ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62340— 2011

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности Требования по предотвращению отказов по общей причине

IEC 62340:2007
Nuclear power plants —
Instrumentation and control systems important to safety —
Requirements for coping with common cause failure
(IDT)

Издание официальное

Москва
Стандартинформ
2012

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 Подготовлен Автономной некоммерческой организацией «Измерительно-информационные технологии» (АНО «Изинтех») и Открытым акционерным обществом «Всероссийский научно-исследовательский институт по эксплуатации атомных электростанций» (ОАО «ВНИИАЭС») на основе аутентичного перевода на русский язык указанного в пункте 4 стандарта, выполненного Российской комиссией экспертов МЭК/ТК 45

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 12 декабря 2011 г. № 770-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 60340:2007 «Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине» [IEC 62340:2007 «Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure»].

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2012

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 3
4 Обозначения и сокращения 6
5 Методы и стратегия по предовращению отказов по общей причине 6
5.1 Общие положения 6
5.2 Свойства отказов по общей причине 6
5.3 Основные механизмы предотвращения отказов по общей причине цифровых систем контроля и управления 6
5.4 Методы по предотвращению отказов по общей причине отдельных систем контроля и управления 7
5.5 Стратегия проектирования по предотвращению отказов по общей причине 8
6 Требования по предотвращению дефектов в спецификации требований 9
6.1 Получение спецификации требований к системам контроля и управления из проектной базы по безопасности станции 9
6.2 Использование принципа глубокоэшелонированной защиты и функционального разнообразия 9
6.3 Проблемы, связанные с отказами по общей причине на существующих станциях 10
7 Инструменты проекта по предотвращению совместных отказов систем контроля и управления . . 10
7.1 Принцип независимости 10
7.2 Проектирование независимых систем контроля и управления 11
7.3 Применение функционального разнообразия 11
7.4 Предотвращение распространения отказа через каналы связи 12
7.5 Инструменты проекта по защите систем от отказа в результате технического обслуживания. 12
7.6 Целостность аппаратных средств системы контроля и управления 12
7.7 Зависимость от взаимосвязей с внешними датами или сообщениями 13
7.8 Гарантия физического разделения и эксплуатационной надежности 13
8 Устойчивость к постулируемым скрытым дефектам программного обеспечения 13
9 Требования к предотвращению отказа системы из-за технического обслуживания во время эксплуатации 14
Приложение А (справочное) Связь между МЭК 60880 и настоящим стандартом 15
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 16

Введение

a) Технические положения, основные вопросы и организация стандарта

Для достижения высокого уровня безопасности используется резервирование как один из элементов проектирования систем управления и контроля, важных для безопасности. Поскольку отказ по общей причине может угрожать эффективности резервирования, необходимо предпринимать соответствующие меры по предотвращению этого отказа. В ядерной промышленности было положено начало проектированию и разработке комплекса мер, направленных на предотвращение отказов по общей причине. За последние тридцать лет такой комплекс был создан, а также был достигнут консенсус по ряду методов предотвращения отказов по общей причине.

Целью настоящего стандарта является рассмотрение всех аспектов предотвращения отказов по общей причине (ООП) и предоставление информации о соответствующих требованиях к системам контроля и управления, которые используются для выполнения функций, важных для безопасности (см. МЭК 61226) на атомных станциях.

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

Международный стандарт МЭК 62340 является документом второго уровня серии стандартов МЭК ПК 45А и рассматривает проблемы, связанные с отказами по общей причине.

Настоящий международный стандарт дополняет требования МЭК 61513 и связанных с ним стандартов требованиями по снижению и предотвращению возможности возникновения отказа по общей причине во время выполнения функций управления и контроля категории А. Требования, представленные в настоящем стандарте, применимы к функциям категории А (см. МЭК 61226), если их отказ является недопустимым в соответствии с проектом безопасности станции.

Детальная информация о структуре серии стандартов МЭК ПК 45А представлена в пункте d) настоящего введения.

c) Рекомендации и ограничения по применению настоящего стандарта

Настоящий стандарт распространяется на системы контроля и управления, важные для безопасности, на новых атомных станциях, а также на замену системы контроля и управления существующей станции. Возможно, функции контроля и управления должны быть сохранены или модернизированы при замене системы контроля и управления. Требования настоящего стандарта также распространяются на замену инструментов контроля и управления, которая влечет за собой изменения в структуре системы контроля и управления.

Для существующих станций могут быть применимы только конкретные требования, представленные в настоящем стандарте, и эти требования должны быть определены в начале реализации любого проекта. Требования и рекомендации, не относящиеся к проектам модернизации или замены систем контроля и управления АС, должны подтверждаться общей оценкой безопасности в каждом конкретном случае. Потенциальные последствия невыполнения требований, изложенных в настоящем стандарте, по некоторым аспектам, связанным с ограничениями, введенными на станции, должны быть рассмотрены в сравнении с уровнем безопасности, который может быть достигнут благодаря модернизации станции в целом.

Во избежание дублирования требований настоящий стандарт ссылается на соответствующие разделы (подразделы) других существующих стандартов, в особенности на стандарты ядерной области МЭК 61513, МЭК 60709, МЭК 60780 и МЭК 60880. Новые требования, не содержащиеся в этих стандартах, представлены в настоящем стандарте.

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

Документом высшего уровня серии стандартов МЭК ПК 45А является МЭК 61513. Этот стандарт касается требований к системам контроля и управления, важных для безопасности атомных станций (АС), и лежит в основе серии стандартов ПК 45А.

В МЭК 61513 имеются непосредственные ссылки на другие стандарты ПК 45А по общим вопросам, связанным с категоризацией функций и классификацией систем, оценкой соответствия, разделением систем, защитой от отказов по общей причине, аспектами программного и технического обеспечений компьютерных систем и проектированием пультов управления. Стандарты, на которые имеются непосредственные ссылки, следует использовать на втором уровне совместно с МЭК 61513 в качестве согласованной подборки документов.

К третьему уровню серии стандартов МЭК ПК 45А, на которые в МЭК 61513 нет непосредственных ссылок, относятся стандарты, связанные с конкретным оборудованием, техническими методами или конкретной деятельностью. Обычно документы, в которых по общим вопросам имеются ссылки на документы второго уровня, могут использоваться самостоятельно.

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

Для МЭК 61513 принята форма представления, аналогичная форме представления базовой публикации по безопасности МЭК 61508, с его структурой общего жизненного цикла безопасности и структурой жизненного цикла системы; в нем приведена интерпретация общих требований МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 для применения в ядерной области. Согласованность с этим стандартом будет способствовать соответствию требованиям МЭК 61508, интерпретированным для ядерной области. В этой структуре МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 применительно к ядерной области.

В МЭК 61513 приведены ссылки на стандарты ИСО, а также на документ МАГАТЭ 50-C-QA по вопросам, связанным с обеспечением качества.

В серии стандартов МЭК ПК 45А последовательно реализуются и детализируются принципы и базовые аспекты безопасности, предусмотренные правилами МАГАТЭ по безопасности атомных электростанций, а также серией документов МАГАТЭ по безопасности, в частности требованиями NS-R-1 «Безопасность атомных электростанций: Проектирование» и руководством по безопасности NS-G-1.3 «Системы контроля и управления, важные для безопасности атомных электростанций». Термины и определения, применяемые в стандартах серии МЭК ПК 45А, согласованы с терминами и определениями, применяемыми в МАГАТЭ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине

Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure

Срок действия с 2012—07—01
до 2017—07—01

1 Область применения

Системы контроля и управления, важные для безопасности, могут разрабатываться с использованием обычного защитного оборудования, компьютерного оборудования или комбинации обоих типов оборудования. В рамках настоящего стандарта представлены требования и рекомендации[1)] к общей архитектуре систем управления и контроля, которые могут содержать одну или обе эти технологии.

Целью настоящего стандарта является:

a) определение требований, связанных с предотвращением отказов по общей причине систем контроля и управления, которые выполняют функции категории А;

b) дополнительные требования по использованию независимых систем контроля и управления для предотвращения отказов по общей причине, когда сокращена вероятность отказа по общей причине, так как строго соблюдаются общие принципы безопасности серии стандартов ПК 45А МЭК (особенно МЭК 61226, МЭК 61513, МЭК 60880 и МЭК 60709);

c) полное рассмотрение требований, относящихся к отказам по общей причине, но без рассмотрения требований, уже описанных в других стандартах. Ссылки на эти стандарты представлены в тексте настоящего стандарта.

В настоящем стандарте подчеркивается потребность в полной и точной спецификации функций безопасности, основанной на анализе проектных аварий и рассмотрении главных целей безопасности станции. Данная спецификация является предпосылкой создания полного набора детальных требований к проектированию систем контроля и управления по предотвращению отказов по общей причине.

В рамках настоящего стандарта представлены следующие принципы и требования по предотвращению отказов по общей причине с использованием средств, гарантирующих независимость[2)]:

a) между системами контроля и управления, выполняющими различные функции по обеспечению безопасности категории А, направленные на достижение одной и той же цели безопасности;

b) между системами контроля и управления, выполняющими различные функции разных категорий, если, например, функция категории В требуется как резервная копия функции категории А;

c) между резервными каналами одной системы контроля и управления.

Выполнение этих требований обеспечивает различные способы предотвращения отказов по общей причине.

[1)] Требования и рекомендации представлены номером пункта для обеспечения их четкого выполнения.

[2)] Независимость между системами контроля и управления или между резервными каналами одной системы контроля и управления – это возможность того, что в случае постулируемого отказа одной системы или одного канала, другие системы или каналы будут выполнять свои функции, как положено.

Издание официальное

Средства по предотвращению отказов по общей причине рассматриваются в настоящем стандарте относительно:

a) подверженности внутренним опасностям на станции и внешним опасностям;

b) распространения физических эффектов в аппаратных средствах (например, высокие напряжения);

c) предотвращения определенных ошибок и уменьшения защищенности систем контроля и управления, в особенности:

1) распространения функционального отказа в системах контроля и управления или между различными системами контроля и управления (например, через коммуникации, ошибки или погрешности на общих ресурсах),

2) появления отказов по общей причине, источник которых был заложен во время проектирования или возник во время эксплуатации системы (например, отказы в результате технического обслуживания),

3) недостаточной валидации системы, в результате которой во время внутренних переходных процессов система не выполняет установленные функции по обеспечению безопасности,

4) недостаточной квалификационной проверки необходимых свойств аппаратных средств, недостаточной верификации элементов программного обеспечения или недостаточной верификации совместимости замененных и существующих компонентов системы.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы. Если указана дата публикации, то именно данное издание следует использовать. При отсутствии даты используют последнее издание указанного документа, включая любые изменения.

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

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

МЭК 60780 Атомные станции. Электрооборудование, относящееся к системам безопасности. Квалификация (IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification)

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

МЭК 60980 Рекомендуемые методы проведения аттестации на сейсмическую безопасность электрооборудования для систем безопасности атомных станций (IEC 60980, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations)

МЭК 61000-4 (все части) Электромагнитная совместимость (EMC). Часть 4: Технологии тестирования и измерения (IEC 61000-4 (all parts), Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques)

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

МЭК 61513 Атомные станции. Контроль и управление, важные для безопасности. Общие требования к системам управления (IEC 61513, Nuclear power plants — Instrumentation and control systems important to safety — General requirements for systems)

Руководство по безопасности МАГАТЭ NS-G-1.3 Системы контроля и управления, важные для безопасности на атомных электростанциях (IAEA Safety Guide NS-G-1.3, Instrumentation and control systems important to safety in Nuclear Power Plants)

Руководство по безопасности МАГАТЭ SG-D11 Общие принципы безопасности при проектировании атомных электростанций (IAEA Safety Guide SG-D11, General design safety principles for nuclear power plants)

Справочник по безопасности МАГАТЭ, издание 2.0, 2006 (IAEA Safety Glossary Ed.2.0, 2006)

3 Термины и определения

В настоящем стандарте применены термины и определения по МЭК 61513 и МЭК 61226, а также следующие термины с соответствующими определениями:

3.1 **отказ по общей причине (ОПП)** [Common Cause Failure (CCF)]: Отказ двух или более конструкций, систем или компонентов вследствие единичного конкретного события или единичной конкретной причины.

[Глоссарий МАГАТЭ по безопасности, издание 2.0, 2006]

Примечание 1 — Одновременный отказ двух или более конструкций, систем или компонентов вызывается определенными недостатками, заложенными в процессе проектирования или производства, ошибками при эксплуатации или в процессе технического обслуживания, которые проявляются в результате воздействия природных явлений, эксплуатационных процессов на станции, действий человека или любых внутренних событий в системе контроля и управления.

Примечание 2 — Одновременный отказ интерпретируется также как последовательность отказов системы или компонентов, когда временной интервал между отказами слишком короток, чтобы предпринять меры по ремонту.

3.2 **глубокоэшелонированная защита** (defence-in-depth): Применение более одной защитной меры для достижения определенной цели безопасности так, чтобы цель была достигнута даже при отказе одной из защитных мер.

[Глоссарий МАГАТЭ по безопасности, издание 2.0, 2006]

Примечание — Предполагается, что защитные меры независимы.

3.3 **разнообразие** (diversity): Наличие двух или более путей или средств достижения установленной цели. Разнообразие специально создается как защита от отказа по общей причине. Оно может быть достигнуто наличием систем, которые физически отличаются одна от другой, или с помощью функционального разнообразия, если аналогичные системы достигают установленной цели различными путями.

[МЭК 60880, пункт 3.14]

Примечание — См. также «функциональное разнообразие».

3.4 **проектирование отказобезопасных систем** (fail-safe design): Проектирование функций системы так, чтобы они реагировали на определенные ошибки заранее заданным, безопасным образом.

3.5 **отказ** (failure): Неспособность конструкции, системы или компонента функционировать в пределах критериев приемлемости.

[Глоссарий МАГАТЭ по безопасности, издание 2.0, 2006]

Примечание 1 — Отказ — это результат неисправности аппаратных средств, дефекта программного обеспечения, неисправности системы или ошибки оператора, связанной с ними сигнальной траекторией, которая и вызывает отказ.

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

3.6 **дефект** (fault): Неисправность или ошибка в компоненте технического обеспечения, программного обеспечения или системы

[МЭК 61513, пункт 3.22]

Примечание 1 — Дефекты могут подразделяться на случайные, например, в результате ухудшения аппаратных средств из-за старения, и систематические, например, ошибки в программном обеспечении, которые вытекают из погрешностей проектирования.

Примечание 2 — Дефект (в особенности дефект проекта) может остаться необнаруженным в системе до тех пор, пока не окажется, что полученный результат не соответствует намеченной функции, то есть возникает отказ.

Примечание 3 — См. также «ошибка программного обеспечения» и «случайный дефект».

3.7 **предотвращение дефекта** (fault avoidance): Использование методов и процедур, которые предотвращают появление дефекта во время любого этапа безопасного жизненного цикла.

[МЭК 61508-4, пункт 3.6.2, измененный]

3.8 **устойчивость к дефектам** (fault tolerance): Встроенные возможности системы обеспечивать непрерывную и правильную работу при наличии ограниченного числа дефектов технического или программного обеспечения.

[МЭК 60880, пункт 3.18]

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

[МЭК 60880, пункт 3.19]

Примечание — См. также «разнообразие».

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

[МЭК 61513, пункт 3.24]

3.11 **ошибка человека (или ошибка)** [human error (or mistake)]: Действие человека, приводящее к непреднамеренному результату.

[МЭК 60880, пункт 3.21]

3.12 независимые системы контроля и управления (independent I&C systems)

Независимые системы обладают следующими свойствами:

a) способность одной системы по выполнению своей функции не зависит от работы или отказа другой системы;

b) способность систем к выполнению своих функций не зависит от эффектов постулируемого исходного события, при котором они должны функционировать;

c) адекватная устойчивость к обычным внешним условиям (например, к землетрясениям и электромагнитным возмущениям) гарантируется проектом систем.

[Измененное определение «независимого оборудования» из Справочника по безопасности МАГАТЭ, издание 2.0, 2006]

Примечание — Способами достижения независимости в соответствии с проектом являются электрическая изоляция, физическое разделение, независимость коммуникаций и свободное управление процессом.

3.13 **переходный процесс входного сигнала** (input signal transient): Временное состояние всех сигналов процесса, включенных в систему контроля и управления.

Примечание — Состояние системы контроля и управления фактически определяется сигнальной траекторией, которая включает в себя внутренние состояния оборудования системы контроля и управления. Спецификация требований, однако, определяет реакции системы контроля и управления, необходимые для обеспечения безопасности в ответ на «входные сигнальные переходные процессы».

3.14 **скрытый дефект** (latent fault): Невыявленные неисправности в системе контроля и управления.

Примечание — Скрытые неисправности могут возникнуть в результате погрешностей в спецификации или проекте, а также в результате производственного дефекта и могут носить любой физический или технический характер. В случае погрешностей в спецификации или проекте считается, что скрытые неисправности могли также возникнуть во всех резервных подсистемах и, таким образом, определенная сигнальная траектория могла вызвать отказ по общей причине рассматриваемой системы контроля и управления.

3.15 **случайный дефект** (random fault): Несистематический дефект аппаратных средств.

Примечание — Неисправности аппаратных средств — это последствие физических или химических эффектов, которые могут возникнуть в любое время. Корректное описание вероятности возникновения случайных неисправностей может быть представлено статистически (частота отказов). Увеличенная частота отказов может быть результатом систематических неисправностей, заложенных при проектировании или изготовлении аппаратных средств, если она возникает без временной корреляции, например, как следствие преждевременного старения.

3.16 **траектория сигнала** (signal trajectory): Временные зависимости всех состояний оборудования, внутренних состояний, входных сигналов и входных действий оператора, которые определяют работу системы.

[МЭК 60880, пункт 3.33]

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

[Глоссарий МАГАТЭ по безопасности, издание 2.0, 2006]

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

[Глоссарий МАГАТЭ по безопасности, издание 2.0, 2006]

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

3.19 **отказ программного обеспечения** (software failure): Отказ системы из-за проявления дефекта в элементе программного обеспечения, заложенного в проекте.

[МЭК 61513, пункт 3.57]

Примечание 1 — Все отказы программного обеспечения происходят из-за дефектов проекта, так как программное обеспечение не изнашивается и не подвержено физическим отказам. Так как пусковые сигналы, которые активизируют неисправности программного обеспечения, возникают произвольно во время работы системы, следовательно, и отказы программного обеспечения также возникают случайно.

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

3.20 **дефект программного обеспечения** (software fault): Дефекты проекта, распространяющиеся на компонент программного обеспечения.

[МЭК 61513, пункт 3.58]

Примечание — См. также «дефект».

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

[МЭК 60880, пункт 3.39]

3.22 **валидация системы** (system validation): Подтверждение экспертизой и предоставлением другого свидетельства того, что система полностью отвечает заданным техническим условиям (функциональность, время реакции, устойчивость к дефектам и ошибкам, надежность).

[МЭК 60880, пункт 3.42]

3.23 **систематический отказ** (systematic failure): Отказ, обусловленный определенной причиной, которая может быть устранена только изменением проекта или производственного процесса, эксплуатационных процедур, документации или других соответствующих факторов.

[МЭК 61513, пункт 3.62]

Примечание — Отказ по общей причине — это вид систематического отказа, при котором совместно возникают отказы отдельных систем, резервного оборудования или компонентов.

3.24 **систематический дефект** (systematic fault): Дефект в аппаратных средствах или программном обеспечении, который систематически затрагивает несколько или все компоненты определенного типа.

Примечание 1 — Систематический дефект может быть вызван погрешностью в спецификации или проекте, производственными дефектами или неправильным техобслуживанием.

Примечание 2 — Компоненты, содержащие систематический скрытый дефект, могут отказать произвольно или совместно, в зависимости от вида неисправности и механизмов, вызывающих дефект.

3.25 **валидация** (validation): Процесс определения того, соответствует ли продукт или услуга своим функциональным требованиям, то есть удовлетворяет ли тем требованиям и целям, для которых был (а) предназначен (а).

[Справочник по безопасности МАГАТЭ, Издание 2.0, 2006]

Примечание — См. также «функциональная валидация» и «валидация системы».

3.26 **верификация** (verification): Процесс определения, соответствует ли качество продукта или услуги установленным требованиям.

[Справочник по безопасности МАГАТЭ, Издание 2.0, 2006]

4 Обозначения и сокращения

АС (NPP) — атомная станция;
ПЗИ (FAT) — заводские приемо-сдаточные испытания;
МАГАТЭ (IAEA) — Международное агентство по атомной энергии;
ООП (CCF) — отказ по общей причине;
ПОИ (SAT) — приемочные испытания на объекте;
ПИС (PIE) — постулируемое исходное событие;
ПА (DBA) — проектная авария[1];
ПС (DBE) — проектное событие[1];
ЭМИ (EMI) — электромагнитное возмущение.

5 Методы и стратегия по предотвращению отказов по общей причине

5.1 Общие положения

Настоящий раздел описывает стратегию по предотвращению отказов по общей причине и представляет требования, приведенные в разделах 6—9.

5.2 Свойства отказов по общей причине

Для систем контроля и управления, которые выполняют функции категории А, применение резервирования вместе с механизмами голосования является проверенным способом, соответствующим критерию единичного отказа. Такое проектирование гарантирует очень низкую вероятность отказа системы контроля и управления.

Системы контроля и управления такого проекта могут отказать, если два или более резервных канала откажут одновременно (отказ по общей причине). Отказ по общей причине может произойти, если скрытый дефект систематически возникает в нескольких или во всех резервных каналах и если этот дефект вызван определенным событием и приведет к совместному отказу нескольких или всех каналов. Резервная система контроля и управления отказывает, если число поврежденных каналов превышает допустимый предел, установленный в проекте.

Скрытые ошибки, которые систематически возникают в нескольких или во всех резервных каналах, могут проявиться на любом этапе жизненного цикла системы контроля и управления. Скрытые дефекты могут возникать в результате ошибок оператора, которые не зависят от технологии системы контроля и управления или в результате производственного процесса, зависящего от технологии системы контроля и управления. Велика вероятность того, что скрытые систематические дефекты связаны с такими основами проекта системы контроля и управления как, например:

- погрешности в спецификации требований к функциям, обеспечивающим безопасность;
- неадекватная спецификация устойчивости проекта аппаратных средств к окружающим условиям (например, к сейсмическим нагрузкам или электромагнитным возмущениям);
- технические дефекты проекта, которые могут вызвать отказ системы из-за повреждения внутренних механизмов.

События, ведущие к отказу по общей причине, могут быть вызваны извне, например, общей загрузкой всех резервных каналов переходными процессами входных сигналов, воздействием окружающей среды или в связи с конкретными значениями текущего времени или календарных дат. Более того, существование скрытых механизмов распространения может привести к тому, что искаженные данные, которые передаются от одной поврежденной системы к соответствующим системам других резервирований, могут вызвать последовательный отказ других резервных каналов. Такой вид распространения отказа свойственен только компьютеризированным системам контроля и управления.

5.3 Основные механизмы предотвращения отказов по общей причине цифровых систем контроля и управления

При использовании электронной техники функции, важные для безопасности каждого резервного канала, как правило, осуществляются цепями отдельных электронных компонентов, в то время как аппаратные средства компьютерных систем выполняют группу установленных функций. Поэтому следующие рассмотрения относятся главным образом к цифровым системам контроля и управления.

---

[1] Сокращения терминов «ПА» и «ПС» используются в соответствии с их определением в МЭК 61226.

При нормальных условиях эксплуатации (без изменений, связанных с техническим обслуживанием, и без физического воздействия окружающей среды, как указано в 7.8), обработка переходных процессов входных сигналов цифровыми системами контроля и управления вносит основной вклад в траектории их сигнала. Специфические траектории сигнала, которые могут вызвать отказ системы, могут возникать во время выполнения запросов по безопасности, из-за непроверенных комбинаций входных сигналов или могут быть вызваны специфическими внутренними состояниями системы. Такие внутренние состояния системы могут быть связаны с сохраненными данными ранних переходных процессов входных сигналов или со скрытыми дефектами, возникшими в результате более раннего техобслуживания, или могли быть вызваны дефектами аппаратных средств.

Отказ по общей причине может возникнуть, если аппаратные средства некоторых или всех резервированных средств подвергаются внешним воздействиям, которые превышают пределы, установленные в проекте аппаратных средств. Причиной такого механизма отказов может быть, например:

- некорректное проектирование физического разделения, при котором единичный отказ одной системы питания мог бы повлиять на два и более резервированных;

- неадекватно указанные пределы в проекте аппаратных средств, например, относительно сейсмических явлений.

Вероятность того, что отказ по общей причине может быть вызван случайными дефектами аппаратных средств, очень мала. Такой механизм возникновения отказа по общей причине предполагает, что определенный дефект может оставаться скрытым в течение более длительного времени и, таким образом, компоненты других резервных средств могут также быть затронуты этим типом неисправности. Наличие скрытого дефекта подразумевает то, что дефект не был обнаружен в процессе самоконтроля или периодического тестирования и затронутые компоненты отказывают не внезапно, а будучи активизированы общим пусковым механизмом в некоторых или во всех резервных средствах.

Последствия отказов системы по общей причине могут быть такими, что в случае запроса система реагирует следующим образом:

- не отвечает или дает ошибочный ответ по сравнению с требуемым ответом, но несмотря на это продолжает работать;

- вынуждена закончить работу и поэтому не дает никакого ответа.

5.4 Методы по предотвращению отказов по общей причине отдельных систем контроля и управления

Свойства отказов по общей причине, приведенные в 5.2, указывают на следующие способы снижения вероятности отказов по общей причине:

a) снижение вероятности скрытых систематических дефектов в резервных каналах отдельной системы контроля и управления;

b) снижение вероятности существования механизмов, которые могут вызвать совместные скрытые систематические дефекты или вызвать единичный отказ в одном канале, распространяющийся на другие каналы (распространение отказа).

Сложность обеспечения эффективной защиты от отказов по общей причине состоит в скрытых механизмах срабатывания системы контроля и управления. Поэтому предотвращение скрытых систематических дефектов и механизмы срабатывания требуют, чтобы проектирование и анализ системы контроля и управления проводились на основе постулатов, которые связаны с опытом возникновения отказов по общей причине на атомных станциях и потенциальными недостатками выбранной технологии создания системы контроля и управления.

Как показывает накопленный опыт, частота возникновений отказов по общей причине систем контроля и управления, которые выполняют функции категории А, очень низка. Это отчасти связано с высоким уровнем качества проектирования, изготовления и технического обслуживания таких систем контроля и управления. Однако частота возникновения отказов по общей причине также обусловлена характером отказа по общей причине, который может произойти только при вероятности совместного существования скрытого систематического дефекта и активации соответствующего механизма срабатывания траектории сигнала. Поэтому эффективная защита от отказов по общей причине должна также включать в себя такие важные действия, как устранение потенциальных механизмов срабатывания и предотвращение скрытых дефектов.

Опыт анализа возникновения отказов по общей причине на атомных станциях показывает, что основными являются следующие причины:

a) скрытые дефекты, которые связаны с ошибками в спецификации требований. Выявление ошибок в спецификации требований к функциям систем контроля и управления является сложным, и такие ошибки могут распространяться на последующие этапы проектирования, включая верификацию и валидацию системы. Скрытые дефекты, связанные с этим потенциальным источником, могут быть обнаружены только в процессе функциональной валидации (см. 3.25);

b) скрытые дефекты, возникающие во время технического обслуживания, потому что возможность анализа и тестирования изменений может быть ограничена условиями станции (например, изменение заданных значений, использование исправленных запасных частей или модернизация компонентов системы);

c) появление скрытых дефектов во время технического обслуживания; вызвано отчасти определенными состояниями системы или некорректными данными, которые не описывают фактическое состояние станции.

В зависимости от технологии создания систем контроля и управления различают несколько типов распространения отказа:

d) аналоговые системы контроля и управления могут подвергаться опасности из-за высоких напряжений, если один канал затрагивается единичным отказом, а соседние каналы затрагиваются последовательными отказами. Причиной этого является превышение пределов разделения каналов;

e) для цифровой технологии распространение отказа через высокие напряжения может быть предотвращено, если использовать волоконную оптику, но также требуется предпринимать определенные меры, сокращающие уязвимость к распространению отказа из-за ошибочных или некорректных данных.

В настоящем стандарте представлено руководство по сокращению возможности существования механизмов, которые могут вызвать постулируемые типы скрытых дефектов проекта, впоследствии приводящих к отказам по общей причине во время переходных процессов (см. разделы 7—9).

Для того, чтобы уменьшить правдоподобие того, что скрытые дефекты проекта могут остаться в окончательном варианте системы контроля и управления на минимально возможном уровне, в настоящем стандарте дана ссылка на требования к проектированию, указанные в серии стандартов МЭК ПК 45А (см. раздел 2).

5.5 Стратегия проектирования по предотвращению отказа по общей причине

Меры проекта по предотвращению отказа по общей причине связаны с архитектурой систем контроля и управления, которая включает в себя, по крайней мере, две системы контроля и управления, выполняющие функции категории А. Доказать то, что любая индивидуальная система контроля и управления не имеет ошибок, невозможно, и поэтому существование скрытых дефектов и связанных с ними механизмов срабатывания не может быть исключено в принципе. Следовательно, возникновение отказов по общей причине не может быть исключено ни для одной индивидуальной системы управления, хотя их ожидаемая частота должна быть ниже намеченной во время жизненного цикла станции.

Если одна система контроля и управления не срабатывает из-за отказа по общей причине, необходимо, чтобы главные функции категории А выполнялись другой системой контроля и управления с тем, чтобы избежать недопустимых последствий и гарантировать выполнение главных целей по обеспечению безопасности на атомной станции. Эта другая система контроля и управления должна выполнять свои назначенные функции по обеспечению безопасности независимо (см. 3.12), так чтобы вероятность совместного отказа обеих систем контроля и управления была снижена до такой степени, чтобы такой отказ не возник во время намеченного жизненного цикла станции.

При снижении совместного отказа независимых систем контроля и управления до минимального уровня требуется, чтобы системами управляли в различных сигнальных траекториях, и системы были хорошо защищены от физических опасностей (см. 5.3). Разные траектории сигнала могут быть обеспечены посредством использования разнообразия (т. е. разнообразия оборудования или функционального разнообразия).

Применение функционального разнообразия формирует единственную возможность обеспечить защиту от постулируемого скрытого функционального дефекта в спецификации требований. Назначение разных функций на независимые системы контроля и управления может в то же время использоваться как средство, гарантирующее управление системой контроля и управления с разными траекториями сигнала.

В рамках настоящего стандарта представлено руководство по проектированию и использованию независимых систем контроля и управления, которые работают с разными сигнальными траекториями (см. 3.16) и, таким образом, вероятность совместного отказа этих независимых систем является незначительной для намеченного жизненного цикла станции, даже если могут существовать скрытые обычные неисправности проекта (см. разделы 6, 7 и 9).

6 Требования по предотвращению дефектов в спецификации требований

6.1 Получение спецификации требований к системам контроля и управления из проектной базы по безопасности станции

Функциональное разнообразие должно гарантировать выполнение основных целей по обеспечению безопасности на станции, несмотря на возможное существование скрытых дефектов, связанных с погрешностями в спецификации требований.

На основе анализа проектных аварий и соответствующих проектных событий, которые могут быть вызваны отказами систем контроля и управления или связанных с ними подсистем, формируется спецификация требований, которая определяет необходимость использования функционального разнообразия. Функциональное разнообразие может зависеть от предполагаемых последствий в случае отказа и предполагаемых частот появления этих проектных событий[1)].

6.1.1 В рамках данного анализа должны быть предприняты следующие меры:

a) Необходимо определить проектные события, которые могут привести к недопустимым последствиям, если отказ по общей причине постулируется для определенной системы контроля и управления. В проекте по предотвращению отказов по общей причине необходимо определить число проектных событий, которые могут возникнуть с частотой, превышающей установленную в спецификации.

b) Для этого числа проектных событий должна быть определена, по крайней мере, половина параметров безопасности станции, и эти параметры должны быть оценены с тем, чтобы составить спецификацию различных функций по обеспечению безопасности[2)].

6.1.2 Функции безопасности, которые определены относительно отказов по общей причине (см. 6.1.1), могут быть выполнены в рамках различных стратегий[3)]. Для принятого проекта с конкретными постулируемыми отказами по общей причине должно быть продемонстрировано успешное выполнение задач по обеспечению безопасности станции при таких отказах по общей причине.

6.2 Использование принципа глубокоэшелонированной защиты и функционального разнообразия

Использование принципа глубокоэшелонированной защиты и функционального разнообразия требует идентификации тех конкретных функций контроля и управления категории А, которые могут независимо гарантировать то, что выполняются главные цели по обеспечению безопасности на станции. Эти функции называются «функциями разнообразия относительно определенной цели по обеспечению безопасности».

6.2.1 Функции разнообразия систем контроля управления и категории А должны быть установлены для независимых систем контроля и управления и осуществляться так, чтобы в случае постулируемого отказа одной из независимых систем контроля и управления главные цели по обеспечению

[1)] Готовность разнообразных защитных функций и, в частности, готовность разнообразных или независимых измерительных сигналов является результатом правильного проектирования технологического комплекса станции. В целом, требования и рекомендации настоящего стандарта предназначены для использования потенциала безопасности технологического комплекса станции при проектировании систем контроля и управления, важных для безопасности (например, существование различных переключателей).

[2)] Большинство переходных процессов влияет почти на все параметры безопасности одновременно и, значит, требуется применение функционального разнообразия в качестве предварительного условия для более подробного анализа проектных аварий, но, как правило, дополнительные параметры безопасности не требуются.

[3)] Примеры стратегий проекта, которые могут быть приемлемыми или считаться приемлемыми в определенных (но не обязательно во всех) национальных контекстах:

- идентифицированные различные функции безопасности группируют таким образом, что каждое соответствующее проектное событие обрабатывается обоими наборами функций безопасности. Каждый набор функций распределяется на любую независимую систему контроля и управления. Оставшиеся функции категории А распространяются на любую из этих систем контроля и управления. Данная процедура распределения функций гарантирует дифференцированные надлежащим образом сигнальные траектории, которые будут обрабатываться независимыми системами контроля и управления так, чтобы они могли быть основаны на той же платформе системы контроля и управления;

- все функции категории А (включая пары разнообразных функций) распределяют на одну систему контроля и управления (первичная защитная система контроля и управления). Затем обработка одной группы идентифицированных различных функций безопасности дублируется независимой вторичной системой защиты, которую может составлять оборудование более низкого класса. Для того, чтобы гарантировать дифференцированные надлежащим образом сигнальные траектории между независимыми системами контроля, необходимо использовать разнообразие оборудования.

безопасности на станции были все равно достигнуты благодаря выполнению этих функций другими независимыми системами контроля и управления.

При проектировании должны быть предприняты следующие меры:

6.2.2 Подтверждение независимости выполнения различных функций должно быть задокументировано в отчете о безопасности.

6.2.3 Если заявлено, что функции контроля и управления категории В обладают независимой эффективностью, например, в качестве резервной для функций категории А, независимость между системой, выполняющей функции категории А, и системой, выполняющей функции категории В, должна быть подтверждена в соответствии с требованиями настоящего стандарта.

6.2.4 Функциональная валидация функций контроля и управления, важных для безопасности, должна проводиться, используя подходящие средства (например, моделирование технологического процесса) и подтверждать правильность применения спецификации функций относительно функциональных и эксплуатационных требований станции. Валидация должна проводиться в соответствии с соответствующими разделами МЭК 61513.

6.2.5 В ходе валидации необходимо продемонстрировать выполнение следующих главных целей безопасности станции, даже если любая из двух независимых систем контроля и управления и назначенная ей группа функций разнообразия будет неэффективна:

a) Валидация системы должна проводиться в соответствии с соответствующими разделами МЭК 61513 и МЭК 60880.

b) Для общей валидации выполняемых функций категории А все действия по валидации должны быть утверждены интегрированным способом при совместном рассмотрении:

1) функциональной валидации (например, применение программного обеспечения, работающего в подходящей аппаратной среде, которая может отличаться от поставляемой системы);

2) проверки интегрированной поставляемой системы в демонстрационной испытательной конфигурации с использованием заводских приемо-сдаточных испытаний;

3) результатов заключительных приемо-сдаточных испытаний на станции.

6.3 Проблемы, связанные с отказами по общей причине на существующих станциях

6.3.1 При модификации системы контроля и управлении на существующей станции исключения из требований настоящего стандарта должны быть обоснованы.

Для обоснования исключений могут быть использованы:

- сопоставление основных слабых сторон и преимуществ модернизации существующих систем контроля и управления;
- физические ограничения, связанные с особенностями существующей станции;
- рассмотрение опыта возникновений отказов по общей причине на атомных станциях;
- повторный анализ проектных основ и их соответствие текущим требованиям к проекту.

7 Инструменты проекта по предотвращению совместных отказов систем контроля и управления

7.1 Принцип независимости

Системы контроля и управления выполняют свои функции безопасности независимо, если постулируемый отказ одной из этих систем не препятствует выполнению другими системами установленных для них функций (см. 3.12).

Для эффективной защиты от отказов по общей причине должны использоваться следующие принципы проектирования:

7.1.1 Цель обеспечения необходимой надежности накладывает требования на проектирование, применение и эксплуатацию систем контроля и управления, которые выполняют функции категории А. Необходимо выполнять конкретные требования к отдельным системам по проектированию системы (см. МЭК 61513), проектированию программного обеспечения (см. МЭК 60880), физическому разделению (см. МЭК 60709) и квалификации (общие положения: см. МЭК 60780 и сейсмической надежности: см. МЭК 60980). Кроме того, требования настоящего стандарта должны выполняться для того, чтобы гарантировать независимое выполнение различных функций безопасности.

7.1.2 Принцип независимых систем контроля и управления предназначен для ограничения влияния отказов по общей причине только на одну систему контроля и управления. Анализ должен проводиться для того, чтобы идентифицировать общие механизмы, которые могут поставить под угрозу

независимость систем контроля и управления. Выявленные общие механизмы должны быть устранены или их число должно быть сокращено.

7.1.3 Проект архитектуры независимой системы контроля и управления должен включать в себя:

a) конкретные пути обработки информации — от определения состояния станции до приведения в действие систем безопасности станции без использования общих компонентов;

b) системы поддержки (например, системы электроснабжения или кондиционирования воздуха), которые состоят из резервных и разделенных подсистем (см. МЭК 60709);

c) средства самоконтроля, которые функционируют независимо для каждой работающей единицы.

7.1.4 Для того, чтобы избежать совместного отказа независимых систем контроля и управления, условия их эксплуатации должны быть проанализированы с целью идентификации общих механизмов срабатывания.

7.1.5 Там, где возможно, предотвращение потенциальных ошибок в спецификации требований к функциям категории А должно использоваться в соответствии с 6.1 (функциональное разнообразие). Эта мера эффективна независимо от используемой технологии контроля и проектирования.

7.2 Проектирование независимых систем контроля и управления

7.2.1 Независимые системы контроля и управления, которые выполняют функции категории А, должны быть спроектированы так, чтобы вероятность появления совместного отказа этих систем из-за одного и того же переходного процесса входного сигнала была сокращена до уровня, при котором эта вероятность стала незначительной для намеченного жизненного цикла станции. Это требование может быть выполнено с использованием мер, гарантирующих разные траектории сигнала (см. 6.1.2 и 7.3).

7.2.2 Независимые системы контроля и управления не должны использовать раздельные компоненты или инструменты, если постулируемый отказ этих общих компонентов или инструментов (например, общее электроснабжение) может вызвать совместный отказ независимых систем контроля и управления.

7.2.3 Использование идентичных аппаратных средств или компонентов программного обеспечения для реализации независимых систем контроля и управления должно быть проанализировано с тем, чтобы удостовериться в незначительном потенциале возникновения отказа по общей причине. В противном случае это использование должно быть ограничено:

- эксплуатацией при различных условиях и нагрузках (главным образом это необходимо, например, для единиц цифровых систем, обрабатывающих различные входные сигналы) и/или

- эксплуатацией, независимой от профиля требования и факторов, влияющих на работу станции (например, от аппаратных средств, которые не подвержены аварийным ситуациям, или программного обеспечения, которое выполняет свои намеченные функции в независимости от обработанных данных).

7.2.4 Если необходимо использование специфических компонентов, зависящих от профиля требований (например, датчиков в защитной оболочке или реле, которые должны быть обеспечены питанием или обесточены в зависимости от конкретных требований), то эти компоненты должны быть пригодны для условий эксплуатации в зависимости от требований (см. МЭК 60780) и подлежать периодическому тестированию (см. МЭК 60671). Применение разнообразных аппаратных средств может иметь положительный результат, но потребность в их разнообразии должна быть проанализирована.

7.3 Применение функционального разнообразия

7.3.1 Для компьютерных систем контроля и управления подверженность отказам по общей причине должна быть проанализирована с использованием оценки потенциального применения и траектории сигнала для следующих отдельных программных модулей:

- применение функционального разнообразия должно использоваться для того, чтобы обеспечить разнообразие «входных сигналов» траектории сигнала. Должно быть рассмотрено и разнообразие других элементов траекторий (например, внутренние состояния);

- исключение для скрытых отказов может иметь место в случае с очень маленькими и простыми программными модулями, анализ дефектов и адекватное тестирование которых могли быть проведены.

7.3.2 Независимые системы контроля и управления не должны выполнять идентичные функции, чтобы сократить возможность возникновения условий, в которых совместный, квазисинхронизированный отказ этих систем может быть вызван переходным процессом одного и того же входного сигнала. Если выполнения идентичных подфункций нельзя избежать в связи с условиями проекта станции, эти

идентичные подфункции должны выполняться, по крайней мере, с входными сигналами от отдельных датчиков.

7.4 Предотвращение распространения отказа через каналы связи

7.4.1 Для того, чтобы справиться с отказом по общей причине, не должно быть связей между независимыми системами контроля и управления, созданных с соблюдением требований по предотвращению отказа по общей причине согласно 6.1.2.

7.4.2 Проект систем контроля и управления, выполняющих функции категории А, должен гарантировать максимально возможную защиту от распространения отказа внутри системы контроля и управления. Для достижения этой цели проекта требуется параллельное применение следующих проектных мер:

a) Системы контроля и управления должны быть разработаны так, чтобы работа системы не подвергалась опасности со стороны центральных подсистем, которые могут, например, предоставлять информацию для отражения на главном пульте управления или поддерживать изменения параметров, отражающих процесс работы станции и, для выполнения таких функций, требуют связи со всеми резервированиями системы контроля и управления, выполняющей функции категории А.

b) Ошибочные данные из дальнейшей обработки в применяемом программном обеспечении должны быть исключены.

c) Все функции, выполняемые программным обеспечением для передачи сообщений, должны осуществляться так, чтобы правильному выполнению этих функций не помешали значения данных зависимых от хода процесса, которые и являются объектами передачи (см. также 8.1).

d) Правильность полученных данных должна проверяться перед дальнейшей обработкой.

e) Физическое разделение резервных подсистем должно быть спроектировано по МЭК 60709.

7.4.3 Обмен входными данными между резервными единицами может создать зависимость между каналами и поэтому он должен быть проанализирован относительно возможности появления отказов по общей причине. Валидация входных данных в режиме он-лайн (например, посредством голосования) должна использоваться как инструмент, препятствующий распространению ошибочных данных. Входные сигналы, которые были определены как ошибочные (например, при выходе за пределы установленных диапазонов) должны быть промаркированы и исключены из дальнейшей обработки.

7.5 Инструменты проекта по защите системы от отказа в результате технического обслуживания

В дополнение к требованиям МЭК 61513 для защиты от отказов по общей причине являются необходимыми следующие специальные требования:

7.5.1 Системы контроля и управления, выполняющие функции категории А, должны анализироваться во время проектирования для того, чтобы продемонстрировать устойчивость системы во время технического обслуживания и при проведении испытаний.

Основные показатели устойчивости системы:

a) Если компоненты процесса могут вызвать проектное событие в случае ложного срабатывания систем контроля и управления, то должны быть предприняты меры по устранению возможности такого ложного срабатывания во время технического обслуживания.

b) Число функций категории А, которые могут быть затронуты одновременно во время технического обслуживания, должно соответствовать принципам проекта безопасности на станции.

7.5.2 Для того, чтобы сократить риск отказа нескольких резервирований, вызванного техническим обслуживанием и он-лайн испытаниями, необходимо использовать инструменты по обнаружению этих ошибок (например, он-лайн мониторинг состояния системы) во время технического обслуживания и средств управления процессом окончания технического обслуживания, при котором система останется в приемлемом состоянии.

7.6 Целостность аппаратных средств системы контроля и управления

Для повышения готовности систем, важных для безопасности, необходима самодиагностика.

Хотя нижеизложенные пункты не относятся непосредственно к отказам по общей причине, их также необходимо рассмотреть.

7.6.1 Во время эксплуатации системы должны использоваться средства самодиагностики (см. МЭК 60880):

a) когда самодиагностика обнаружит отказ, должно быть принято заранее заданное и специально определенное состояние;

b) это состояние должно быть выбрано по принципу «отказоустойчивости», используя анализ предпочтительных действий, которые будут предприняты в случае возникновения отказа. Средства самодиагностики могут приводить в действие системы безопасности, но и также могут предотвратить их несанкционированное ложное срабатывание, если оно может привести к проектному событию;

c) сокращение возможности возникновения отказа системы, вызванного накоплением невыявленных дефектов аппаратных средств.

7.6.2 В отношении активаций систем безопасности, которые были предотвращены или автоматически сработали, если отказ идентифицирован самодиагностикой, должны срабатывать аварийные сигнализации, передающие информацию на главный пульт управления.

7.6.3 Как показывает опыт эксплуатации аналоговых систем контроля и управления в нормальных условиях эксплуатации, модули аппаратных средств с систематическими незначительными производственными дефектами, которые работают, как ожидается во время ввода системы в эксплуатацию, неисправности приводят к увеличению числа отказов в дальнейшем. Для раннего обнаружения систематических неисправностей все отказы аппаратных средств должны быть проанализированы и зарегистрированы так, чтобы персонал технического обслуживания был заранее предупрежден о необходимости принятия мер, прежде чем возникнет отказ по общей причине. (Модули аппаратных средств с производственными дефектами, которые исключают успешный ввод в эксплуатацию, не относятся к возникновению отказов по общей причине).

7.6.4 Компоненты применяемой технологии контроля и управления могут обладать уменьшенной частотой повреждений в начале своего жизненного цикла. Поэтому устранение дефектов компонента или системы по обеспечению безопасности проводят до начала его(ее) эксплуатации.

7.7 Зависимость от взаимосвязей с внешними датами или сообщениями

7.7.1 Системы контроля и управления, выполняющие функции категории А, должны разрабатываться так, чтобы их эксплуатация не зависела от таких внешних влияний, как определенные календарные даты.

7.7.2 Требования к предотвращению доступа к системам контроля и управления постороннему персоналу и непреднамеренному отказу из-за неправильных действий уполномоченных сотрудников — в соответствии с МЭК 60880.

7.8 Гарантия физического разделения и эксплуатационной надежности

Необходимо обеспечить достаточную надежность систем управления и контроля, выполняющих функции категории А. Все известные механизмы отказа, вызванные внешними условиями, ставят под угрозу аппаратные средства системы контроля и управления. Для предотвращения появления отказа по общей причине необходимо следовать требованиям, указанным в опубликованных стандартах. Поэтому эта группа механизмов отказа упомянута только для обеспечения полноты содержания настоящего стандарта.

Для предотвращения отказов по общей причине, возникающих из-за внешних факторов, для систем, выполняющих функции категории А, соответствующие требования содержатся в:

МЭК 60780 — (общая) квалификация оборудования;

МЭК 60980 — сейсмическая квалификация;

МЭК 61000-4 — электромагнитная совместимость;

МЭК 60709 — к разделению и изоляции.

8 Устойчивость к постулируемым скрытым дефектам программного обеспечения

8.1 Цифровые системы контроля и управления, выполняющие функции категории А, должны разрабатываться в соответствии с МЭК 61513, чтобы системы могли работать друг с другом независимо от профиля запросов. Нижеследующие требования к программному обеспечению являются дополнительными к требованиям МЭК 60880 и совместимыми с ними. Эти требования сокращают возможность данных, зависящих от переходных процессов в работе станции, вызывать скрытые дефекты программного обеспечения:

a) Прикладное и системное программное обеспечение должны быть разделены так, чтобы алгоритмическую обработку данных о работе станции полностью выполняло прикладное программное обеспечение.

b) Выполнение функций программного обеспечения системы не должно подвергаться влиянию данных, которые прямо или косвенно зависят от состояния станции (например, передача данных о процессе в виде битовых строк). В дополнение к этому общему требованию необходимо следовать требованиям, представленным в В.2 приложения В МЭК 60880 и включающим в себя:

- постоянную периодическую обработку прикладных функций;
- постоянство загрузки процесса и коммуникаций;
- предотвращение прерываний, вызванных данными о процессе (для ограниченного использования прерываний, см. В.2 приложения В МЭК 60880).

8.2 Прикладное программное обеспечение должно разрабатываться так, чтобы быть устойчивым к неверным единичным или групповым входным сигналам или ложным краткосрочным переходным процессам входных сигналов, — к таким, чтобы гарантировалось безопасное функционирование, но исключались случайные срабатывания.

8.3 Некорректные или поврежденные входные сигналы должны быть идентифицированы интерактивно. Если поврежденные сигналы идентифицируются и обрабатываются путем сравнения с резервной информацией, то появившаяся зависимость между резервными подсистемами должна быть проанализирована так же и на возможность появления отказов по общей причине.

8.4 Если система контроля и управления выполняет различные функции, и один или несколько сигналов, используемых одной функцией, будут некорректными, то все другие функции с неискаженными входными сигналами затронуты быть не должны.

8.5 Программное обеспечение должно разрабатываться так, чтобы обеспечивалась безопасность даже в случае многократных совместных отказов или явных отказов входных сигналов. Обеспечение безопасности должно применяться для предотвращения проектного события, вызванного ложным срабатыванием, и отключения сигнализации, как определено в функциональных требованиях к системе.

9 Требования к предотвращению отказа системы из-за технического обслуживания во время эксплуатации

9.1 Для систем контроля и управления, выполняющих функции категории А, одновременность действий должна быть ограничена единственным резервированием с тем, чтобы избежать отказа более чем одной резервной цепи, канала или подсистемы (например, посредством блокировок или административных процедур).

9.2 Влияния технического обслуживания во время работы под нагрузкой должны быть проанализированы, чтобы предотвратить отказы других систем контроля и управления, выполняющих функции категории А, которые не подвергались данному техническому обслуживанию.

9.3 В случаях замены аппаратных средств должна быть обеспечена соответствующая квалификация свойств аппаратных средств и программного обеспечения и проведена верификация совместимости замененных и существующих компонентов с тем, чтобы надежность системы контроля и управления не снижалась и не возникали новые виды отказа. Достаточность квалификационных мер должна быть подтверждена, принимая во внимание сложность компонентов.

9.4 Для того, чтобы уменьшить влияние снижения надежности компонента из-за старения, должны приниматься во внимание сроки службы компонентов контроля и управления.

Приложение А
(справочное)

Связь между МЭК 60880 и настоящим стандартом

Во время завершающей стадии разработки МЭК 60880 (издание 2, 2006 г.) рабочая группа А3 подкомитета ПК 45А решила включить в него раздел 13 МЭК 60880-2:2000 «Об отказах по общей причине». Предложение о включении определенных требований по предотвращению отказов программного обеспечения по общей причине из раздела 8 настоящего стандарта в приложение В МЭК 60880 было отклонено.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60671	—	*
МЭК 60709	IDT	ГОСТ Р МЭК 60709—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
МЭК 60780	—	*
МЭК 60880	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютеризированных систем, выполняющих функции категории А»
МЭК 60980	—	*
МЭК 61000-4 (все части)	—	*
МЭК 61226	IDT	ГОСТ Р МЭК 61226—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
МЭК 61513:2001	IDT	ГОСТ Р МЭК 61513—2011 «Атомные станции. Контроль и управление, важные для безопасности. Общие требования»
Руководство по безопасности МАГАТЭ NS-G-1.3	—	**
Руководство по безопасности МАГАТЭ SG-D11	—	**
Справочник по безопасности МАГАТЭ, издание 2.0, 2006	—	**

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

** Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод текста документа на русский язык, который доступен на http://www.iaea.org/.

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

IDT — идентичные стандарты.

УДК 621.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; отказ по общей причине; независимость; физическое разделение; резервирование

Редактор *В.Н. Копысов*
Технический редактор *Н.С. Грошанова*
Корректор *В.И. Варенцова*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 31.05.2012. Подписано в печать 20.06.2012. Формат 60x84 1/8. Гарнитура Ариал. Усл. печ. л. 2,79.
Уч.-изд. л. 2,10. Тираж 86 экз. Зак. 562.

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

gost.e-ecolog.ru