ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 60965— 2020

РЕЗЕРВНЫЙ ПУНКТ УПРАВЛЕНИЯ АТОМНОЙ СТАНЦИИ, ИСПОЛЬЗУЕМЫЙ ПРИ ОТКАЗЕ БЛОЧНОГО ПУНКТА УПРАВЛЕНИЯ

Общие требования

(IEC 60965:2016, Nuclear power plants — Control rooms — Supplementary control room for reactor shutdown without access to the main control room, IDT)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 февраля 2020 г. № 85-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 60965:2016 «Атомные станции. Пункты управления. Резервный пункт управления для остановки реактора без доступа к блочному пункту управления (IEC 60965:2016 «Nuclear power plants — Control rooms — Supplementary control room for reactor shutdown without access to the main control room», 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 документов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте настоящего стандарта приведены для пояснения текста применяемого международного стандарта

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

6 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, оформление, 2020

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

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 2
4 Сокращения 3
5 Правила проектирования 4
5.1 Общие требования 4
5.2 Основные цели 4
5.3 Принципы безопасности 6
5.4 Принципы учета человеческого фактора при проектировании 8
6 Процесс проектирования 8
7 Функциональное проектирование 9
7.1 Общие требования 9
7.2 Человеческий фактор 9
7.3 Расположение и маршрут доступа 9
7.4 Окружающая среда резервного пункта управления 10
7.5 Пространство и конфигурация 11
7.6 Информационное и контрольное оборудование 11
7.7 Системы связи 11
7.8 Дополнительное оснащение 12
7.9 Тестирование и проверки 12
8 Верификация и валидация системы 13
Приложение А (справочное) Оценка периода времени безопасной передачи управления из блочного пункта управления в резервный пункт управления 14
Приложение ДА (справочное) Сведения о соответствии ссылочных международных документов национальным и межгосударственным стандартам 15
Библиография 16

Введение

a) Технический опыт, основные вопросы и организация стандарта

Стандарт МЭК 60965:1989 был разработан для обеспечения требований, связанных с проектированием резервных пунктов управления (РПУ) атомных станций (АС), обеспечивающих остановку реактора без доступа к блочному пункту управления (БПУ). Первое издание МЭК 60965 широко используется в ядерной отрасли. Однако в 2007 г. было признано, что требования к новым техническим разработкам, особенно к тем, которые основаны на информационных технологиях, должны быть включены в данный стандарт. Было также признано, что связи со стандартом на блочный пункт управления (МЭК 60964) и другими стандартами по этой тематике (т.е. МЭК 61227, МЭК 61771, МЭК 61772, МЭК 61839 и МЭК 62241) должны быть конкретными и обоснованными. В 2009 г. было опубликовано второе издание МЭК 60965.

В июне 2013 г. во время московского совещания эксперты РГ А8 рекомендовали провести ограниченный пересмотр стандарта, чтобы учесть уроки аварии на атомной станции TEPCO Fukushima Daiichi, а также замечания, сформулированные в ходе изучения второго издания окончательного проекта международного стандарта. В ходе пересмотра наименование стандарта было изменено — был введен термин «резервный пункт управления» аналогично наименованию стандарта МАГАТЭ SSR-2/1.

В стандарте МЭК 60965:2016 особое внимание уделяется процессу функционального проектирования резервного пункта управления АС. Предполагают, что стандарт будут использовать проектировщики АС, проектные организации, поставщики, энергетические компании и т.п.

b) Положение стандарта МЭК 60965:2016 в структуре серии стандартов подкомитета МЭК ПК 45А

МЭК 60965 — это документ третьего уровня в структуре серии стандартов подкомитета МЭК ПК 45А, в стандарте рассматривается вопрос о конструкции резервного пункта управления АС.

МЭК 60965 следует применять в комплексе с МЭК 60964, предназначенным для проектирования блочного пункта управления, и упомянутыми выше стандартами. МЭК 60964 является документом, входящим в серию стандартов подкомитета МЭК ПК 45А и содержащим руководства оператора по управлению, верификации и валидации проекта, применению наглядных отображений, функциональному анализу и распределению, а также функциям сигнализации и представления.

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

c) Рекомендации и ограничения в отношении применения настоящего стандарта

Целью настоящего стандарта, подготовленного на основе указанного стандарта МЭК, является представление функциональных требований к конструкциям, которые будут использоваться при проектировании резервного пункта управления атомной станции для удовлетворения требований ее безопасности.

Стандарт предназначен для применения в проектах резервного пункта управления, разработка которых начинается после его публикации. Рекомендации настоящего стандарта могут быть применены для изменений, обновлений и модификаций существующих РПУ.

В соответствии со стандартами безопасности МАГАТЭ в настоящем стандарте приведены специальные рекомендации по следующим аспектам:

- определение составных частей (включая оборудование) БПУ и атомной станции, которые необходимо представить в резервном пункте управления;
- изложение требований по доступу персонала атомной станции в резервный пункт управления при чрезвычайных ситуациях;
- обеспечение безопасной окружающей среды для персонала станции, присутствующего в резервном пункте управления при его эксплуатации;
- предоставление в резервный пункт управления информации о состоянии критических функций реактора;
- передача функций управления и индикации из БПУ в РПУ при чрезвычайных ситуациях;
- независимость и разделение кабелей, используемых РПУ и БПУ;
- обеспечение результатов в достижении безопасного состояния станции при использовании РПУ;
- изложение требований к средствам связи между РПУ и руководством станции.

Для гарантии того, что настоящий стандарт будет актуальным и в будущем, основное внимание в нем уделяется принципиальным вопросам, а не конкретным технологиям.

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

Документом верхнего уровня серии стандартов подкомитета МЭК ПК 45А является стандарт МЭК 61513. Он содержит общие требования безопасности систем контроля и управления и оборудования, которые используются для выполнения функций, важных для безопасности АС. МЭК 61513 структурирует серию стандартов подкомитета МЭК ПК 45А.

МЭК 61513 напрямую ссылается на другие стандарты подкомитета МЭК ПК 45А для общих тем, связанных с категоризацией функций и классификацией систем, аттестацией, разделением систем, защитой от сбоев по общей причине, программными аспектами компьютерных систем, аппаратными аспектами компьютерных систем и проектированием пунктов управления. Стандарты, указанные непосредственно на этом (втором) уровне, должны рассматриваться вместе с МЭК 61513, как согласованный набор документов.

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

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

МЭК 61513 заимствовал формат представления из базовой публикации по безопасности МЭК 61508 с общей картой жизненного цикла безопасности и схемой жизненного цикла системы. Что касается ядерной безопасности, то МЭК 61513 обеспечивает интерпретацию общих требований МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 для сектора ядерных приложений в отношении ядерной безопасности. В этой структуре МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 для сектора ядерных приложений. МЭК 61513 ссылается на стандарты ИСО, а также документы GS-R-3, МАГАТЭ GS-G-3.1 и МАГАТЭ GS-G-3.5 по темам, связанным с обеспечением качества.

