ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 61500— 2021

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНОЙ СТАНЦИИ

Передача данных в системах, выполняющих функции категории А

(IEC 61500:2018, Nuclear power plants — Instrumentation and control systems important to safety — Data communication in systems performing category A functions, IDT)

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 декабря 2021 г. № 1820-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 61500:2018 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Передача данных в системах, выполняющих функции категории А» (IEC 61500:2018 «Nuclear power plants — Instrumentation and control systems important to safety — Data communication in systems performing category A functions», IDT).

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

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

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

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

6 ВЗАМЕН ГОСТ Р МЭК 61500—2012

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

© IEC, 2018
© Оформление. ФГБУ «РСТ», 2022

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 4
5 Общие требования 4
5.1 Принципы выбора методов и оборудования передачи данных 4
5.2 Функциональные требования 4
5.3 Требования к рабочим характеристикам 5
5.4 Связь в пределах выделенного участка и между участками 5
5.5 Интерфейсы для взаимодействия с системами менее важными для безопасности 5
6 Электрическая изоляция и физическое разделение 5
6.1 Электрическая изоляция 5
6.2 Физическое разделение 6
7 Функциональная независимость 6
8 Надежность (отказоустойчивость) 6
8.1 Самоконтроль и смягчение последствий отказов 7
8.2 Испытания 8
8.3 Предупреждение отказов (включая ООП) 8
8.4 Кибербезопасность 8
9 Квалификация 8
10 Обслуживание и модификация 8
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам 10
Библиография 11

Введение

a) Техническая справка, основные вопросы и организация настоящего стандарта

Оборудование для передачи данных атомной станции (АС) в режиме онлайн может упростить кабельные соединения распределенных систем контрольно-измерительной аппаратуры, управления, защиты и мониторинга, необходимых для безопасной эксплуатации АС. Такие системы связи могут иметь преимущества перед прямым кабельным соединением с точки зрения развязки электрических цепей, 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 АС.

Настоящий стандарт предназначен для использования операторами АС (эксплуатирующими организациями), изготовителями оборудования связи, специалистами по разработке и внедрению систем и лицензирующими организациями.

b) Положение настоящего стандарта в структуре серии стандартов подкомитета 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 следует рассматривать совместно с МЭК 61513, который является надлежащим документом МЭК ПК 45А, устанавливающим общие требования к системам контроля и управления, важным для безопасности, МЭК 60880, который является надлежащим документом МЭК ПК 45А, дающим представление об аспектах программного обеспечения компьютеризированных систем, выполняющих функции категории А, и МЭК 60987, являющимся надлежащим документом МЭК ПК 45А, который касается средств технического обеспечения компьютеризированных систем.

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

c) Рекомендации и ограничения, касающиеся применения настоящего стандарта

Следует отметить, что настоящий стандарт не устанавливает дополнительных функциональных требований к системам 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, к системам, менее важным для безопасности;
- требования к надежности передачи данных.

Для того, чтобы настоящий стандарт оставался актуальным в будущем, акцент делается скорее на принципы, чем на конкретные технологии.

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

Документами высшего уровня серии стандартов МЭК ПК 45А являются МЭК 61513 и МЭК 63046. МЭК 61513 устанавливает общие требования к системам контроля и управления (СКУ) и оборудованию, которое используется для выполнения функций, важных для безопасности АС. МЭК 63046 содержит общие требования к электроэнергетическим системам АС. Он касается систем электроснабжения, включая электроснабжение СКУ. МЭК 61513 и МЭК 63046 следует рассматривать совместно как стандарты одного уровня. МЭК 61513 и МЭК 63046 формируют структуру серии стандартов подкомитета МЭК ПК 45А, а также полный набор общих требований в отношении СКУ и электрических систем АС.

