ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61500— 2012

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Передача данных в системах, выполняющих функции категории А

IEC 61500:2009
Nuclear power plants — Instrumentation and control important to safety — Data communication in systems performing category A functions
(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 Открытым акционерным обществом «Всероссийский научно-исследовательский институт атомных электростанций» (ОАО «ВНИИАЭС») и Автономной некоммерческой организацией «Измерительно-информационные технологии» (АНО «Изинтех») на основе аутентичного перевода на русский язык стандарта, указанного в пункте 4, 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 сентября 2012 г. № 292-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61500:2009 «Атомные станции. Системы контроля и управления, важные для безопасности. Передача данных в системах, выполняющих функции категории А» (IEC 61500:2009 «Nuclear power plants — Instrumentation and control important to safety — Data communication in systems performing category A functions»).

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 1
3 Термины и определения 2
4 Обозначения и сокращения 3
5 Общие положения 3
5.1 Принципы выбора методов и оборудования передачи данных 3
5.2 Функциональные требования 3
5.3 Требования к рабочим характеристикам 3
5.4 Обнаружение отказов 4
5.5 Связь в пределах выделенного участка 4
5.6 Интерфейсы с системами более низкой важности для безопасности 4
6 Физическое разделение и изоляция 4
6.1 Электрическая изоляция 4
6.2 Физическое разделение 4
7 Функциональная независимость 5
8 Надежность (отказоустойчивость) 5
8.1 Самоконтроль и смягчение отказов 5
8.2 Испытание 6
8.3 Предупреждение отказов (включая ООП) 6
9 Квалификация 7
10 Обслуживание и изменение 7
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации 8
Библиография 9

Введение

a) Технические положения, основные вопросы и организация стандарта

Оборудование связи для передачи оперативных данных станции может быть упрощено при помощи проводного соединения распределенных систем для контрольно-измерительной аппаратуры, устройств управления, защиты и контроля, необходимых для безопасной эксплуатации атомных станций. Такой способ соединения может давать системам преимущества перед прямым кабельным соединением в части электрической изоляции, снижения пожароопасности кабелей или по иным причинам. В распределенной компьютеризированной системе оборудование связи является неотъемлемой частью самой системы. Передача данных обычно имеет важнейшее значение для реализации систем контроля и управления, важных для безопасности на атомных станциях.

Настоящий стандарт предназначен для использования операторами атомных станций (энергетическими компаниями), изготовителями оборудования связи, специалистами по оценке систем и лицензирующими организациями.

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

МЭК 61500 является документом МЭК ПК 45А третьего уровня, касающимся характерных проблем передачи данных для оборудования, выполняющего функции категории А.

МЭК 61500 должен рассматриваться совместно с МЭК 61513, являющимся надлежащим документом МЭК ПК 45А, дающим представление об общих требованиях к системам контроля и управления, важным для безопасности, МЭК 60880, являющимся надлежащим документом МЭК ПК 45А, дающим представление об аспектах программного обеспечения для компьютеризированных систем, выполняющих функции категории А, и МЭК 60987, являющимся надлежащим документом МЭК ПК 45А, дающим представление об аспектах технических средств для компьютеризированных систем.

Более подробное описание структуры серии стандартов МЭК ПК 45А см. в перечислении d) настоящего введения.

c) Рекомендации и ограничения по применению настоящего стандарта

Важно отметить, что настоящий стандарт не устанавливает дополнительных функциональных требований для систем обеспечения безопасности.

В настоящем стандарте даны особые рекомендации по следующим аспектам:

- требования к передаче данных в системах, выполняющих функции категории А;
- требования к передаче данных между частями (секциями) систем, выполняющих функции категории А;
- требования к передаче данных от систем, выполняющих функции категории А, в системы более низкой важности для безопасности;
- требования к надежности передачи данных.

Для гарантии того, что настоящий стандарт останется актуальным и в будущем, акцент делается скорее на принципы, чем на конкретные технологии.

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. Передача данных в системах, выполняющих функции категории А

Nuclear power plants.
Instrumentation and control important to safety.
Data communication in systems performing category A functions

Дата введения — 2013 –06 — 01

1 Область применения

Настоящий стандарт устанавливает требования к передаче данных в системах, выполняющих функции категории А на атомных станциях.