Серия стандартов подкомитета МЭК ПК 45А последовательно реализует и детализирует принципы и основные аспекты безопасности, представленные в кодексе МАГАТЭ по безопасности АС и серии стандартов по безопасности МАГАТЭ, в частности документа «Требования SSR-2/1», устанавливающего требования безопасности, связанные с проектированием атомных станций, и документа «Руководство по безопасности NS-G-1.3», касающегося систем контроля и управления, важных для безопасности атомных станций. Термины и определения, используемые в стандартах серии подкомитета МЭК ПК 45А, соответствуют терминам и определениям, используемым МАГАТЭ.

Примечание — Предполагается, что при проектировании систем контроля и управления на АС, которые реализуют обычные функции безопасности (например, обеспечения безопасности работников, защиты активов, защиты от химических опасностей, защиты от энергетической опасности технологических процессов), будут применяться международные или национальные стандарты, которые основаны на требованиях стандартов, аналогичных МЭК 61508.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

РЕЗЕРВНЫЙ ПУНКТ УПРАВЛЕНИЯ АТОМНОЙ СТАНЦИИ, ИСПОЛЬЗУЕМЫЙ ПРИ ОТКАЗЕ БЛОЧНОГО ПУНКТА УПРАВЛЕНИЯ

Общие требования

Supplementary control room of nuclear power plant,
used with shutdown of the main control room. General requirements

Дата введения — 2020—07—01

1 Область применения

Настоящий стандарт устанавливает требования к резервному пункту управления (РПУ) атомной станции (АС), который должен обеспечивать возможность персоналу переводить реактор в подкритическое состояние и поддерживать реактор сколько необходимо в подкритическом и расхоложенном состоянии в том случае, когда управление функциями безопасности больше не может осуществляться из блочного пункта управления (БПУ) из-за его отказа или недоступности. В проекте должно быть обосновано исключение отказа или недоступности РПУ и БПУ по общей причине.

Настоящий стандарт устанавливает требования к выбору функций, проектированию и организации человеко-машинного интерфейса (ЧМИ), а также к соответствующему порядку и процедурам, которые должны систематически использоваться для верификации и валидации функционального проектирования резервного пункта управления.

Предполагают, что РПУ, предусмотренный для остановки реактора при отказе БПУ, будет отключен при обычных условиях эксплуатации (кроме периодического тестирования РПУ). Требования к РПУ отражают применение инженерных принципов, учитывающих особенности человеко-машинного интерфейса как при периодических испытаниях БПУ, так и при нарушениях нормальной эксплуатации.

Настоящий стандарт не распространяется на специальные средства реагирования при чрезвычайных ситуациях (например, на центр технической поддержки) или объекты, предназначенные для обращения с радиоактивными отходами. Рабочее проектирование оборудования также выходит за рамки настоящего стандарта.

Настоящий стандарт следует принципам, изложенным в документах МАГАТЭ: SSR-2/1 и NS-G-1.3.

Целью настоящего стандарта также является определение функциональных требований, которые используются при проектировании резервного пункта управления атомной станции, и соблюдение требований безопасности.

Настоящий стандарт следует применять для резервного пункта управления, концептуальное проектирование которого начинается после публикации настоящего стандарта. Если необходимо применить его к существующим АС или проектам, необходимо соблюдать особую осторожность, чтобы обеспечить совместимость с существующими проектными основами. Это относится, например, к таким факторам, как согласованность между РПУ и БПУ, эргономичный подход, уровень автоматизации и информационные технологии, а также к степени модификаций, которые должны быть реализованы в системе контроля управления (СКУ).

Издание официальное

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 к нему)]:

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

IEC 60964:2009 Nuclear power plants — Control rooms — Design (Атомные станции. Пункты управления. Проектирование)

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

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 положения)

IEC 61771, Nuclear power plants — Main control-room — Verification and validation of design (Атомные станции — Блочный пункт управления — Верификация и валидация проекта)

IEC 62646, Nuclear power plants — Control rooms — Computer based procedures (Атомные станции. Пункты управления. Компьютерно-ориентированные процедуры)

ISO 11064 (all parts), Ergonomic design of control centres (Эргономическое проектирование центров управления)

ISO 11064-1, Ergonomic design of control centres — Part 1: Principles for the design of control centres (Эргономическое проектирование центров управления. Часть 1. Принципы проектирования)

ISO 11064-3, Ergonomic design of control centres — Part 3: Control room layout (Эргономическое проектирование центров управления. Часть 3. Расположение зала управления)

ISO 11064-6, Ergonomic design of control centres — Part 6: Environmental requirements for control centres (Эргономическое проектирование центров управления. Часть 6. Требования к окружающей среде)

IAEA SSR-2/1:2012, Safety of Nuclear Power Plants: Design (Безопасность атомных станций. Проектирование)[1)]

IAEA Safety Guide NS-G-1.3:2002, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants (Приборы и системы управления, важные для безопасности на атомных станциях)[2)]

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

персонал пункта управления (control room staff): Группа работников АС, находящихся в БПУ и несущих ответственность за достижение целей эксплуатации АС, управляя ею посредством ЧМИ[3)].

[МЭК 60964:2009, пункт 3.3]

3.2

запроектные условия (design extension conditions): Постулируемые условия аварии, которые не учитываются при проектных авариях, но которые учитываются в процессе проектирования объекта в соответствии с реалистическим (неконсервативным) анализом и для которых выбросы радиоактивного материала сохраняются в допустимых пределах[4)].

[МАГАТЭ SSR-2/1:2012, определения изменены как в DS462]

---

1) Заменен. Действует IAEA SSR-2/1:2016.

2) Заменен. Действует IAEA Specific Safety Guide SSG-39:2016.

3) Обычно персонал БПУ состоит из операторов, выполняющих функции контроля, и операторов, которые фактически манипулируют органами управления, однако может также включать в себя работников и специалистов, допущенных в БПУ, например во время длительно развивающихся событий.

4) Запроектные условия включают в себя условия при событиях без существенной деградации топлива и условия с плавлением активной зоны ядерного реактора.

3.3

местные пункты управления, местные щиты и пульты управления (local control points/facilities): Размещенные за пределами БПУ пункты (или средства), с помощью которых местные операторы осуществляют управляющую деятельность.

[МЭК 60964:2009, пункт 3.17]

3.4

местные операторы (local operators): Оперативный персонал, выполняющий задачи за пределами БПУ.

[МЭК 60964:2009, пункт 3.18]

3.5

оперативный персонал (operating staff): Персонал АС, работающий посменно и осуществляющий эксплуатацию АС[1)].

[МЭК 60964:2009, пункт 3.20]

3.6 **резервный пункт управления** (supplementary control room): Место, с которого может осуществляться ограниченное управление реакторной установкой и/или ее контроль для выполнения функций безопасности, определенных анализом безопасности, как это требуется в случае потери возможности выполнять эти функции с БПУ[2)].