МЭК 61513 и МЭК 63046 содержат прямые ссылки на другие стандарты ПК 45А по общим вопросам, связанным с категоризацией функций и классификацией систем, аттестацией систем, разделением систем, защитой от отказов по общей причине, проектированием пунктов управления, электромагнитной совместимостью, кибербезопасностью, аспектами программного и технического обеспечений компьютерных систем, координацией требований к безопасности и защите, а также управлением старением. Стандарты, на которые имеются прямые ссылки, являются стандартами второго уровня, которые следует использовать совместно с МЭК 61513 и МЭК 63046 как подборку согласованных документов.

К третьему уровню серии стандартов подкомитета МЭК ПК 45А, на которые в МЭК 61513 или МЭК 63046 нет прямых ссылок, относятся стандарты, связанные с конкретным оборудованием, тех-

ническими методами или конкретной деятельностью. Как правило, данные стандарты используют как самостоятельные, однако по общим вопросам в них содержатся ссылки на стандарты второго уровня.

Четвертый уровень серии стандартов, подготовленных подкомитетом МЭК ПК 45А, образуют технические отчеты, не являющиеся нормативными документами.

Серия стандартов подкомитета МЭК ПК 45А последовательно реализует и детализирует принципы и базовые аспекты безопасности, предусмотренные соответствующими стандартами МАГАТЭ и серией документов МАГАТЭ по ядерной безопасности (NSS). Данная серия документов включает, в частности, требования МАГАТЭ SSR-2/1, которые касаются безопасности при проектировании АС, руководство по безопасности МАГАТЭ SSG-30, которое касается классификации систем, конструкций и компонентов АС по безопасности, руководство по безопасности МАГАТЭ SSG-39, которое относится к проектированию СКУ АС, руководство по безопасности МАГАТЭ SSG-34, которое касается проектирования электроэнергетических систем АС и руководство NSS17 по компьютерной безопасности АС. Термины и определения в области безопасности, применяемые в стандартах подкомитета МЭК ПК 45А, соответствуют терминам и определениям, применяемым в МАГАТЭ.

В МЭК 61513 и МЭК 63046 использован такой же формат представления, как и в основном стандарте по безопасности МЭК 61508, в котором рассмотрены общие принципы безопасности жизненного цикла и общая структура систем жизненного цикла. Что касается ядерной безопасности, в МЭК 61513 и МЭК 63046 дана интерпретация общих требований МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 применительно к ядерной отрасли. В этой структуре МЭК 60880, МЭК 62138 и МЭК 62566 соответствуют МЭК 61508-3 применительно к ядерной отрасли. МЭК 61513 и МЭК 63046 ссылаются на стандарты ИСО, а также на документы МАГАТЭ GS-R-3, GS-G-3.1 и GS-G-3.5 по вопросам, связанным с обеспечением качества (ОК).

На втором уровне исходным документом для серии стандартов подкомитета МЭК ПК 45А, касающихся ядерной безопасности, является МЭК 62645. Он основан на актуальных принципах высокого уровня и основных концепциях общих стандартов по безопасности, в частности, ИСО/МЭК 27001 и ИСО/МЭК 27002. Он адаптирует и дополняет эти стандарты, чтобы обеспечить возможность их применения в атомной энергетике, и увязывает с серией стандартов МЭК 62443. Кроме этого, на втором уровне исходным документом для стандартов подкомитета МЭК ПК 45А, касающихся пунктов управления, является МЭК 60964, а для стандартов, касающихся управления старением, — МЭК 62342.

Примечания

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

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНОЙ СТАНЦИИ

Передача данных в системах, выполняющих функции категории А

Instrumentation and control systems important to safety of a nuclear power plant.
Data communication in systems performing category A functions

Дата введения — 2022—09—01

1 Область применения

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

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 ограничена передачей данных в системе контроля и управления безопасности АС и не охватывает связь посредством телефона, радио, голоса, факса, электронной почты, систем оповещения и т. д.

К области применения настоящего стандарта не относятся внутреннее функционирование и подробная техническая спецификация оборудования для передачи данных. Настоящий стандарт неприменим к внутренним соединениям и передаче данных процессора, его памяти и логике управления, а также к внутренней обработке данных компьютеризированных СКУ.