Настоящий стандарт также устанавливает требования к интерфейсу для передачи данных между оборудованием, выполняющим функции категории А, и другими системами, включая системы, выполняющие функции категории В и С, и функции, не важные для безопасности.

Область применения настоящего стандарта ограничивается рассмотрением передачи данных в системах контроля и управления станции и не охватывает связь посредством телефона, радио, голоса, факса, электронной почты, систем оповещения и т. д.

Область применения настоящего стандарта не распространяется на внутреннее функционирование и подробную техническую спецификацию оборудования передачи данных. Настоящий стандарт также неприменим к внутренним соединениям и передаче данных блока обработки данных, его памяти и логике управления, внутренней обработке в компьютеризированных системах контроля и управления.

Требования к функциям и свойствам оперативной передачи данных станции в настоящем стандарте приведены в виде ссылок на МЭК 60880 и МЭК 60987, разработанных в структуре МЭК 61513. Настоящий стандарт предусматривает классификацию функций связи в соответствии с МЭК 61226, который, в свою очередь, предусматривает квалификацию по условиям окружающей среды и сейсмической безопасности (т. е. окружающей среды, в которой для эксплуатации необходима функция безопасности) в соответствии с МЭК 60780 и МЭК 60980.

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 публикации используют последнее издание указанного документа, включая любые изменения.

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

МЭК 60780:1998 Атомные станции. Электрическое оборудование системы безопасности. Квалификация (IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification)

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

Издание официальное

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

МЭК 60987:2007 Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризированных систем (IEC 60987:2007, Nuclear power plants — Instrumentation and control systems — Important to safety — Hardware design requirements for computer-based systems)

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

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

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

МЭК 62340:2007 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 (CCF)]

Руководство МАГАТЭ NS-G-1.3:2002 Системы контрольно-измерительных приборов и управления, важные для безопасности атомных электростанций. (IAEA NS-G 1.3:2002, Instrumentation and control systems important to safety in nuclear power plants)

3 Термины и определения

В настоящем стандарте применены термины по МЭК 60880, глоссарию безопасности МАГАТЭ и руководству МАГАТЭ по безопасности NS-G-1.3, а также следующие термины с соответствующими определениями:

3.1 **канал связи** (communication channel): Логическая связь между двумя конечными точками в системе передачи информации.

[МЭК 61784-3:2007]

3.2 **узел связи** (communication node): Точка связи в сети передачи информации, в которой данные передаются по каналам связи в эту точку или из нее в другие точки сети.

3.3 **система связи** (communication system): Совокупность технических средств, программного обеспечения и среды передачи данных, позволяющая передачу сообщений (прикладной уровень ИСО/МЭК 7498) от одного приложения к другому.

[МЭК 61784-3:2007]

3.4 **передача данных** (data communication): Обмен данными между узлами связи через каналы связи.

3.5 **оборудование передачи данных** (data communication equipment): Вариант реализации части устройства в зависимости от среды передачи данных, модуляции и кодирования для устройства, соединенного с магистралью передачи данных, включая части более низкого физического уровня в устройстве.

[МЭК 61784-3:2007, модифицировано]

3.6 **сообщение** (message): Упорядоченный ряд цифровых состояний в определенных группах, используемый для передачи информации.

[МЭК 61784-3:2007, модифицировано]

3.7 **протокол** (protocol): Соглашение о форматах данных, временны́х последовательностях и устранении ошибок при обмене данными в системах связи.

[МЭК 61158-3-19:2007]

3.8 **процессор** (блок обработки данных) (processing unit): Один или более модулей (ядер) обработки данных, инструкции которых предназначены для управления сетевыми или коммуникационными функциями, в данном конкретном стандарте передачи данных.

4 Обозначения и сокращения

В настоящем разделе применены следующие обозначения и сокращения:
ООП — отказ по общей причине;
ЭМС — электромагнитная совместимость;
АХПО — анализ характера и последствий отказов;
ОК — обеспечение качества.

5 Общие положения

5.1 Принципы выбора методов и оборудования передачи данных

Оборудование связи должно соответствовать требованиям к системам, выполняющим функции категории А.