Примечание — Для существующих АС резервный пункт управления может быть специальным (отдельным) пунктом управления, но во многих случаях он включает в себя комплекты панелей управления и дисплеи в помещениях распределительных устройств или аналогичных местах. В последнем случае для таких панелей управления и дисплеев в настоящем стандарте используется термин «резервный пункт управления».

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

АС (NPP) — атомная станция;

БПУ (MCR) — блочный пункт управления;

ВиВ (V&V) — верификация и валидация;

КП (CBP) — компьютеризированная процедура[3)];

МПУ (LCP) — местный пункт управления,

ПИС (PIE) — проектное исходное событие;

РПУ (SCR) — резервный пункт управления;

СКУ (I&C) — система контроля и управления.

[1)] Оперативный персонал состоит из персонала БПУ, инженеров по эксплуатации и обслуживанию и др.

[2)] Резервный пункт управления — это часть блока АС, размещаемая в предусмотренном проектом АС помещении и предназначенная при отказе БПУ для непрерывного контроля состояния реактора, перевода реактора в подкритическое состояние, расхолаживания реактора и поддержания его сколько необходимо в подкритическом и расхоложенном состоянии, приведения в действие систем безопасности в случае необходимости, а также для управления теплоотводом от бассейна выдержки отработанного ядерного топлива (ОЯТ) (Федеральные нормы и правила НП-001-15).

[3)] Компьютеризированные процедуры (Computer Based Procedures; CBP) — интерактивное компьютерное приложение, используемое для представления методического руководства операторам станции, которое может дополнительно содержать информацию о динамических процессах, включая доступ к органам управления пульта оператора (в отличие от процедур на бумажном носителе, которые являются фиксированным документом, КП предлагают опции динамических показаний. Данные опции позволяют оператору перемещаться от одного шага к другому различными усовершенствованными способами, размещать закладки и использовать параллельную дисплейную индикацию).

5 Правила проектирования

5.1 Общие требования

Требование 66 документа МАГАТЭ SSR-2/1 гласит: «Контрольно-измерительные приборы и оборудование управления должны быть доступны предпочтительно в одном месте (резервном пункте управления), которое физически, электрически и функционально должно быть отделено от пункта управления АС. Резервный пункт управления должен быть оборудован таким образом, чтобы реактор можно было остановить и поддерживать в остановленном состоянии, остаточное тепло можно было бы удалять, а основные параметры АС можно было контролировать (в том случае, если пункт управления потерял способность выполнять основные функции безопасности)».

Примечание 1 — Ссылка на «пункт управления» интерпретируется в документе МАГАТЭ SSR-2/1, как «блочный пункт управления (БПУ)».

Примечание 2 — Функциональное разделение означает, что функционирование РПУ не зависит от работоспособности (от наличия определенных в проекте отказов) БПУ.

Примечание 3 — Полное функциональное разделение каналов управления (от устройства ввода команды до исполнительного устройства) может быть сложно осуществить для всех функций, например в случае, когда срабатывание исполнительного механизма требует команды контроллера сравнения и выбора приоритета управления с БПУ или с РПУ. Использование подобного общего для РПУ и БПУ оборудования приемлемо, если предусмотрено резервное оборудование, с использованием которого может быть выдана инициирующая команда. При этом должен быть минимизирован риск того, что резервируемое и резервирующее оборудование может подвергаться общим опасным воздействиям, способным привести к отказу выполнения рассматриваемой функции управления.

В МАГАТЭ NS-G-1.3 (пункты 6.15—6.30) содержатся рекомендации по требованиям к резервным пунктам управления, включая требования, связанные с:

- определением основных проектных решений АС, которые требуют использования РПУ (пункты 6.17, 6.19, 6.20);
- определением расположения и конфигурации РПУ для обеспечения быстрого ввода в действие (пункт 6.29);
- определением пути доступа к РПУ с указанием опасностей вдоль этого пути и подходящих компенсационных мероприятий против этих опасностей (пункты 6.27, 6.28);
- установлением мер по предотвращению несанкционированного доступа к РПУ или несанкционированного использования РПУ (пункт 6.21);
- определением функций безопасности БПУ и РПУ, не затронутых одним и тем же ПИС, и обеспечением независимости от БПУ цепей (электрических, пневматических и др.), связанных с РПУ (пункты 6.20, 6.23);
- определением приоритетов между БПУ и РПУ в управлении и порядка в передаче управления от БПУ к РПУ (пункты 6.18, 6.20, 6.24);
- описанием ручного управления в РПУ, выполняемого простыми действиями (пункт 6.22);
- применением в РПУ панелей и элементов управления, аналогичных (насколько это возможно) тем, которые имеются в БПУ (пункт 6.22);
- рассмотрением различий в назначениях БПУ и РПУ (пункт 6.25),
- обеспечением в РПУ (если предполагается его долгосрочное использование) соответствующих условий нахождения персонала и необходимого рабочего пространства для решения персоналом производственных задач (пункт 6.30).

5.2 Основные цели

Требования МАГАТЭ по разработке РПУ, приведенные в первом абзаце 5.1, следует выполнять в соответствии с настоящим стандартом.

РПУ должен быть снабжен средствами, обеспечивающими прекращение работы реактора, доведение АС до безопасного состояния и поддержание реактора в этом состоянии в случае отказа БПУ. РПУ не предназначен для выполнения в полном объеме всех функций контроля и управления, которые могут быть выполнены на БПУ. Применительно к конкретным типам АС на основе результатов соответствующего анализа безопасности в РПУ могут быть интегрированы ресурсы для предотвращения и уменьшения последствий определенного в проекте набора ПИС.

Применение РПУ обязательно при потере способности БПУ выполнять функции безопасности. Возможные причины указанной потери включают пожар в помещении пункта управления, появление избыточного дыма или опасной атмосферы в БПУ, крупное повреждение БПУ или его кабелей (такое, что функции безопасности не могут быть выполнены), отказ оборудования пункта управления.

В проекте необходимо определить перечни ПИС и пути протекания аварий, для которых требуется использование РПУ. Такое определение должно включать идентификацию и условия подтверждения предполагаемых обстоятельств на всей АС, а также определение продолжительности соответствующих событий, для которых может потребоваться РПУ.

Поскольку события, приводящие к выходу из строя БПУ, очень редки, можно ожидать, что анализ безопасности АС покажет, что такие события могут совпадать с другими независимыми событиями на АС только с приемлемо низкой частотой (в частности, при этом предполагается, что одновременно не будет поврежден первый контур реактора). При этом, однако, следует учитывать потенциально возможные неисправности оборудования, которые могут возникнуть в результате процесса перевода реактора в подкритическое состояние, и вероятные отказы оборудования, которые могут наложиться на этот процесс. В частности, проект РПУ должен учитывать возможный долгосрочный выход из строя БПУ из-за пожара или по другим причинам.