Настоящий стандарт представляет требования к функциям и свойствам передачи оперативных данных АС путем ссылок на МЭК 60880 и МЭК 60987, разработанных в структуре МЭК 61513. Настоящий стандарт предусматривает категоризацию коммуникационных функций в соответствии с МЭК 61226, который, в свою очередь, подразумевает квалификацию по условиям окружающей среды и сейсмической безопасности (т. е. учет окружающей среды, в которой для эксплуатации необходима функция безопасности) в соответствии с IEC/IEEE 60780-323 и МЭК 60980.

2 Нормативные ссылки

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

IEC 60671:2007, Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing (Атомные электростанции. Системы контроля и управления, важные для безопасности. Контрольные испытания)

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

[1)] Действует IEC 60709:2018

Издание официальное

IEC/IEEE 60780-323:2016, Nuclear facilities — Electrical equipment important to safety — Qualification (Объекты использования атомной энергии. Электрооборудование, важное для безопасности. Квалификация)

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

IEC 60980[1)], Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations (Рекомендуемая практика проведения сейсмической квалификации электрооборудования системы безопасности для атомных электростанций)

IEC 60987:2007[2)], Nuclear power plants — Instrumentation and control important to safety — Hardware design requirements for computer-based systems, IEC 60987:2007/Amd.1:2013 (Электростанции атомные. Контрольно-измерительные приборы и системы управления, важные для обеспечения безопасности. Требования к проектированию аппаратуры для компьютерных систем, с Изм. 1:2013)

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

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

IEC 62003[3)], Nuclear power plants — Instrumentation and control important to safety — Requirements for electromagnetic compatibility testing (Атомные станции. Системы контроля, управления и электроэнергетические системы. Требования для испытаний на электромагнитную совместимость)

IEC 62340:2007, Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF) (Электростанции атомные. Системы приборного оснащения и управления, важные для обеспечения безопасности. Требования, позволяющие выдержать отказ по общей причине)

IEC 62566:2012, Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions (Атомные электростанции. Системы контроля и управления, важные для безопасности. Разработка HDL-программируемых интегральных схем для систем, выполняющих функции категории А)

IEC 62645:2014[4)], Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based systems (Электростанции атомные. Контрольно-измерительные приборы и системы управления. Требования к программам безопасности для систем, управляемых ЭВМ)

IEC 62859, Nuclear power plants — Instrumentation and control systems — Requirements for coordinating safety and cybersecurity (Атомные станции. Системы контроля и управления. Требования к координации безопасности и кибербезопасности)

IAEA safety guide No. SSG-39:2016, Design of instrumentation and control systems for nuclear power plants (Проектирование систем контроля и управления атомных электростанций)

3 Термины и определения

В настоящем стандарте применены термины по МЭК 60880, глоссарию МАГАТЭ по безопасности, нормам безопасности МАГАТЭ SSG-39, а также следующие термины с соответствующими определениями:

[1)] Заменен на IEC/IEEE 60980-344:2020.

[2)] Заменен. Действует IEC 60987:2021. Однако для однозначного соблюдения требований настоящего стандарта, приведенного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

[3)] Действует IEC 62003:2020.

[4)] Заменен на IEC 62645:2019. Однако для однозначного соблюдения требований настоящего стандарта, приведенного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

3.1

канал связи[1)] (communication channel): Логическая связь между двумя узлами связи в системе передачи информации.

[МЭК 61784-3:2016, пункт 3.1.8]

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

3.3 **система связи** (communication system): Совокупность технических средств, программного обеспечения и среды распространения, позволяющая передачу сообщений (прикладной уровень по ИСО/МЭК 7498-1) от одного приложения к другому.