Примечание — Для того чтобы гарантировать приемлемость для использования в ядерной технике, допускается применять один из следующих принципов выбора методов и оборудования передачи данных:

- использование протоколов, реализующих меры обеспечения безопасности;
- использование протоколов промышленного стандарта с дополнительными уровнями безопасности;
- использование протоколов, где более высокие уровни протокола, реализующие небезопасные или ненужные функциональные возможности, удаляют или заменяют уровнями с сокращенной и безопасной функциональностью.

Аппаратное и программное обеспечение должно быть аттестовано (см. раздел 9).

5.2 Функциональные требования

Как правило, каждый канал связи для передачи данных является частью общей системы, выполняющей сервисные функции сбора и воспроизведения информации, управления или защиты атомной станции.

Для непрерывной работы оборудование, выдающее циклические данные по каналу связи, не должно зависеть от получения подтверждающих сообщений от получателя.

Каналы передачи данных должны распределяться не динамически в течение времени работы системы, а статически и быть определены проектом системы.

Все сообщения прикладного программного обеспечения должны передаваться периодически в пределах предопределенной вариации продолжительности цикла.

Сообщения должны иметь фиксированную длину, определенную проектом.

Система связи должна позволять пересылку и получение сообщений от измерительных приборов или другого внестанционного оборудования с помощью канала связи в пределах заданного интервала времени наряду с информацией о состоянии целостности данных (если это реализовано).

Топология сети передачи данных и управление доступом к среде передачи данных должны быть спроектированы и реализованы так, чтобы избегать ООП автономных систем или подсистем (см. 8.3).

Данные могут распределяться посредством передачи в резервированные системы, чтобы обеспечить непрерывную эксплуатацию оборудования при повреждении одной системы.

Угрозы нарушения безопасности в результате использования передачи данных должны быть учтены в планах по обеспечению безопасности в соответствии с МЭК 61513.

5.3 Требования к рабочим характеристикам

Каналы связи для передачи данных должны обеспечивать достаточную производительность, которая гарантирует, что любое сообщение, отправленное из любого узла связи, будет своевременно получено намеченным узлом назначения.

Передача данных должна отвечать требованиям функций. Используемые механизмы и протоколы должны гарантировать, чтобы любая задержка, которая может возникнуть во время связи или доступа к оборудованию связи, была известна и ограничена проектом.

Каналы связи должны быть проверены на соответствие заданным требованиям по отклику в реальном времени к выполняемым функциям категории А при вероятных наихудших условиях. Требуемый отклик в реальном времени и наихудшие условия должны быть обоснованы проведенным анализом. Должны использоваться детерминированные системы связи, чтобы нагрузка линий связи не менялась независимо от производственных условий.

Там, где оборудование связи используется для ручного управления станцией и индикации через пульт управления, промежуток времени от приведения в действие физического переключателя или программируемого устройства управления до подтверждения действия индикацией изменившегося состояния на пульте управления следует оценивать при всех потенциальных обстоятельствах, включая наихудшие условия.

5.4 Обнаружение отказов

Отказы аппаратного обеспечения оборудования связи необходимо обнаруживать и сообщать о них. Обнаруженные отказы оборудования связи, приводящие к недопустимой деградации функций ядерной безопасности системы контроля и управления, должны отображаться операторам станции в пунктах управления.

Передача данных, включая работу функций реагирования на ошибки (если используются), должна пройти верификацию и валидацию до эксплуатационного использования оборудования для выполнения функций категории А.

5.5 Связь в пределах выделенного участка

Передача данных на отдельном участке (шлейфе) должна быть защищена от неблагоприятного влияния из-за пределов участка. Таким образом, сообщения на участке должны передаваться непосредственно от передающего узла связи к принимающему узлу, не затрагивая оборудования связи вне участка.

Передача данных на участке должна быть отделена от других участков.

Однако связь между участками может быть приемлема, если ее требует использование мажоритарной логики.

5.6 Интерфейсы с системами более низкой важности для безопасности

Оборудование связи систем, выполняющих функции категории А, должно быть отделено от оборудования связи систем, выполняющих только функции более низкой категории.

Если для станционных систем различных категорий требуется связь по каналам передачи данных, то поток данных станции должен идти от функций категории А к функциям более низких категорий.

Следует предотвращать поток данных от функций более низких категорий к функциям категории А, если только не предусмотрена такая конструкция канала связи, чтобы соединение такого рода не могло неблагоприятно повлиять на функции категории А.

6 Физическое разделение и изоляция

6.1 Электрическая изоляция

Электрическая изоляция систем, выполняющих функции категории А, соединенных каналами связи с другими системами, должна рассматриваться в соответствии с МЭК 60709. Степень электрической изоляции будет зависеть от напряжений имеющихся источников питания станции, национальной практики и специализированных требований станции.

Примечание — Один из методов достижения высокой степени электрической изоляции — метод достижения посредством оптоволоконных соединений или оптоэлектронных изоляторов.

Должна быть продемонстрирована соответствующая изоляция между оборудованием передачи данных и подключенным оборудованием. Этой изоляции должно быть достаточно для предотвращения неблагоприятного влияния неисправностей подключенного оборудования и кабелей на работу оборудования передачи данных. В подключенное оборудование входят датчики, контакты, источники электроснабжения и прочее оборудование связи.

6.2 Физическое разделение

Оборудование связи должно быть спроектировано так, чтобы отказы не распространялись из одной части оборудования в другую часть или в другую систему. В МЭК 60709 представлены требования к физическому разделению оборудования и, в особенности, к передаче данных от оборудования, выполняющего функции одной категории, к оборудованию, выполняющему функции другой категории.

В отношении кабелей каналов связи, важных для безопасности, должны применяться требования МЭК 60709.

В качестве предпочтительного метода физического разделения и защиты кабелей каналов связи, несущих электрические или оптические сигналы, следует использовать специализированные кабельные оболочки или коробы, обеспечивающие адекватную защиту от факторов риска.

В системе могут потребоваться резервные маршруты для связи, от которых может потребоваться обеспечение резервирования на случай возникновения факторов риска, таких, например, как пожар, способных повлиять на локализованный участок. Резервированное оборудование, обеспечивающее защиту от такой физической угрозы, должно быть отделено физически.

Примечание — Требования по преодолению отказов по общей причине приведены в МЭК 62340.

7 Функциональная независимость

Для получения и передачи данных от отдельных блоков обработки данных и к ним должны быть предусмотрены модули программного обеспечения, имеющие интерфейсы установленного типа с сетью передачи данных, системным и прикладным программным обеспечением соответствующего блока обработки данных, чтобы избежать распространения неисправности.

В проекте должны использоваться отдельные модули программного обеспечения для численных и логических операций, выполняемых над сигналами и содержимым сообщений, и отдельные модули — для операций проверки сообщений и передачи данных. Это упростит верификацию и валидацию.

8 Надежность (отказоустойчивость)

8.1 Самоконтроль и смягчение отказов

8.1.1 Обнаружение ошибок связи

Оборудование связи должно проверять целостность передаваемых данных, чтобы подтвердить правильную передачу или зарегистрировать/сообщить о сбоях при передаче.

Оборудование связи должно иметь технические средства обнаружения ошибок согласно требованиям 4.2, перечисление d) МЭК 60987 и 4.8 МЭК 60880. Эти технические средства должны гарантировать, что ошибки передачи данных будут обнаружены и при этом ошибочные данные не повлияют на качество исполнения функций категории А. В частности, должны решаться следующие проблемы, связанные с:

a) ошибочной вставкой единичных битов или группы битов в передаваемое сообщение;

b) искажением битов передаваемого сообщения;

c) передачей устаревших данных;

d) потерей сообщения.

8.1.2 Реакция на отказ

При обнаружении неисправностей связи системы контроля и управления, выполняющие функции категории А, должны предпринимать надлежащие действия.

При обнаружении отказов оборудования связи должны быть предприняты соответствующие автоматические меры, например:

a) изоляция неисправных каналов связи;

b) индикация неисправного оборудования для оповещения операторов об отказе (см. также 5.4).

Должно быть точно определено действие, которое следует предпринять при обнаружении отказов, например, регистрация, предупреждение ремонтной бригаде, сигнализация для выполнения немедленных действий по исправлению или смягчению последствий отказа.

Частью процесса обоснования проекта должен быть систематический анализ оборудования и процессов передачи данных с помощью соответствующих методов, например, анализа характера и последствий отказов (FMEA) относительно последствий отказов для функций категории А.

Отказы или нарушения функционирования одиночного узла связи не должны влиять на готовность и надежность системы контроля и управления.

В процессе проектирования должно быть рассмотрено потенциальное влияние отказа любого узла или канала связи на исполнение функций категории А, и этот анализ должен быть документально зафиксирован. Должны быть определены все необходимые действия, которые будут предприняты си-

стемой при обнаружении отказа, например, зарегистрировать отказ, выдать сигнал тревоги или перевести станцию в безопасное состояние.

Каналы связи должны быть устойчивы к «безопасным» ошибкам, таким как пропущенное сообщение или ошибка в одиночном сообщении, при условии, что частота таких ошибок не настолько высока, чтобы поставить под угрозу исполнение функций категории А. Такие «безопасные» ошибки не должны приводить к отключению канала, но эти ошибки должны регистрироваться системой.

8.2 Испытание

К каналам связи класса 1 должны применяться соответствующие требования к испытаниям, приведенные в разделе 10 МЭК 60987. Также к каналам связи систем, выполняющих функции категории А, должны применяться требования 7.10 (контролепригодность), 7.11 (технологические байпасы) и 7.12 (устройства управления доступом к оборудованию систем защиты) руководства по безопасности МАГАТЭ NS-G-1.3.

Исполнение функций передачи данных должно быть проверено прежде, чем оборудование будет введено в полное оперативное использование. Должны быть охвачены следующие аспекты функциональности системы:

a) обработка ошибок передачи;

b) правильная работа при максимальных скоростях передачи данных.

В МЭК 60880 и МЭК 60987 содержится требование о том, что система передачи данных должна иметь способность к самопроверке (см. 8.1). В течение срока службы оборудования должны быть предусмотрены дополнительные периодические испытания в дополнение к самопроверкам, как это требуется для снижения вероятности необнаруженных аппаратных отказов, ставящих под угрозу исполнение функций категории А, например:

1) изменение состояния или значения входных сигналов и контроль изменения в принимающем оборудовании;

2) прерывание передачи и подтверждение того, что принимающее оборудование это обнаружит и предпримет надлежащие действия.

Примечание — По соображениям ядерной безопасности такое испытание может быть нежелательным при работе на мощности.

Для эксплуатационного использования оборудование связи должно пройти функциональные испытания в соответствии с 4.79 — 4.96 руководства по безопасности МАГАТЭ NS-G-1.3. Испытание модулей оборудования должно проводиться во время заводских или эксплуатационных испытаний на площадке либо должно быть представлено доказательство предыдущих типовых испытаний в соответствии с 5.3 МЭК 60780.

8.3 Предупреждение отказов (включая ООП)

На оборудование передачи данных могут повлиять условия, которые вызывают отказ нескольких резервированных частей системы одновременно. Для того чтобы устранить или минимизировать возможность одновременных отказов нескольких модулей от факторов риска, при которых система обязана сохранять работоспособность, необходимо рассмотреть следующие потенциальные риски:

- сейсмическое возмущение или другие соответствующие внешние факторы риска;
- огонь, дым или затопление в зонах нахождения оборудования или прокладки кабеля;
- утеря контроля состояния окружающей среды, теплоснабжения и вентиляции;
- чрезмерное излучение или другие внешние по отношению к оборудованию факторы и
- факторы, внутренние по отношению к самому оборудованию.

Кабельные короба, содержащие кабели для передачи данных между разделенными резервированиями/каналами систем, должны быть спроектированы и разделены в соответствии с требованиями МЭК 60709 так, чтобы возможные факторы риска были ограничены и соблюдалась заданная отказоустойчивость для системы контроля и управления в целом.

Передача данных должна быть рассчитана на предотвращение распространения неисправности, например, путем передачи поврежденных данных (см. 7.4, МЭК 62340).

Принимаемые во внимание потенциальные отказы и заявляемые свойства, нацеленные на предотвращение или смягчение этих отказов, должны быть проанализированы и документально зафиксированы.

Примечание — Требования по преодолению отказов по общей причине приведены в МЭК 62340.

9 Квалификация

Аппаратные средства связи систем класса 1 должны соответствовать установленным критериям согласно соответствующим требованиям МЭК 60780 (квалификация по условиям окружающей среды), МЭК 60980 (квалификация на сейсмическую безопасность, если оборудование должно проходить квалификацию на сейсмическую безопасность) и соответствующего стандарта ЭМС серий стандартов МЭК 62003 или МЭК 61000 (испытание ЭМС).

Программное обеспечение связи для системы, выполняющей функции категории А, должно быть разработано, проверено и утверждено в соответствии с ядерными стандартами (например, МЭК 60880) или другими соответствующими стандартами (например, стандартами серии МЭК 61508). Пригодность избранного стандарта для квалификации должна быть проанализирована и обоснована в документации установленной формы.

10 Обслуживание и изменение

Аппаратные средства и программное обеспечение связи систем, выполняющих функции категории А, должны обслуживаться и видоизменяться в соответствии с МЭК 61513, МЭК 60880 и МЭК 60987.

Если один из узлов связи выходит из строя, должна быть возможность его быстрой замены без снятия энергоснабжения. Замену узла связи следует проводить простым образом без неблагоприятного воздействия на работоспособность системы и в пределах заданной готовности системы.

Изменения оборудования передачи данных должны проводиться согласно строгим процедурам процесса модификации станции.

Изменения должны быть основаны на четких требованиях. Должно быть подтверждено, что эти изменения соответствуют первоначальным требованиям безопасности, функциональности и производительности оборудования передачи данных посредством надлежащей верификации, как предусмотрено в соответствующих случаях МЭК 61513, МЭК 60880 или МЭК 60987.

После внесения изменений путем испытаний до установки на станции (например, на репрезентативном испытательном стенде для функционального испытания) и после установки в запланированную систему (например, на соответствие требованиям производительности системы и требованиям к интерфейсу) (см. 8.2) должно быть доказано, что передача данных соответствует функциональным требованиям и требованиям производительности.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60709	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 компьютерных систем, выполняющих функции категории А»
МЭК 60980	—	*
МЭК 60987	—	*
МЭК 61000 (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	IDT	ГОСТ Р МЭК 61513—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
МЭК 62340	—	*
МАГАТЭ NS-G-1.3	—	**

* 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 gost.e-ecolog.ru

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

IDT — идентичные стандарты.

Библиография

[1]	IEC 60068 (all parts)	Environmental testing
[2]	IEC 60721 (all parts)	Classification of environmental conditions
[3]	IEC 60964	Nuclear power plants — Control rooms — Design
[4]	IEC 60965	Nuclear power plants — Control rooms — Supplementary control points for reactor shutdown without access to the main control room
[5]	IEC 61158-3-19	Industrial communication networks — Fieldbus specifications — Part 3-19: Data-link layer service definition — Type 19 elements
[6]	IEC 61508-1	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements
[7]	IEC 61508-2	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
[8]	IEC 61508-3	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements
[9]	IEC 61508-4	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations
[10]	IEC 61784-3	Industrial communication networks — Part 3: Functional safety fieldbuses
[11]	IEC 62003	Nuclear power plants — Instrumentation and control important to safety — Requirements for electromagnetic compatibility testing
[12]	IEC 62138	Nuclear power plants — Instrumentation and control important to safety — Saftware aspects for computer-based systems performing category B or C functions
[13]	IEC 62241	Nuclear power plants — Main control room — Alarm functions and presentation
[14]	ISO/IEC 7498	Information processing systems — Open systems interconnection — Basic reference model

УДК 621.311.25:006.354 ОКС 27.120.20

Ключевые слова: атомная станция; система контроля и управления, важная для безопасности АС; передача данных; система связи; категория А функции безопасности; физическое разделение; изоляция; функциональная независимость; отказоустойчивость

Редактор *В.Н. Копысов*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *А.В. Бестужевой*

Сдано в набор 21.11.2012. Подписано в печать 19.12.2012. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,35. Тираж 90 экз. Зак. 1125.

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