Критерии использования РПУ должны быть четко указаны в соответствующих инструкциях и руководствах.

Должна быть предусмотрена возможность оценки и полного определения состояния безопасности за пределами БПУ и предпочтительно в пределах РПУ. РПУ должен обеспечивать контроль состояния соответствующих систем, оборудования и основных параметров АС. Вся представленная на РПУ информация должна соответствовать эргономическим принципам, представленным в соответствующих частях серии стандартов ИСО 11064.

Для обеспечения эффективного контроля и последующего анализа произошедших событий необходима запись ключевых параметров, которая позволяет реализовать возможности последующего отображения тенденций изменения параметров АС и получения в дальнейшем доступа к этим параметрам для проведения автономного анализа. Рекомендуется автоматическая запись ключевых параметров АС. Если предположить, что БПУ и РПУ не будут доступны персоналу в течение продолжительного времени, то должна быть предусмотрена автоматическая запись ключевых параметров АС.

С оперативной точки зрения (например, для упрощения работы и во избежание недоразумений) предпочтительнее иметь только один резервный пункт управления. Однако при проектировании следует соблюдать требования, вытекающие из требований безопасности, в частности требований резервирования и независимости. Если для существующей АС предусмотрены два или более резервных пункта управления, каждый резервный пункт управления должен отображать всю информацию, необходимую для выполнения задач оператора.

Компьютерные средства отображения и предоставления информации на РПУ должны обеспечивать такую же функциональность для предоставления важной для безопасности информации, как и соответствующие дисплеи в БПУ. Предоставляемая на компьютерных средствах отображения информация для каждого состояния АС и каждого задания оператора должна быть такая же, как в БПУ.

Персоналу должно быть предоставлено достаточно времени для перехода в РПУ, прежде чем от него потребуются необходимые действия. РПУ должны быть обеспечены достаточным количеством оборудования для необходимой связи в пределах и за пределами площадки АС всего задействованного в функционировании РПУ персонала. Требования к средствам связи приведены в 7.7.

Номенклатура контрольно-измерительного оборудования, способы и режимы предоставления информации должны обеспечивать оперативный персонал достаточным объемом информации для оценки состояния АС. Состав контрольно-измерительных приборов и режимы предоставления информации в РПУ должны обеспечивать контроль перевода реактора в подкритическое состояние, расхолаживания реактора и поддержания его сколько необходимо в подкритическом и расхоложенном состоянии, а также контроль за удержанием всех радиоактивных веществ.

Системы АС, которые могут управляться из РПУ, могут быть ограничены только теми системами, которые выполняют и обеспечивают функции безопасности.

Для установленных перечней ПИС, условий и событий, при которых БПУ не может быть использован, РПУ должен обеспечивать достаточный контроль состояния функций безопасности и их выполнения для достижения и поддержания безопасного состояния АС. Процессы контроля и управления на РПУ должны обеспечивать проверку состояния функций безопасности, включая контроль их инициро-

вания и завершения выполнения, а также контроль состояния основных функций безопасности (см. документ МАГАТЭ SSR-2/1: 2012, требование 4).

Средства контроля физической безопасности, контроля доступа и противопожарные средства оповещения, используемые при функционировании БПУ, должны быть также расположены и в независимом месте, например в РПУ или в месте, на которое не оказывают отрицательного влияния события и условия, приводящие к необходимости использования РПУ. Места расположения таких средств должны быть устойчивыми к вредным и опасным воздействиям не менее, чем РПУ. Таким независимым местом расположения указанных средств может быть или сам РПУ, или иное место, на которое не будет влиять одно и то же событие, вызвавшее использование РПУ. Если такое место расположения используется, то оно должно иметь такую же, как у РПУ, способность выдерживать опасные воздействия.

Проект РПУ должен сочетаться и соответствовать проекту БПУ. Процесс идентификации и проектирования соответствующих элементов управления и контроля, необходимых для РПУ, должен соответствовать (как указано в разделе 6) требованиям МЭК 60964.

5.3 Принципы безопасности

5.3.1 Проектные и запроектные условия

В проекте должно быть обосновано, что указанные события не влияют на БПУ и РПУ (а также на местные пункты управления)[1),2)], вызывая их одновременную непригодность и неэффективность при выполнении безопасного перевода реактора в подкритическое состояние, контроля состояния реактора, а также контроля и управления состоянием критических функций безопасности.

В проекте должно быть обосновано, что запроектные события и воздействия или маловероятные наложения отказов не приводят к одновременному отказу БПУ и РПУ. При обосновании выполнения процесса передачи управления на РПУ должны учитываться ограничения, обусловленные использованием РПУ при проектных и запроектных событиях.

Рассмотренные выше требования об одновременной непоражаемости БПУ и РПУ должны также применяться к обеспечивающим и поддерживающим системам и элементам БПУ и РПУ.

5.3.2 Функциональная классификация и аттестация (квалификация)

Функции РПУ должны классифицироваться по МЭК 61226 с должным учетом критериев использования РПУ, описанных в 5.2.

Оборудование и системы РПУ должны быть спроектированы со степенью резервирования в соответствии с их классификацией безопасности. При расположении в непосредственной близости друг от друга систем безопасности, систем нормальной эксплуатации (в том числе резервирующих систем) следует учитывать необходимость соблюдения принципов функциональной изоляции и физического разделения (см. МЭК 60709).

Оборудование РПУ должно соответствовать условиям окружающей среды, в которых предполагается его использование. Оборудование должно быть аттестовано (квалифицировано) в соответствии с его классификацией по безопасности с учетом ПИС и путей протекания аварий. Для обоснования необходимой надежности и устойчивости оборудования в запроектных условиях могут потребоваться дополнительные испытания и исследования.

5.3.3 Доступность резервного пункта управления и время перехода в него персонала

Принимая в расчет определенные в проекте причины невозможности функционирования БПУ, РПУ должен быть спроектирован (и, если необходимо, расположен) так, чтобы даже в аварийных условиях доступ персонала в него обеспечивался по безопасным маршрутам движения (см. 7.3 для получения дополнительной информации).

Принятыми проектными решениями персоналу пункта управления должно быть предоставлено достаточное время для перехода в РПУ после того, как БПУ станет недоступен или неработоспособен. В проекте должно быть установлено, что продолжительность работы функций безопасности в автоматическом режиме (для обеспечения безопасности АС) и длительность эффекта воздействия от выполнения этих функций после их запуска в БПУ должны соответствовать периоду времени перехода персонала на РПУ вплоть до момента, когда РПУ становится работоспособным. Это время должно

---

1) Требование доступности МПУ устанавливают только одновременно с требованием доступности РПУ.

2) Требование доступности МПУ устанавливают только в том случае, когда МПУ нужны для выполнения каких-либо функций по безопасному останову реактора и дальнейшей поддержке его безопасного состояния совместно с РПУ (см. 5.4).

включать время контроля доступа персонала в РПУ и время оценки состояния оборудования РПУ. В приложении А приведены факторы, которые должны быть рассмотрены при теоретической оценке периода времени безопасной передачи управления из БПУ в РПУ.

5.3.4 Передача управления, приоритетность управления и физическая защита

Проектом должны быть предусмотрены средства отключения функций управления БПУ и передачи управления из БПУ в РПУ. Эти средства должны классифицироваться в соответствии с самой высокой категорией функции безопасности, управление которой может быть потеряно на БПУ. Должна быть доказана высокая надежность средств отключения функций управления БПУ и передачи управления из БПУ в РПУ и, если требуется, их соответствие критерию единичного отказа. Необходимо проанализировать и принять во внимание возможные отказы системы физической защиты РПУ и влияние уязвимостей кибербезопасности РПУ на физическую защиту СКУ.

Примечание — Изложенное выше исключает любые требования по отключению функций по переводу реактора в подкритическое состояние из БПУ.

Средства передачи управления должны обеспечивать отключение расположенных в БПУ средств управления, чтобы гарантировать, что пожар или повреждения, влияющие на БПУ, не вызовут выдачу ложных управляющих воздействий. Эти средства также должны быть такими, чтобы избежать или минимизировать переходные процессы для контролируемых переменных во время передачи управления в обоих направлениях: от БПУ в РПУ и от РПУ в БПУ.

Средства передачи управления могут находиться в БПУ, или в РПУ, или на маршруте перехода из БПУ в РПУ, если предварительный анализ проектных решений показывает, что принятое размещение средств передачи управления не ведет к отказам, связанным с передачей управления или с возможностью управления с РПУ. Если средства передачи управления расположены в БПУ, то должны быть предусмотрены дополнительные средства передачи управления, которые не включаются в состав БПУ.

В состав РПУ должны быть включены средства идентификации состояния управляющего статуса РПУ и БПУ (т. е. «включено» или «отключено»).

СКУ должны быть спроектированы так, чтобы предотвратить одновременное управление системами АС из БПУ и из РПУ.

СКУ должны быть спроектированы так, чтобы обеспечить приемлемо низкую вероятность появления ложных сигналов от элементов систем БПУ, влияющих на безопасность АС. СКУ должны быть спроектированы так, чтобы при нормальной эксплуатации и при нарушении нормальной эксплуатации была приемлемо низкая вероятность появления от элементов систем РПУ ложных сигналов, препятствующих контролю за АС из БПУ или управлению АС из БПУ. Примерами проектных решений для достижения этих целей является использование переключателей передачи, кодированных сигналов и оптически изолированных линий связи.

Неисправность оборудования, контролирующего передачу управления от БПУ к РПУ, может привести к непреднамеренной изоляции БПУ. Следовательно, режимы отказа оборудования, реализующего функцию передачи управления, должны быть проанализированы и должна быть показана его приемлемость. В этом анализе должны учитываться все ПИС, при которых определены операции из БПУ.

Действия, предпринимаемые из РПУ при его использовании, должны иметь приоритет над любыми другими действиями ручного управления, за исключением случаев, когда управление должно выполняться с использованием местного пункта управления.

Проект РПУ должен включать положения по предотвращению несанкционированного доступа в РПУ и предотвращению его несанкционированного использования. Принятые в проекте средства передачи управления должны предотвращать несанкционированную передачу управления от БПУ к РПУ и наоборот. Доступ в РПУ и любые попытки передачи управления в РПУ должны идентифицироваться сигналами тревоги в БПУ.

Если во время нормальной работы АС обслуживающий персонал не находится в РПУ, то следует регулярно проверять РПУ, чтобы гарантировать соблюдение определенного уровня безопасности.

Все процедуры, применяемые при модификации программного обеспечения БПУ, также применяются при модификации программного обеспечения РПУ.

5.3.5 Эксплуатационные соображения

РПУ должен быть спроектирован с учетом необходимости обеспечить минимизацию вероятности возникновения ошибок операторов.

Проект должен включать предоставление в РПУ документированных инструкций, описывающих функционирование:

- систем АС и устройств контроля и управления;
- информационных и записывающих систем;
- оборудования связи;
- любого другого оборудования, которое должно работать в РПУ.

Инструкции и регламенты, характеризующие действия оперативного персонала, которые необходимо предпринять из РПУ (например, расхолаживание АС), должны быть простыми и понятными. Они должны основываться на тех же принципах и способах предоставления, что и инструкции для оперативного персонала БПУ, и могут отличаться от них только в тех случаях, когда органы управления и доступные средства и системы управления имеют различия. Если оперативные инструкции отличаются в части действий для выполнения одной и той же функции на БПУ и на РПУ, то должна быть обеспечена дополнительная подготовка и тренировка персонала.

Даже если для РПУ реализованы КП, персоналу должны быть доступны описания этих процедур, представленные на бумажном носителе. Это позволяет уменьшить влияние отказов оборудования КП и облегчить управление с РПУ в комбинации с управляющими действиями с локальных пунктов управления. При проектировании КП следует руководствоваться МЭК 62646.

Проектировщик должен указать процедуры регулярных испытаний и проверок оборудования РПУ, подтверждающие соответствие проекту и принципам безопасности. Требования к регулярным испытаниям и проверкам оборудования приведены в 7.9.

Проект должен предусматривать регулярное обучение и тренировки по использованию РПУ без воздействий на исполнительные части управляющих систем АС.

5.4 Принципы учета человеческого фактора при проектировании

Для оптимального распределения функций, обеспечивающего максимальное использование возможностей оператора и системы управления, а также для обеспечения максимальной безопасности АС особое внимание в проекте должно быть уделено учету человеческого фактора, характеристикам человеческих качеств персонала в аварийных условиях, особенно в ситуациях, требующих немедленных действий, т. е. действий, которые должны быть выполнены в течение короткого времени после приведения в готовность персонала на РПУ.

Если анализ безопасности показывает, что может потребоваться долгосрочное использование РПУ, то для него должны быть предусмотрены средства жизненного обеспечения РПУ (например, вентиляция). Требования к подобным средствам могут отличаться от аналогичных требований для БПУ.

ЧМИ для РПУ должен быть спроектирован по тем же правилам, что и для БПУ, особенно в отношении конструкции ЧМИ для контроля основных параметров АС. ЧМИ для РПУ должен соответствовать эргономическим принципам, представленным в серии стандартов ИСО 11064.

Если для существующей АС необходимы несколько резервных пунктов управления и/или МПУ, то должны быть разработаны четкие указания по их использованию, укомплектованию их персоналом и координации действий персонала при использовании этих объектов. Кроме того, необходимо проанализировать факторы, связанные с человеческими возможностями, для доказательства того, что требуемые задачи могут быть решены надежно и в сроки, принятые при анализе безопасности.