3.4 **кибербезопасность** (cybersecurity): Комплекс мероприятий и мер, целью которых является предотвращение, обнаружение и реагирование на:

- злонамеренное раскрытие информации (нарушение конфиденциальности), которая может быть использована для совершения злонамеренных действий, могущих привести к возникновению аварии, небезопасной ситуации или снижению производительности АС;
- злонамеренное модифицирование (нарушение целостности) функций, что может привести к нарушению реализации или целостности задачи, выполняемой компьютеризированными системами контроля и управления (включая потерю контроля), что в свою очередь может привести к возникновению аварии, небезопасной ситуации или снижению производительности АС;
- злонамеренную приостановку или прекращение доступа к передаче информации, данных или ресурсов (включая потерю изображения), что может привести к нарушению реализации задачи, выполняемой СКУ (нарушение работоспособности), что в свою очередь может привести к возникновению аварии, небезопасной ситуации, или снижению производительности АС.

Примечания

1 Данное определение строго соответствует области применения МЭК 62645 и общей структуре документов подкомитета МЭК ПК 45А. Известно, что термин «кибербезопасность» имеет более широкое значение в других стандартах и руководствах, часто включая угрозы, не связанные со злым умыслом, человеческие ошибки и защиту от стихийных бедствий. Эти аспекты, за исключением человеческих ошибок, которые снижают уровень кибербезопасности, не входят в понятие кибербезопасности, используемое в серии стандартов подкомитета МЭК ПК 45А. Более подробную информацию о данных исключениях см. в приложении А МЭК 62645:2014.

2 В настоящем стандарте термины «компьютерная безопасность», «безопасность» и «кибербезопасность» являются синонимами.

[МЭК 62645:2014, пункт 3.6, с изменениями: слова «раскрытие информации» заменены на «злонамеренное раскрытие информации», примечания 1 и 2 изменены]

3.5 **передача данных** (data communication): Обмен цифровой информацией между узлами связи через каналы связи.

3.6 **оборудование передачи данных** (data communication equipment): Материальное воплощение среды (носители), модулирующей и кодируемой части устройства, соединенного с шиной, включая части более низкого физического уровня в устройстве.

[МЭК 61158-2:2014, пункт 3.1.9, с изменениями: слова «полевой шиной» заменены на «шиной»]

3.7 **участок** (division): Совокупность элементов, включая соединения между ними, которые образуют один резервный элемент резервной системы или группу безопасности. Участки могут включать в себя множество каналов.

[МАГАТЭ SSG-39:2016]

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

[МЭК 61784-3:2016, пункт 3.1.26, с изменениями: слово «октеты» заменено на «цифровые состояния в определенных группах»]

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

[МЭК 61158-3-19:2014, пункт 3.3.29]

[1)] *Согласно НП-026-16 канал (системы, функциональной группы) — это часть системы (функциональной группы), выполняющая функцию системы (функциональной группы) в установленном проектом АС объеме.*

4 Обозначения и сокращения

В настоящем стандарте использованы следующие сокращения:
АХПО (FMEA) — анализ характера и последствий отказа;
ОК (QA) — обеспечение качества;
ООП (CCF) — отказ по общей причине;
СКУ(I&C) — система контроля и управления;
ЭМС (EMC) — электромагнитная совместимость

5 Общие требования

5.1 Принципы выбора методов и оборудования передачи данных

Оборудование для передачи данных должно соответствовать требованиям к системам, выполняющим функции категории А.

Для того чтобы гарантировать приемлемость методов и оборудования передачи данных для использования в атомной промышленности, при выборе следует руководствоваться одним из следующих принципов:

- использование протоколов, реализующих меры обеспечения безопасности;
- использование стандартных промышленных протоколов, дополненных уровнями безопасности;
- использование протоколов, где более высокие уровни протокола, реализующие небезопасные или ненужные функции, 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 АС.

Для непрерывной работы оборудование, обеспечивающее данные посредством канала связи, должно осуществлять этот процесс циклически, независимо от получения подтверждающих сообщений от пользователя.

Каналы связи, включая управление и распределение памяти для отправки/получения данных, не должны перераспределяться в динамическом режиме при работе системы, они должны быть распределены статически и предопределены проектом системы.

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

Сообщения должны иметь фиксированную длину, определяемую проектом.

Система связи должна обеспечивать возможность обмена данными по каналам связи с измерительными приборами и другим оборудованием в пределах заданного интервала времени.

Сообщения должны содержать информацию о целостности данных.

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

Необходимо иметь возможность посредством передачи распределять данные в резервные 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 62645.

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 получено намеченным узлом назначения за время, не превышающее установленный максимальный период.

Передача данных должна отвечать требуемым характеристикам в отношении времени отклика и объема данных, которые основаны на функциональных потребностях и проектной архитектуре СКУ. Используемые механизмы и протоколы действий должны гарантировать, что любая задержка, которая может возникнуть во время связи или получения доступа к оборудованию связи, известна и ограничена проектом.

Каналы связи должны быть проверены на соответствие заданным требованиям к реальному времени отклика при выполнении функций категории А в наихудших условиях. Значения требуемого реального времени отклика и наихудшие условия должны быть обоснованы проведенным анализом. Следует использовать детерминированные системы связи, чтобы нагрузка линий связи не менялась независимо от производственных условий.

В случае, когда оборудование связи используют для ручного управления АС 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.

Что касается функций контроля и ручного управления, которые необходимы в аварийных условиях для возврата АС в безопасное состояние, наихудшее время отклика и ограниченное использование ресурсов должны быть подтверждены соответствующими анализами.

5.4 Связь в пределах выделенного участка и между участками

Передача данных в пределах отдельного участка (канала) должна быть защищена от неблагоприятных влияний извне. Так сообщения на участке должны передаваться непосредственно от передающего узла связи к принимающему узлу без участия оборудования связи, находящегося вне участка.

Передача данных на участке должна быть отделена от других участков. Однако связь между участками может быть приемлема с точки зрения логики выбора.

5.5 Интерфейсы для взаимодействия с системами менее важными для безопасности

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

При необходимости коммуникации посредством каналов передачи данных между системами станции, выполняющими функции различных категорий, поток данных АС должен идти только от систем, выполняющих функции категории А к системам, выполняющим функции более низких категорий.

Поток данных от систем с более низкой категорией функций к системам, выполняющим функции категории А, следует предотвращать, если только проектом канала связи не обеспечено отсутствие неблагоприятного влияния такого взаимодействия на выполнение функций категории А.

Если оборудование связи систем, выполняющих функции категории А, сопряжено с системами, менее важными для безопасности, то необходимо применять меры по обеспечению кибербезопасности согласно МЭК 62645 и МЭК 62859.

6 Электрическая изоляция и физическое разделение

6.1 Электрическая изоляция

Электрическую изоляцию систем, выполняющих функции категории А, соединенных каналами связи с другими системами, осуществляют в соответствии с МЭК 60709.

Примечания

1 Степень электрической изоляции зависит от электрического напряжения источников питания АС, национальной практики и специализированных требований АС.

2 Для достижения высокой степени электрической изоляции используют оптоволоконные соединения или оптоэлектронные изоляторы.

Необходимо обеспечить требуемый уровень изоляции между оборудованием передачи данных и сопряженным оборудованием. Этот уровень изоляции должен быть достаточным для предотвращения неблагоприятного влияния дефектов сопряженного оборудования и кабелей на работу оборудования передачи данных. К сопряженному оборудованию относят датчики, контактные соединения, источники электроснабжения и прочее оборудование связи.

6.2 Физическое разделение

Оборудование связи должно быть спроектировано так, чтобы дефекты не распространялись от одной части оборудования к другой части оборудования или к другой системе. В МЭК 60709 установлены требования к физическому разделению оборудования и, в особенности, для случаев передачи

данных от оборудования, выполняющего функции одной категории, к оборудованию, выполняющему функции другой категории.

В отношении кабелей каналов связи, важных для безопасности, следует применять 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 короба, обеспечивающие адекватную защиту от факторов риска.

В системе могут быть предусмотрены резервные маршруты для связи, которые могут потребоваться для дублирования в случае угрозы, например пожара, способного повлиять на локализованном участке. Резервированное оборудование, обеспечивающее защиту от такой физической угрозы, должно быть отделено физически.

Примечание — Требования, касающиеся мер борьбы с отказами по общей причине, приведены в 8.3.

7 Функциональная независимость

Требования, перечисленные ниже, направлены на предотвращение распространения дефектов (неисправностей):

a) независимые модули обработки должны быть спроектированы таким образом, чтобы они продолжали функционировать, даже если партнер по связи вышел из строя.

Примечание — Данное положение означает применение таких мер, как исключение подтверждения установления связи;

b) модули обработки должны обеспечивать отдельные интерфейсы коммуникации для независимых линий связи.

В проекте следует использовать отдельные модули программного обеспечения для обработки прикладных данных и коммуникации.

Примечание — Это уменьшит сложность объекта и упростит верификацию и валидацию.

8 Надежность (отказоустойчивость)

8.1 Самоконтроль и смягчение последствий отказов

8.1.1 Обнаружение ошибок связи

Оборудование связи должно иметь функцию самоконтроля. Информация об обнаруженных отказах должна передаваться в пункт управления. Оборудование связи должно проверять целостность передаваемых данных, чтобы подтвердить правильную передачу или зарегистрировать/сообщить об отказах функции передачи.

Оборудование связи должно иметь технические средства обнаружения ошибок согласно требованиям 6.2 МЭК 60880:2006 или 8.3.9 МЭК 62566:2012. Эти технические средства должны обеспечивать должную гарантию того, что отказы при передаче данных будут обнаружены, чтобы ошибочные данные не повлияли на качество исполнения функций категории А. В частности, функция самоконтроля оборудования связи должна обеспечивать обнаружение:

a) ошибочной вставки единичных битов или группы битов в передаваемое сообщение (относящееся к действующему или неизвестному/неожиданному источнику);

b) искажения битов передаваемого сообщения;

c) передачи устаревших данных (возникающей из-за непредусмотренного повторения старого сообщения);

d) потери сообщения;

e) некорректного направления сообщения;

f) неприемлемой задержки сообщения;

g) неверной последовательности сообщений.

8.1.2 Реакция на отказ

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

Информация об обнаруженных отказах оборудования связи, которые приводят к неприемлемому нарушению функций СКУ, отвечающих за ядерную безопасность, должна поступать в пункты управления к операторам АС.

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

a) изоляция неисправных каналов связи;

b) сигнализация о неисправности оборудования для оповещения операторов об отказе.

Должно быть указано действие, которое следует предпринять при обнаружении отказов для осуществления немедленной корректировки или смягчения последствий отказа, например зарегистрировать соответствующую информацию в журнале, предупредить ремонтную бригаду, подать сигнал тревоги.

Частью процесса верификации проекта должен быть систематический анализ оборудования для передачи данных и эксплуатации программного обеспечения с использованием соответствующих методов, например, АХПО с точки зрения влияния отказов на выполнение функций категории А.

Отказы или нарушения функционирования одиночного узла связи не должны влиять на работоспособность СКУ.

В процессе проектирования должно быть рассмотрено потенциальное влияние отказа любого узла связи на исполнение функций категории А, и результаты этого анализа должны быть задокументированы. Необходимо определить все необходимые действия, которые должна предпринять система при обнаружении отказа, например зарегистрировать отказ, выдать сигнал тревоги или перевести АС в безопасное состояние.

Каналы связи должны быть устойчивы к временным дефектам, таким как пропущенное сообщение или ошибка в одиночном сообщении, при условии, что частота таких дефектов не настолько высока, чтобы поставить под угрозу исполнение функций категории А. Такие временные дефекты не должны приводить к отключению канала, но должны быть зарегистрированы СКУ.

8.2 Испытания

Контрольные испытания каналов связи класса 1 должны соответствовать требованиям, приведенным в разделе 11 МЭК 60987:2007 и МЭК 60671. Вместе с тем, к каналам связи систем, выполняющих функции категории А, следует применять требования 7.35—7.38 (система защиты — технологические байпасы) и 6.153—6.158 (управление доступом к системам, важным для безопасности) руководства по безопасности МАГАТЭ SSG-39:2016.

Исполнение функций передачи данных, включая устранение дефектов, должно быть проверено и подтверждено прежде, чем оборудование будет введено в оперативное использование для выполнения функций категории А. При этом должны быть охвачены следующие аспекты функциональности системы:

a) обработка ошибок передачи;

b) правильная работа при максимальных скоростях передачи данных.

В МЭК 60880, МЭК 60987 и МЭК 62566 содержится требование о том, что система передачи данных должна иметь способность к самоконтролю (см. 8.1.1). В течение срока службы оборудования должны быть предусмотрены дополнительные периодические испытания в дополнение к самоконтролю, необходимые для снижения вероятности не выявленных аппаратных отказов, ставящих под угрозу исполнение функций категории А, например:

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

d) задержка передачи и подтверждение того, что принимающее оборудование обнаружит ее и предпримет надлежащие действия.

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

До ввода в промышленную эксплуатацию оборудование передачи данных должно пройти функциональные испытания в соответствии с 6.78, 6.79 и 6.92 руководства по безопасности МАГАТЭ SSG-39:2016. Испытание модулей оборудования следует проводить во время производственных или пусковых испытаний на площадке АС, либо должно быть представлено доказательство проведенных ранее типовых испытаний в соответствии с 7.4.1 IEC/IEEE 60780-323:2016.

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 при воздействии факторов риска, при которых система обязана сохранять работоспособность, необходимо рассмотреть следующие потенциальные риски:

a) сейсмическое возмущение или другие соответствующие внешние угрозы;

b) пожар, задымление или затопление в зонах нахождения оборудования или кабеля;

c) отказ систем контроля состояния окружающей среды, теплоснабжения и вентиляции;

d) чрезмерное ионизирующее излучение или другие внешние по отношению к оборудованию факторы;

e) факторы, внутренние по отношению к самому оборудованию.

Кабельные короба, содержащие кабели для передачи данных между отдельными резервными каналами/пакетами, должны быть спроектированы и разделены в соответствии с требованиями МЭК 60709, чтобы ограничить возможные факторы риска и соблюсти заданную отказоустойчивость СКУ в целом.

Система передачи данных должна быть спроектирована таким образом, чтобы обеспечить предотвращение распространения отказа в результате, например, передачи поврежденных данных (см. МЭК 62340:2007, 7.4).

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

Примечание — Требования, касающиеся мер борьбы с отказами по общей причине, приведены в МЭК 62340.

8.4 Кибербезопасность

Планирование, разработку, внедрение и эксплуатацию систем передачи данных следует проводить в соответствии с МЭК 62645 и МЭК 62859 на протяжении всего жизненного цикла данных систем.

9 Квалификация

Аппаратные средства связи систем класса 1 должны быть квалифицированы в соответствии с требованиями, установленными IEC/IEEE 60780-323 (квалификация по условиям окружающей среды), МЭК 60980 (квалификация по сейсмической безопасности) и соответствующим стандартом на электромагнитную совместимость, например МЭК 62003 или серией стандартов МЭК 61000 (ЭМС-испытание).

Средства связи систем, выполняющих функции категории А, должны быть разработаны, верифицированы и признаны в соответствии с МЭК 61513, МЭК 60880, МЭК 60987, МЭК 62645 и МЭК 62566. Пригодность стандарта, выбранного для квалификации, должна быть проанализирована и обоснована в документации установленной формы.

10 Обслуживание и модификация

Средства связи систем, выполняющих функции категории А, обслуживают и видоизменяют в соответствии с требованиями МЭК 61513, МЭК 60880, МЭК 60987, МЭК 62645 и МЭК 62566.

При выходе из строя одного из узлов связи должна быть возможность его быстрой замены без прерывания нормального режима работы АС. Замена узла связи должна быть легко осуществима без нарушения и неблагоприятного воздействия на работоспособность системы. В подобных случаях необходимо принять соответствующие меры для подтверждения корректности работы узла связи, который был установлен в качестве замены.

Модификацию оборудования передачи данных следует проводить согласно строгим процедурам модификации АС.

Модификация должна быть основана на четких требованиях. Соответствие первоначальным требованиям безопасности, функциональности и производительности оборудования передачи данных

после его модификации должно быть подтверждено путем надлежащей верификации, как предусмотрено МЭК 61513, МЭК 60880, МЭК 60987, МЭК 62645 и МЭК 62566.

После внесения изменений в систему связи процесс передачи данных должен быть проверен на соответствие функциональным и производственным требованиям путем проведения испытаний до установки на АС (например, на репрезентативном стенде для функционального тестирования) и после установки в запланированную систему (например, на соответствие требованиям производительности системы и требованиям к интерфейсу) (см. 8.2).

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 60671:2007	IDT	ГОСТ Р МЭК 60671—2021 «Системы контроля и управления, важные для безопасности атомных станций. Контрольные испытания»
IEC 60709	IDT	ГОСТ Р МЭК 60709—2011[1)] «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
IEC/IEEE 60780-323:2016	—	*
IEC 60880:2006	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
IEC 60980	—	**
IEC 60987:2007	—	**
IEC 61000 (все части)	IDT	ГОСТ IEC 61000 «Электромагнитная совместимость» (все части)
IEC 61513	IDT	ГОСТ Р МЭК 61513—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 62003	—	**
IEC 62340:2007	—	**
IEC 62566:2012	—	**
IEC 62645:2014	—	**
IEC 62859	—	**
IAEA safety guide No. SSG-39:2016	—	*

* Соответствующий национальный стандарт отсутствует. Текст документа на русском языке доступен на gost.e-ecolog.ru

** Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

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

- IDT — идентичные стандарты.

[1)] Стандарт идентичен IEC 60709:2004, который заменен на IEC 60709:2018.

Библиография

IEC 60068 (all parts)	Environmental testing
IEC 60721 (all parts)	Classification of environmental conditions
IEC 60964	Nuclear power plants — Control rooms — Design
IEC 60965	Nuclear power plants — Control rooms — Supplementary control room for reactor shutdown without access to the main control room
IEC 61158-3-19	Industrial communication networks — Fieldbus specifications — Part 3-19: Data-link layer service definition — Type 19 elements
IEC 61226[1)]	Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions
IEC 61508-1	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements
IEC 61508-2	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements
IEC 61508-4	Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations
IEC 61784-2[2)]	Industrial communication networks — Profiles — Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3
IEC 61784-3	Industrial communication networks — Profiles — Part 3: Functional safety fieldbuses – General rules and profile definitions
IEC 62138[3)]	Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions
IEC 62241	Nuclear power plants — Main control room — Alarm functions and presentation
IEC TR 62987	Nuclear power plants — Instrumentation and control systems important to safety — Use of Failure Mode and Effects Analysis (FMEA) and related methods to support the justification of systems
ISO/IEC 7498 (all parts)	Information technology — Open Systems Interconnection — Basic reference model

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

[2)] Действует IEC 61784-2:2019 «Industrial communication networks — Profiles — Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC/IEEE 8802-3».

[3)] Действует IEC 62138:2018 «Nuclear power plants — Instrumentation and control systems important for safety — Software aspects for computer-based systems performing category B or C functions».

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; передача данных; оборудование передачи данных; система связи; узел связи; канал связи

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 23.12.2021. Подписано в печать 14.01.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru