR, которое может быть значительным, должно быть установлено с учетом времени срабатывания логического устройства;

- благодаря механической конструкции EMR должны быть прочными, чтобы противостоять ударам и ускорениям при сейсмических событиях.

- EMR с несколькими полюсами и изолированными контактами подходят для проектирования логических функций между несколькими сигналами.

За длительное время эксплуатации подвижные элементы изнашиваются и могут выйти из строя. Из-за искрения меняется электрическое сопротивление, контакты подвергаются эрозии, что делает реле непригодным, сокращая его срок службы. Работоспособность EMR зависит от нескольких параметров, включая число совершаемых операций, напряжение и ток на контактах.

Реле подлежат квалификации на время срабатывания и функционирование в конкретных условиях системы безопасности. Хотя требование ко времени срабатывания реле может меняться в зависимости от типа и/или механизма действия, необходимо обоснованное доказательство того, что время срабатывания реле подходит для останова ядерного реактора и для функционирования ESF. Обоснование должно касаться также пригодности с точки зрения охраны окружающей среды в соответствии с серией стандартов МЭК 60255.

B.1.4 Твердотельные реле

Твердотельное реле (SSR) представляет собой электронный компонент, который выполняет такую же функцию, как и электромагнитное реле, но не имеет подвижных элементов, что увеличивает продолжительность его срока службы.

В твердотельном реле для переключения управляемой нагрузки вместо соленоида применяют тиристор или другое твердотельное переключающее устройство, приводимое в действие управляющим сигналом.

Для изолирования управляющих и управляемых схем можно использовать оптическую развязку (светоизлучающий диод совместно с фототранзистором). Но такая конструктивная особенность предполагает обеспечение отдельного энергоснабжения.

Время переключения SSR очень короткое, а собственная индуктивность незначительна, что усложняет реализацию схемы контроля целостности цепи.

B.2 Магнитные усилители

Магнитный усилитель представляет собой электромагнитное устройство на основе нескольких очень простых компонентов, таких как катушки индуктивности, ферромагнитный сердечник и диоды. В нем нет подвижных элементов и изнашивающегося механизма, и он имеет хорошую устойчивость к механическим ударам и колебаниям. Многочисленные изолированные сигналы можно суммировать с помощью дополнительных управляющих обмоток на магнитных сердечниках. Обмотки магнитного усилителя более устойчивы к кратковременным перегрузкам, чем сопоставимые твердотельные устройства. Сердечники магнитных усилителей устойчивы к воздействию радиации. По этой причине они давно нашли применение в ядерной энергетике.

Благодаря своей простой конструкции магнитный усилитель имеет очень низкую частоту отказов и может работать без отказов очень долгое время.

Применение магнитных усилителей ограничено выполнением простых функций, сочетающихся с размерами и массой таких компонентов. Квалификацию на сейсмостойкость следует предусмотреть в самом начале проектирования, чтобы обеспечить жесткое крепление тяжелых компонентов.

B.3 Применение динамической логики для повышения отказобезопасности системы

Динамическая логика является электронной технологией на основе дискретных компонентов и преобразователей, использующая переменный тактовый сигнал, с несколькими ячейками для выполнения логической функции. На протяжении времени существования тактового сигнала выходной сигнал устройства корректен. В случае любого отказа тактовый сигнал прекращается, и выходной сигнал становится равным нулю. Данная особенность интересна с точки зрения характеристики отказобезопасности системы, т. к. выходной сигнал прогнозируем, а также может быть использована для повышения характеристик безопасности логического устройства.

Необходимо выполнить формальный анализ проекта и оформить это документально для подтверждения того факта, что проект соответствует требованиям функциональной надежности и не содержит неизвестных режимов отказа.

B.4 Твердотельные схемы

B.4.1 Общие положения

Как правило, для функционирования твердотельных логических устройств необходимы сигналы меньшей мощности, чем для работы реле. В связи с этим необходимо уделять особое внимание минимизации внешних (шумовых) сигналов от электромагнитных излучений, электростатических разрядов, блуждающих токов и бросков напряжения источников электропитания.

Необходимо установить соответствующие методы определения допустимых пределов нарушения функционирования при наличии влияния источников наихудших постулированных помех.

При соблюдении вышеуказанных условий маловероятно повреждение компонентов логических устройств в результате электрических помех. Тем не менее компоненты, применяемые на входных и выходных интерфейсах

логического устройства (например, оптические вентили), должны без повреждений выдерживать постулированные наихудшие уровни электрических помех, индуцируемых в соединительных кабелях.

В.4.2 Дискретные компоненты

В твердотельных схемах для генерирования выходных электрических сигналов из входных электрических сигналов и выполнения необходимых функций применяют такие дискретные электронные компоненты, как транзисторы, конденсаторы, диоды и т. д.

Наиболее важно то, что в случае отказа выходной сигнал твердотельной схемы нельзя прогнозировать, он может быть инициирован или нет.

Более того, в некоторых особых случаях отказ может привести к неустойчивым управляющим сигналам.

В проект логического устройства с твердотельными схемами необходимо включать дублирующие схемы, ограничивающие последствия отказа. Дублирующие выходные управляющие сигналы должны быть связаны с очень простой и надежной логической функцией.

В.4.3 HPD в качестве интегрированных компонентов логических устройств

Электронные компоненты естественным образом развиваются в направлении большей миниатюризации и становятся пригодны в качестве компонентов с высоким уровнем интеграции: HDL-программируемые устройства (HPD), такие как программируемые логические интегральные схемы (ПЛИС), ПЛУ, СПЛУ.

По сути, это проводные компоненты (узлы с большим количеством логических элементов), но их сложность такова, что требует применения вычислительных средств при их проектировании, например, конфигурацию ПЛИС обычно определяют с использованием программы на основе языка описания аппаратных средств (HDL). Кроме того, они могут воспроизводить поведение некоторых микропроцессоров.

Современный быстрый процесс миниатюризации технологий субмикронных комплементарных металл-оксидных полупроводников, используемых в качестве компонентов HPD, выявил три фундаментальных проблемы, относящиеся к привлечению этих компонентов для выполнения функций безопасности, и эти проблемы усугубляются с повышением степени миниатюризации:

- данные компоненты склонны к одиночным отказам из-за интерференции частиц;
- на них может влиять миграция токов, что может сократить срок их службы;
- сложность высоко интегрированных компонентов не оправдывает повышение безопасности.

В связи с вышесказанным применение HPD в качестве интегрированных компонентов при проектировании SLA следует ограничить простыми логическими функциями, и их следует выбирать из тех, которые имеют доказанные характеристики, свидетельствующие о сроке службы, сопоставимом с заданным сроком службы системы, и отвечают требованиям, необходимым для обоснования безопасности. По этой причине применение в качестве компонентов логических устройств HPD с высокой степенью миниатюризации не рекомендовано.

Компоненты HPD с высокой плотностью распределения элементов проектируют для выполнения сложных функций, и это не относится к функциям, выполняемым логическими устройствами. Для логических устройств следует выбирать HPD компоненты малой сложности.

Показатели, характеризующие работоспособность и безопасность логических устройств, должны быть тщательно оценены и согласованы с работоспособностью и безопасностью системы защиты, в которой их используют. В соответствии с требованиями МЭК 62566 указанные компоненты могут быть использованы для выполнения функций категории А.

Приложение С
(справочное)

Надежность и ее характеристики

С.1 Общие положения

Основной характеристикой логического устройства является функционирование должным образом, когда необходимо формировать команду управления исполнительным элементам. Понятие надежности включает методы и функциональные особенности, позволяющие минимизировать риск отказа при необходимости команды. Понятие надежности не сводится только к работоспособности. Последствия отказа следует рассматривать с двух сторон:

- несрабатывание по запросу (небезопасный отказ): следствием этого является то, что безопасность АС подвергается риску;
- ложное срабатывание (безопасный отказ): следствием этого является то, что АС остановлена, безопасна, но не находится в состоянии готовности.

Для каждого из этих событий характерна определенная вероятность.

С.2 Качественные и количественные характеристики надежности

На рисунке С.1 изображена диаграмма, на которой показана взаимосвязь между различными количественными и качественными характеристиками надежности, касающимися конечных рисков в отношении исполнительных элементов: несрабатывание по запросу (относится к безопасности) или срабатывание без запроса (относится к готовности). При составлении диаграммы использованы определения МАГАТЭ и МЭК.

Основной и принципиальной характеристикой является работоспособность. Логическое устройство надежно работает, когда вероятность отказа мала (работоспособность). При отсутствии отказа логическое устройство готово к работе (готовность).

Вероятность случайного отказа является количественной характеристикой, которую можно вычислить по различным базам данных с учетом описания компонентов и внешних условий их функционирования (температура, вибрационные воздействия и др.). Исходя из этой вероятности легко получить вероятность отсутствия отказа, что непосредственно связано с работоспособностью.

<table>
<tr><td>Вероятность надлежащего функционирования (без отказа)</td><td colspan="2">Вероятность отказа</td></tr>
<tr><td>РАБОТОСПОСОБНОСТЬ</td><td>Вероятность безопасного отказа (ложное срабатывание)</td><td>Вероятность небезопасного отказа (блокирование безопасного срабатывания)</td></tr>
<tr><td colspan="2">БЕЗОПАСНОСТЬ</td><td></td></tr>
<tr><td>АС в состоянии готовности и безопасности</td><td>АС в безопасности, но не в состоянии готовности</td><td>АС в состоянии готовности, но не в безопасности</td></tr>
</table>

Рисунок С.1 — Характеристики надежности. Взаимосвязь между работоспособностью и конечным риском применительно к безопасности

Работоспособность повышают путем обнаружения отказов и проведением мелкого и быстрого ремонта, чтобы максимально сократить время функционирования при отказе. Соответствующими характеристиками являются возможность испытаний и простота обслуживания. Эти характеристики по сути качественные.

В случае отказа логического устройства выходной сигнал не соответствует действительной команде и:

- либо приводит к срабатыванию (ложное срабатывание), и в этом случае происходит аварийный останов ядерного реактора (срабатывают выключатели аварийной защиты) или АС находится непосредственно перед остановкой автоматической или при ручном управлении оператора. АС находится в состоянии безопасности, но не готовности;
- либо находится в заблокированном состоянии (блокирование срабатывания), и в этом случае АС находится в небезопасном состоянии, но все еще в состоянии готовности. В общем, данная ситуация соответствует необнаруженному отказу.

Поскольку логические устройства применяют для обеспечения безопасности, их проект должен быть ориентирован на отказобезопасность.

Таким образом, оба вида риска (ложное срабатывание и блокирование срабатывания средств безопасности) могут быть снижены путем использования таких специальных конструктивных особенностей, как резервирование с соответствующей мажоритарной логикой.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным и национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 60255 (все части)	IDT	ГОСТ IEC 60255-1—2014 «Реле измерительные и защитное оборудование. Часть 1. Общие требования»[1)]
	IDT	ГОСТ IEC 60255-5—2014 «Реле электрические. Часть 5. Координация изоляции измерительных реле и защитных устройств. Требования и испытания»[2)]
	IDT	ГОСТ IEC 60255-8—2014 «Реле электрические. Часть 8. Электротепловые реле»[3)]
	IDT	ГОСТ IEC 60255-12—2014 «Реле электрические. Часть 12. Реле направления и реле мощности с двумя входными воздействующими величинами»
	IDT	ГОСТ IEC 60255-13—2014 «Реле электрические. Часть 13. Процентно-дифференциальные реле»
	IDT	ГОСТ IEC 60255-16—2013 «Реле электрические. Часть 16. Реле измерения полного сопротивления»[4)]
	IDT	ГОСТ IEC 60255-26—2017 «Реле измерительные и защитное оборудование. Часть 26. Требования электромагнитной совместимости»[5)]
	IDT	ГОСТ IEC 60255-27—2013 «Реле измерительные и защитное оборудование. Часть 27. Требования безопасности»[6)]
IEC 60255 (все части)	IDT	ГОСТ IEC 60255-127—2014 «Реле измерительные и защитное оборудование. Часть 127. Функциональные требования к защите от сверхнапряжений и недостаточных напряжений»
	IDT	ГОСТ IEC 60255-151—2014 «Реле измерительные и защитное оборудование. Часть 151. Функциональные требования к защите от сверхтоков и/или минимального тока»
IEC 60671	IDT	ГОСТ Р МЭК 60671—2021 «Системы контроля и управления, важные для безопасности атомных станций. Контрольные испытания»
IEC 60709	IDT	ГОСТ Р МЭК 60709—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
IEC/IEEE 60780-323	—	*
IEC 60812	—	*

[1)] Идентичен IEC 60255-1:2009, который заменен на IEC 60255-1:2022.

[2)] Идентичен IEC 60255-5:2000, который заменен на IEC 60255-27:2013.

[3)] Идентичен IEC 60255-8:1990, который заменен на IEC 60255-149:2013.

[4)] Идентичен IEC 60255-16:1982, который заменен на IEC 60255-121:2014.

[5)] Идентичен IEC 60255-26:2013, который заменен на IEC 60255-26:2023.

[6)] Идентичен IEC 60255-27:2005, который заменен сначала на IEC 60255-27:2013, а затем — на IEC 60255-27:2023.

Продолжение таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 60964	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 61000 (все части)	IDT	ГОСТ IEC 61000-3-2:2021 «Электромагнитная совместимость (ЭМС). Часть 3-2. Нормы. Нормы эмиссии гармонических составляющих тока (оборудование с выходным током не более 16 А на фазу)»
	IDT	ГОСТ IEC 61000-3-3:2015 «Электромагнитная совместимость (ЭМС). Часть 3-3. Нормы. Ограничение изменений напряжения, колебаний напряжения и фликера в общественных низковольтных системах электроснабжения для оборудования с номинальным током не более 16 А (в одной фазе), подключаемого к сети электропитания без особых условий»
	IDT	ГОСТ IEC 61000-3-11:2022 «Электромагнитная совместимость (ЭМС). Часть 3-11. Нормы. Ограничение изменений напряжения, колебаний напряжения и фликера в общественных низковольтных системах электроснабжения для оборудования с номинальным током не более 75 А при соблюдении особых условий подключения»
	IDT	ГОСТ IEC 61000-3-12:2016 «Электромагнитная совместимость (ЭМС). Часть 3-12. Нормы. Нормы гармонических составляющих тока, создаваемых оборудованием, подключаемым к общественным низковольтным системам, с входным током более 16 А, но не более 75 А в одной фазе»
	IDT	ГОСТ IEC 61000-4-3:2016 «Электромагнитная совместимость (ЭМС). Часть 4-3. Методы испытаний и измерений. Испытание на устойчивость к излучаемому радиочастотному электромагнитному полю»[1)]
	IDT	ГОСТ IEC 61000-4-4:2016 «Электромагнитная совместимость (ЭМС). Часть 4-4. Методы испытаний и измерений. Испытание на устойчивость к электрическим быстрым переходным процессам (пачкам)»
	IDT	ГОСТ IEC 61000-4-5:2017 «Электромагнитная совместимость (ЭМС). Часть 4-5. Методы испытаний и измерений. Испытание на устойчивость к выбросу напряжения»
	IDT	ГОСТ IEC 61000-4-8:2013 «Электромагнитная совместимость (ЭМС). Часть 4-8. Методы испытаний и измерений. Испытания на устойчивость к магнитному полю промышленной частоты»
	IDT	ГОСТ IEC 61000-4-9:2013 «Электромагнитная совместимость. Часть 4-9. Методы испытаний и измерений. Испытания на устойчивость к импульсному магнитному полю»[2)]

[1)] Идентичен IEC 61000-4-3:2010, который заменен на IEC 61000-4-3:2020.

[2)] Идентичен IEC 61000-4-9:2001, который заменен на IEC 61000-4-9:2016.

Продолжение таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 61000 (все части)	IDT	ГОСТ IEC 61000-4-10:2014 «Электромагнитная совместимость. Часть 4-10. Методы испытаний и измерений. Испытания на устойчивость к колебательному затухающему магнитному полю»[1)]
	IDT	ГОСТ IEC 61000-4-12:2016 «Электромагнитная совместимость (ЭМС). Часть 4-12. Методы испытаний и измерений. Испытание на устойчивость к звенящей волне»[2)]
	IDT	ГОСТ IEC 61000-4-13:2016 «Электромагнитная совместимость (ЭМС). Часть 4-13. Методы испытаний и измерений. Воздействие гармоник и интергармоник, включая сигналы, передаваемые по электрическим сетям, на порт электропитания переменного тока. Низкочастотные испытания на помехоустойчивость»
	IDT	ГОСТ IEC 61000-4-14:2016 «Электромагнитная совместимость (ЭМС). Часть 4-14. Методы испытаний и измерений. Испытание оборудования с потребляемым током не более 16 А на фазу на устойчивость к колебаниям напряжения»
	IDT	ГОСТ IEC 61000-4-18:2016 «Электромагнитная совместимость (ЭМС). Часть 4-18. Методы испытаний и измерений. Испытание на устойчивость к затухающей колебательной волне»[3)]
	IDT	ГОСТ IEC 61000-4-20:2014 «Электромагнитная совместимость. Часть 4-20. Методы испытаний и измерений. Испытания на помехоэмиссию и помехоустойчивость в ТЕМ-волноводах»[4)]
	IDT	ГОСТ IEC 61000-4-27:2016 «Электромагнитная совместимость (ЭМС). Часть 4-27. Методы испытаний и измерений. Испытание на устойчивость к несимметрии напряжений для оборудования с потребляемым током не более 16 А на фазу»
	IDT	ГОСТ IEC 61000-4-29:2016 «Электромагнитная совместимость (ЭМС). Часть 4-29. Методы испытаний и измерений. Испытания на устойчивость к провалам напряжения, кратковременным прерываниям и изменениям напряжения на входном порте электропитания постоянного тока»
	IDT	ГОСТ IEC 61000-4-30:2017 «Электромагнитная совместимость (ЭМС). Часть 4-30. Методы испытаний и измерений. Методы измерений качества электрической энергии»
	IDT	ГОСТ IEC 61000-4-31:2019 «Электромагнитная совместимость (ЭМС). Часть 4-31. Методы испытаний и измерений. Испытание на устойчивость к широкополосным кондуктивным помехам, воздействующим на порты электропитания переменного тока»
	IDT	ГОСТ IEC 61000-4-34:2016 «Электромагнитная совместимость (ЭМС). Часть 4-34. Методы испытаний и измерений. Испытания на устойчивость к провалам, кратковременным прерываниям и изменения напряжения электропитания оборудования с потребляемым током более 16 А на фазу»

[1)] Идентичен IEC 61000-4-10:2001, который заменен на IEC 61000-4-10:2016.

[2)] Идентичен IEC 61000-4-12:2006, который заменен на IEC 61000-4-12:2017.

[3)] Идентичен IEC 61000-4-18:2011, который заменен на IEC 61000-4-18:2019.

[4)] Идентичен IEC 61000-4-20:2010, который заменен на IEC 61000-4-20:2022.

Продолжение таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 61000 (все части)	IDT	ГОСТ IEC 61000-4-39:2019 «Электромагнитная совместимость (ЭМС). Часть 4-39. Методы испытаний и измерений. Излучаемые поля в непосредственной близости. Испытание на помехоустойчивость»
	IDT	ГОСТ IEC 61000-6-3:2016 «Электромагнитная совместимость (ЭМС). Часть 6-3. Общие стандарты. Стандарт электромагнитной эмиссии для жилых, коммерческих и легких промышленных обстановок»[1)]
	IDT	ГОСТ IEC 61000-6-4:2016 «Электромагнитная совместимость (ЭМС). Часть 6-4. Общие стандарты. Стандарт электромагнитной эмиссии для промышленных обстановок»[2)]
	IDT	ГОСТ IEC 61000-6-5:2017 «Электромагнитная совместимость (ЭМС). Часть 6-5. Общие стандарты. Помехоустойчивость оборудования, используемого в обстановке электростанции и подстанции»
	IDT	ГОСТ IEC 61000-6-7:2019 «Электромагнитная совместимость (ЭМС). Часть 6-7. Общие стандарты. Требования помехоустойчивости для оборудования, предназначенного для выполнения функций в системе, связанной с безопасностью (функциональная безопасность) в промышленных расположениях»
	IDT	ГОСТ IEC/TR 61000-1-5:2017 «Электромагнитная совместимость (ЭМС). Часть 1-5. Общие положения. Воздействия электромагнитные большой мощности (ЭМБМ) на системы гражданского назначения»
	IDT	ГОСТ IEC/TR 61000-1-6:2014 «Электромагнитная совместимость (ЭМС). Часть 1-6. Общие положения. Руководство по оценке неопределенности измерений»
	IDT	ГОСТ IEC/TR 61000-3-6:2020 «Электромагнитная совместимость (ЭМС). Часть 3-6. Нормы. Оценка норм электромагнитной эмиссии для подключения установок, создающих помехи, к системам электроснабжения среднего, высокого и сверхвысокого напряжения»
	IDT	ГОСТ IEC/TR 61000-3-7:2020 «Электромагнитная совместимость (ЭМС). Часть 3-7. Нормы. Оценка норм электромагнитной эмиссии для подключения установок, создающих колебания напряжения, к системам электроснабжения среднего, высокого и сверхвысокого напряжения»
	IDT	ГОСТ IEC/TR 61000-3-14:2019 «Электромагнитная совместимость (ЭМС). Часть 3-14. Оценка норм эмиссии для гармоник, интергармоник, колебаний напряжения и несимметрии при подключении установок, создающих помехи, к низковольтным системам электроснабжения»
	IDT	ГОСТ IEC/TS 61000-1-2:2015 «Электромагнитная совместимость (ЭМС). Часть 1-2. Общие положения. Методология достижения функциональной безопасности электрических и электронных систем, включая оборудование, в отношении электромагнитных помех»[3)]

[1)] Идентичен IEC 61000-6-3:2010, который заменен на IEC 61000-6-3:2020.

[2)] Идентичен IEC 61000-6-4:2011, который заменен на IEC 61000-6-3:2018.

[3)] Идентичен IEC/TS 61000-1-2:2008, который заменен на IEC 61000-1-2:2016.

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного, национального стандарта
IEC 61000 (все части)	IDT	ГОСТ IEC/TS 61000-3-5:2013 «Совместимость технических средств электромагнитная. Ограничение колебаний напряжения и фликера, вызываемых техническими средствами с номинальным током более 75 А, подключаемыми к низковольтным системам электроснабжения. Нормы и методы испытаний»
IEC 61225	IDT	ГОСТ Р МЭК 61225—2021 «Атомные станции. Системы контроля, управления и электроснабжения. Требования к статическим системам бесперебойного электроснабжения постоянного и переменного тока»
IEC 61226	IDT	ГОСТ Р МЭК 61226—2023 «Системы контроля и управления и электроэнергетические системы, важные для безопасности атомных станций, и выполняемые ими функции. Классификация
IEC 61227	IDT	ГОСТ Р МЭК 61227—2020 «Органы управления оператора пунктов управления атомной станции. Требования к проектированию»
IEC 61513	IDT	ГОСТ Р МЭК 61513—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 62003	—	*
IEC 62241	IDT	ГОСТ Р МЭК 62241—2021 «Системы сигнализации блочного пункта управления атомных станций. Функциональные требования»
IEC 62566:2012	—	*

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

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

- IDT — идентичные стандарты.

Библиография

IEC 60050-395, International Electrotechnical Vocabulary — Part 395: Nuclear instrumentation: Physical phenomena, basic concepts, instruments, systems, equipment and detectors

IEC 60300 (all parts) Dependability management

IEC 60706 (all parts) Maintainability of equipment

IEC 60880 Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions

IEC 62340 Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF)

IAEA Safety fundamentals — SF-1, Fundamental safety principles

IAEA Safety Glossary — edition 2016

IAEA Specific Safety Guide — SSG-30, Safety classification of structures, systems and components in nuclear power plants

IAEA — SSG-39, Design of Instrumentation and Control Systems for NPP (Specific Safety Guide)

IAEA — SSR-2/1 Rev1, Safety of Nuclear Power Plants Design (Specific Safety requirements)

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; логические устройства; классификация систем

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *С.И. Фирсова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 11.10.2023. Подписано в печать 23.10.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,76.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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