Если по требованиям резервирования и независимости (например, для разделения противопожарным барьером двух однотипных кабельных каналов) для существующей АС требуется более одного пункта управления, то в этом случае эти пункты должны быть оснащены не отбрасывающими блики мнемосхемами с четкой и ясной идентификацией соответствующих элементов АС (см. МЭК 60964).

6 Процесс проектирования

Для разработки спецификации РПУ следует использовать системный подход. Процессы разработки спецификаций РПУ и БПУ должны проходить параллельно. Оба процесса должны использовать аналогичные процедуры, критерии и методы. К задачам и принципам проектирования (и документирования результатов проектирования) РПУ следует применять элементы следующих процессов:

a) определение проектных и запроектных сценариев, их целей и критериев отказов (см. 5.2);

b) определение на основе проектного анализа функций, которые требуется выполнять с использованием РПУ;

c) назначение основных функций СКУ или эксплуатирующему персоналу и распределение этих функций по рабочим местам;

d) классификация функций РПУ в отношении их важности для безопасности и определение соответствующих проектных и квалификационных требований;

e) проектирование станционного РПУ в соответствии с общими правилами, приведенными в МЭК 60964:2009, раздел 5;

f) проведение верификации концептуального проекта РПУ (в том числе тренировок, инструкций и регламентов для участвующего в управлении АС персонала) и валидации РПУ в целом (см. раздел 8).

g) завершение спецификации проекта РПУ на основе вышеизложенного (см. также раздел 7);

h) разработка рабочего проекта РПУ и выполнение его окончательной верификации и валидации (ВиВ) на АС после завершения проектирования (см. раздел 8).

В результате реализации описанного выше процесса должен быть определен перечень систем, подлежащих управлению из РПУ, их конфигурация, а также перечень параметров АС, подлежащих контролю из РПУ.

7 Функциональное проектирование

7.1 Общие требования

Из-за нечастого использования РПУ и относительно небольшого числа задач, которые необходимо выполнять в РПУ, его проектирование должно быть нацелено на минимизацию количества оборудования, располагаемого в РПУ, высокую надежность выполнения оборудованием РПУ своих функций и разработку конфигурации РПУ, доступной для легкого и быстрого понимания.

7.2 Человеческий фактор

Антропометрические соображения, демографические стереотипы, интенсивность звуковых сигналов, углы поля зрения и углы обзора отображающих устройств, а также предпочтение, отдаваемое аналоговым или цифровым индикаторам для РПУ, следует выбирать по аналогии с теми, которые выбраны для БПУ, и они должны соответствовать эргономическим принципам, приведенным в серии стандартов ИСО 11064.

В РПУ должен быть принят достаточный уровень освещенности для обеспечения достаточной видимости при выполнении оперативным персоналом задач на постоянной основе без чрезмерной усталости. РПУ должен соответствовать требованиям ИСО 11064-6.

Звуковая окружающая среда в РПУ должна обеспечивать четкую голосовую связь и соответствовать требованиям ИСО 11064-6.

Если рабочие зоны РПУ предусмотрены для использования в течение длительного времени, в них должны быть предусмотрены средства, отвечающие требованиям эргономики для сидячей работы, ведения записей, работы со справочными и с другими размещенными в РПУ документами.

Если в РПУ используют компьютерную информацию или управление, то их следует использовать точно так же, как и аналогичные элементы управления и индикации БПУ. Параметры окружающей среды и требования надежности могут потребовать применения в РПУ оборудования, отличного от применяемого в БПУ, однако при этом следует использовать операционные последовательности, соответствующие последовательностям, применяемым в БПУ, и совместимые с ними.

7.3 Расположение и маршрут доступа

Место расположения РПУ должно быть выбрано и его средства защиты должны быть спроектированы так, чтобы никакая последовательность событий ПИС не могла одновременно отрицательно влиять на выполнение функций РПУ и БПУ. Процесс проектирования должен включать рассмотрение событий, которые могут повлиять на пункты управления либо непосредственно, либо через системы, предназначенные для обеспечения и обслуживания БПУ и РПУ.

Примечание — Практическая реализация указанного выше требования к месту расположения заключается в том, чтобы область размещения РПУ была физически и электрически отделена от области размещения БПУ.

Для физического разделения БПУ и РПУ как части функционального (физического и электрического) разделения должно быть обеспечено достаточное разделение прокладываемых кабелей.

Сигналы по кабелям от оборудования нижнего уровня и к этому оборудованию следует направлять непосредственно в (из) РПУ, а не через БПУ, и наоборот. Системы вентиляции также должны быть спроектированы с учетом требований к функциональному разделению и независимости БПУ и РПУ.

Пожар является опасной угрозой, из-за которой может потребоваться использование РПУ. В проекте РПУ должна быть проведена оценка его противопожарной защиты и маршрутов движения людей при пожаре. Результаты такой оценки должны подтверждать доступность местоположения РПУ. Для других проектных и запроектных исходных событий и условий, при которых может быть использован РПУ, должны быть сделаны аналогичные оценки для всех обеспечивающих систем (особенно систем отопления, вентиляции и кондиционирования), маршрутов движения персонала и трасс прокладки кабелей. При оценке трасс прокладки кабелей должно быть продемонстрировано обоснование независимости кабелей РПУ от кабелей БПУ.

Доступ персонала в РПУ должен быть свободным, безопасным и проходить в течение отведенного на это времени, учитывающего проведение необходимого контроля доступа. Доступ в РПУ должен быть возможен как из БПУ (при его эвакуации), так и по маршрутам, пролегающим вне БПУ и вне любых зон, потенциально подверженных опасностям, в результате которых требуется использование РПУ. Следует рассмотреть вопрос о необходимости защиты персонала от радиоактивного излучения вдоль этих маршрутов доступа.

Вдоль маршрута доступа от БПУ до РПУ должно быть обеспечено размещение указателей потенциальных опасностей (например, пожара) и указателей соответствующих защитных мер и размещения средств защиты (например, мест размещения оборудования для дыхания). Перед получением доступа в РПУ оперативный персонал должен быть уверен, что окружающая среда на РПУ безопасна.

До всего оперативного персонала (особенно покинувшего свои рабочие места перед эвакуацией БПУ) должна быть четко доведена информация о выходе БПУ из строя и невозможности его использования для целей управления до возобновления доступа к нему.

7.4 Окружающая среда резервного пункта управления

Условия окружающей среды в РПУ должны отвечать требованиям, предъявляемым к ней на основе результатов анализа безопасности в нормальных и аварийных условиях. Проектные требования к окружающей среде в РПУ следует составлять с учетом соответствующих планов защиты и федеральных норм и правил. Для РПУ и путей доступа к нему должна быть предусмотрена защита от радиоактивного излучения, за исключением случаев, когда анализ показывает, что в этом нет необходимости. Такой анализ должен включать рассмотрение возможностей доступа в РПУ из-за пределов площадки (территории АС), а также из БПУ.

Для всех случаев (вплоть до проектных аварий, требующих использования РПУ) определенные из анализа безопасности условия окружающей среды для предполагаемого места размещения РПУ и путей доступа к нему не должны быть хуже условий окружающей среды для незащищенного человека. Если требуется использование РПУ в запроектных условиях, включая доступ по планам мероприятий по защите персонала и населения, то должно быть показано, что в этих условиях в месте расположения РПУ обеспечивается нормальный доступ в него человека. Несмотря на это для РПУ должен быть предусмотрен радиационный контроль.

Система аварийного освещения с питанием от аккумуляторных батарей должна быть постоянно доступна в РПУ даже после отказа основной системы освещения или ее источника питания. Система аварийного освещения должна обеспечивать достаточное освещение для выполнения задач в условиях ограниченного операционного периода, отвечающего требованиям аварийного планирования на АС.

Должны быть предусмотрены возможности по использованию переносных аккумуляторных батарей, расположенных за пределами площадки АС, для восстановления источников питания освещения и любых других объектов, необходимых для дальнейшего использования РПУ в случае долгосрочного отказа системы нормального электроснабжения.

Источники питания для оборудования и освещения РПУ должны быть спроектированы в соответствии с классом безопасности и сценариями использования РПУ. Проект, как правило, должен предусматривать возможность питания оборудования от источника аварийного бесперебойного питания.

В зависимости от рассмотренных в проекте сценариев использования РПУ должны быть предусмотрены возможности для подключения внешнего дополнительного источника питания. Эти дополнительные возможности могут включать в себя использование переносного оборудования для заряда,

прокладку кабелей, а также инструменты технического обслуживания и ремонта, которые могут потребоваться для подключения резервного источника питания и обеспечения совместимости соединений для этой цели.

Решения по применению резервного источника питания для пунктов управления (БПУ, РПУ) должны соответствовать возможностям резервных источников питания (для приводов, двигателей и т.п.), предусмотренным на случай потери электропитания для собственных нужд оборудования АС (клапанов, двигателей и т. д.).

7.5 Пространство и конфигурация

В РПУ должно быть достаточно места для:

- размещения всего необходимого информационного и контрольного оборудования в хорошо структурированном расположении;
- написания и оформления документов и проведения процедур;
- хранения документов;
- размещения коммуникационного оборудования.

В РПУ должны быть предусмотрены запасные пространства на случай модернизаций и расширений РПУ.

Конфигурация РПУ должна обеспечивать быструю готовность оперативного персонала по прибытии в РПУ. ИСО 11064-1 предлагает руководство по принципам эргономического проектирования центров управления, а ИСО 11064-3 предлагает руководство по принципам компоновки помещений центров управления.

7.6 Информационное и контрольное оборудование

Вся информация, дисплеи, оборудование для записи и управления должны быть организованы и структурированы в соответствии с их функциями и приоритетами, чтобы свести к минимуму вероятность ошибок оператора. Интерфейс оборудования РПУ должен быть таким же, как соответствующий интерфейс БПУ.

Для улучшения предоставления информации могут быть использованы мнемосхемы.

Представление элементов управления, индикаторов и мнемосхем, выбранных для РПУ, должно соответствовать тем же принципам проектирования и компоновки, которые применяют для БПУ.

Принципы кодирования, маркировки и группировки в РПУ должны соответствовать принципам кодирования, маркировки и группировки, применяемым в БПУ.

Для функций безопасности в соответствии с 5.2 должно быть предусмотрено отображение и управление. Отображающие дисплеи и элементы управления должны иметь степень резервирования в соответствии с их классификацией безопасности и требованиями проекта.

Если для соответствующей АС единичный резервный пункт управления не обеспечивает требования по необходимому резервированию и если для резервирования не предусмотрен альтернативный резервный пункт управления, то в определенных конкретных проектах возможно применение местного пункта управления, с использованием которого возможно осуществлять необходимый контроль или управление в случае отказа функционирования резервного пункта управления. В исключительных случаях, если это требуется по соображениям безопасности, использование местного пункта управления следует рассматривать как независимое инженерное решение, которое не является расширением резервного пункта управления. Для этих особых случаев должны быть обоснованы доступность и временные границы доступности МПУ.

7.7 Системы связи

Должны быть предусмотрены средства связи РПУ с администрацией АС и центром технической поддержки, при его наличии. Должны быть обеспечены нормальная внутренняя телефонная связь и другие средства связи, такие как пейджинг, как того требуют аварийные инструкции и руководства. Средства связи должны гарантированно обеспечивать связь между РПУ и местными пунктами управления. Если для проекта конкретной АС требуется более одного резервного пункта управления, то должна быть обеспечена связь между этими резервными пунктами управления.

Резервное оборудование связи, использующее различные маршруты и каналы передачи данных, должно быть доступно для оперативных целей, для руководства операциями по переводу реактора в подкритическое состояние и для связи с центрами аварийного реагирования или их эквивалентами.

Такое резервное оборудование должно быть доступно для связи между РПУ и/или местными пунктами управления.

В дополнение к указанным выше средствам коммуникации должны быть предоставлены разнообразные средства коммуникации между РПУ и конкретными местами, как того требуют аварийные инструкции и руководства. Эти разнообразные средства коммуникации должны быть.

- спроектированы таким образом, чтобы только один способ коммуникации мог быть затронут одним и тем же отказом, вредным воздействием или ПИС;
- способны работать независимо от внутренних (местных) и внешних систем электропитания.

Обычное станционное коммуникационное оборудование может быть использовано для связи с БПУ при тренировках, испытаниях, проверках или для других целей.

7.8 Дополнительное оснащение

Дополнительное оснащение, которое должно быть либо расположено в РПУ, либо быть легкодоступным из РПУ, включает:

- медицинское оборудование для оказания первой помощи,
- оборудование, которое используют во время опасных ситуаций в соответствии с противоаварийным планированием на АС;
- документацию по противоаварийному планированию на АС;
- переносное освещение, детекторы излучения и противопожарное оборудование;
- защитную одежду и средства защиты органов дыхания.

Следует определить принципы работы, которые должны соблюдаться, когда по условиям, возникшим в БПУ, требуется использование РПУ в части контроля доступа, физической безопасности и действий в ответ на пожары. Если не указано иное, конструкция РПУ должна включать средства для выполнения указанных функций в течение времени, когда БПУ не может быть использован.

7.9 Тестирование и проверки

Следует проводить регулярное тестирование функций, связанных с использованием РПУ, включающее испытания и проверки:

a) аварийного освещения вдоль маршрутов перемещения операторов от БПУ до РПУ и из-за пределов площадки до РПУ;

b) средств контроля доступа к РПУ и связанных с ним функций физической защиты;

c) функций передачи управления из БПУ в РПУ;

d) ручного управления из РПУ переводом реактора в подкритическое состояние;

e) ручного управления с РПУ для поддержания реактора в подкритическом и расхоложенном состоянии;

f) непрерывного контроля состояния реактора с РПУ, включая функции моделирования развития событий;

g) функций связи РПУ;

h) других сервисных функций РПУ [например, вентиляции, освещения, источников питания (включая аварийную установку переносных аккумуляторных батарей)];

i) контроля неорганизованного поступления воздуха из смежных помещений и окружающей среды (неорганизованных протечек) в помещение РПУ с целью предотвращения поступления радиоактивных веществ в помещение РПУ в случае радиационной аварии.

Частота испытаний должна полностью соответствовать допущениям анализа безопасности.

В проекте должны быть указаны меры и мероприятия по проверкам и испытаниям, которые не оказывают неблагоприятного влияния на безопасность, а также на работоспособность и доступность оборудования АС.

Кроме того, следует проводить регулярные проверки:

- отсутствия помех, препятствующих безопасному перемещению персонала по маршрутам от БПУ до РПУ и из-за пределов площадки до РПУ;
- общих условий и состояния готовности оборудования РПУ и РПУ в целом.

Во всех необходимых случаях оперативный персонал должен быть вовлечен в работы по тестированию и проверкам, а также в подготовку отзывов о работе РПУ.

8 Верификация и валидация системы

Процесс верификации и валидации (ВиВ) систем РПУ тесно связан с процессом верификации и валидации (ВиВ) систем БПУ. Предписания по человеко-машинному интерфейсу, следующие из функциональных требований, определяются одновременно и для БПУ, и для РПУ.

Примечание — МЭК 61513 содержит общие требования к верификации и валидации СКУ. Настоящий стандарт учитывает лишь дополнительные требования к верификации и валидации, характерные для РПУ.

В связи с тем, что задачи, выполняемые в РПУ, упрощаются, сокращается количество действий и обрабатываемой информации, процессы ВиВ могут быть проще, чем для БПУ. ВиВ для РПУ следует планировать с подходящими критериями, основанными на требованиях МЭК 60964 и МЭК 61771.

В ходе окончательной проверки должно быть подтверждено, что события, которые могут привести к потере возможности выполнения функций безопасности БПУ, не влияют на РПУ или его функции. Пригодность и надежность РПУ необходимо проверить на площадке АС при вводе его в эксплуатацию.

Приложение А
(справочное)

Оценка периода времени безопасной передачи управления из блочного пункта управления в резервный пункт управления

В 5.3.3 настоящего стандарта указано, что персоналу пункта управления должно быть предоставлено достаточное время для перехода в РПУ после того, как БПУ станет недоступен или неработоспособен.

В настоящем приложении указаны факторы, которые должны быть учтены при рассмотрении требований, приведенных в 5.3.3, а именно:

a) предположения относительно достоверных сценариев «потери БПУ» (например, причина и форма «потери БПУ»), влияние событий этих сценариев на персонал пункта управления (т. е. на способность перехода персонала в РПУ), на окружающие условия вблизи БПУ и маршрутов движения к РПУ;

b) допущения относительно автоматического управления АС во время передачи управления от БПУ к РПУ (например, допущения, связанные с автоматической работой защитных систем после ручного инициирования перевода реактора в подкритическое состояние до эвакуации с БПУ или с автоматическим управлением в случае, если не удалось инициировать перевод реактора в подкритическое состояние);

c) анализ продолжительности периодов времени безопасной передачи управления для разных вероятных сценариев (т. е. для каждого сценария по результатам анализа определяется время, в течение которого не требуется никаких действий оператора по обеспечению безопасности);

d) анализ времени, необходимого для безопасного перехода персонала и приведения РПУ и персонала в готовность для различных вероятных сценариев (т. е. времени с момента эвакуации БПУ до тех пор, пока оперативный персонал не будет перемещен и мобилизован в РПУ, а затем полностью не оценит состояние АС и таким образом не будет готов предпринять какие-либо требуемые действия);

e) обоснование того, что передача управления из БПУ в РПУ может быть выполнена надежно и в течение требуемого времени, т. е. результаты указанного в перечислении d) анализа, при проведении которого учитываются возможные опасные воздействия, надежность оборудования и влияние человеческого фактора, который в свою очередь зависит от особенностей политики отбора персонала, требований к персоналу на площадке АС и от требований норм и правил.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных документов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного документа	Степень соответствия	Обозначение и наименование соответствующего национального, межгосударственного стандарта
IEC 60709	IDT	ГОСТ Р МЭК 60709—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
IEC 60964:2009	IDT	ГОСТ Р МЭК 60964—2012 «Атомные станции. Пункты управления. Проектирование»
IEC 61226	IDT	ГОСТ Р МЭК 61226—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
IEC 61513	IDT	ГОСТ Р МЭК 61513—2020 «Системы контроля и управления, важные для безопасности атомной станции. Общие требования»
IEC 61771	—	*
IEC 62646	—	*
ISO 11064-1	IDT	ГОСТ Р ИСО 11064-1—2015 «Эргономическое проектирование центров управления. Часть 1. Принципы проектирования»
ISO 11064-3	IDT	ГОСТ Р ИСО 11064-3—2015 «Эргономическое проектирование центров управления. Часть 3. Расположение зала управления»
ISO 11064-6	IDT	ГОСТ Р ИСО 11064-6—2013 «Эргономическое проектирование центров управления. Часть 6. Требования к окружающей среде»
IAEA SSR-2/1:2012	—	**
IAEA Safety Guide NS-G-1.3:2002	—	**

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

** Текст документа на русском языке доступен на сайте http://www.iaea.org/.

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

- IDT — идентичные стандарты.

Библиография

IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification

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

IEC 60980, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations

IEC 61227, Nuclear power plants — Control rooms — Operator controls

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 61772, Nuclear power plants — Control rooms — Application of visual display units (VDUs)

IEC 61839, Nuclear power plants — Design of control rooms — Functional analysis and assignment

IEC 62138, Nuclear power plants — Instrumentation and control systems important to 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 62645, Nuclear power plants — Instrumentation and control systems — Requirements for security programmes for computer-based systems

ISO 9241, Ergonomics of human-system interaction

IAEA GS-R-3:2006, The management system for facilities and activities

IAEA Safety Guide No, GS-G-3.1:2006, Application of the management system for facilities and activities

IAEA Safety Guide No, GS-G-3.5:2009, Management system for nuclear installations

IAEA SSR-2/2, Safety of Nuclear Power Plants: Commissioning and Operation

IAEA Safety Guide NS-G-1.3:2002, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants

IAEA Safety Glossary: 2007, Terminology used in nuclear safety and radiation protection

УДК 621.311.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: резервный пункт управления, блочный пункт управления, атомные станции, системы контроля и управления, важные для безопасности; категории функций безопасности, верификация, отказ

БЗ 3—2020/27

Редактор *Л.И. Нахимова*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.023.2020 Подписано в печать 10.03.2020. Формат 60×84⅛ Гарнитура Ариал
Усл. печ. л. 2,79. Уч.-изд. л. 2,40.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к 2.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru