Настоящая публикация была заменена публикацией SSG-39.

СЕРИЯ НОРМ МАГАТЭ ПО БЕЗОПАСНОСТИ

Системы контрольно-измерительных приборов и управления, важные для безопасности атомных электростанций

РУКОВОДСТВО

№ NS-G-1.3

IAEA
Международное агентство по атомной энергии

СИСТЕМЫ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ
АВСТРИЯ
АЗЕРБАЙДЖАН
АЛБАНИЯ
АЛЖИР
АНГОЛА
АРГЕНТИНА
АРМЕНИЯ
АФГАНИСТАН
БАНГЛАДЕШ
БЕЛАРУСЬ
БЕЛЬГИЯ
БЕЛИЗ
БЕНИН
БОЛГАРИЯ
БОЛИВИЯ
БОСНИЯ И ГЕРЦЕГОВИНА
БОТСВАНА
БРАЗИЛИЯ
БУРКИНА-ФАСО
БЫВШАЯ ЮГОСЛ. РЕСП. МАКЕДОНИЯ
ВЕНГРИЯ
ВЕНЕСУЭЛА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАНА
ГВАТЕМАЛА
ГЕРМАНИЯ
ГОНДУРАС
ГРЕЦИЯ
ГРУЗИЯ
ДАНИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО
ДОМИНИКАНСКАЯ РЕСПУБЛИКА
ЕГИПЕТ
ЗАМБИЯ
ЗИМБАБВЕ
ИЗРАИЛЬ
ИНДИЯ
ИНДОНЕЗИЯ
ИОРДАНИЯ
ИРАК
ИРАН, ИСЛАМСКАЯ РЕСПУБЛИКА
ИРЛАНДИЯ
ИСЛАНДИЯ
ИСПАНИЯ
ИТАЛИЯ
ЙЕМЕН
КАЗАХСТАН
КАМЕРУН
КАНАДА
КАТАР
КЕНИЯ
КИПР
КИТАЙ
КОЛУМБИЯ
КОРЕЯ, РЕСПУБЛИКА
КОСТА-РИКА
КОТ-Д'ИВУАР
КУБА
КУВЕЙТ
КЫРГЫЗСТАН
ЛАТВИЯ
ЛИБЕРИЯ
ЛИВАН
ЛИВИЙСКАЯ АРАБСКАЯ ДЖАМАХИРИЯ
ЛИТВА
ЛИХТЕНШТЕЙН
ЛЮКСЕМБУРГ
МАВРИКИЙ
МАВРИТАНИЯ
МАДАГАСКАР
МАЛАВИ
МАЛАЙЗИЯ
МАЛИ
МАЛЬТА
МАРОККО
МАРШАЛЛОВЫ ОСТРОВА
МЕКСИКА
МОНАКО
МОНГОЛИЯ
МОЗАМБИК
МЬЯНМА
НАМИБИЯ
НИГЕР
НИГЕРИЯ
НИДЕРЛАНДЫ
НИКАРАГУА
НОВАЯ ЗЕЛАНДИЯ
НОРВЕГИЯ
ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ
ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ
ПАКИСТАН
ПАЛАУ
ПАНАМА
ПАРАГВАЙ
ПЕРУ
ПОЛЬША
ПОРТУГАЛИЯ
РЕСПУБЛИКА МОЛДОВА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
РУМЫНИЯ
САЛЬВАДОР
САУДОВСКАЯ АРАВИЯ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СВЯТЕЙШИЙ ПРЕСТОЛ
СЕНЕГАЛ
СЕРБИЯ
СИНГАПУР
СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
СЛОВАКИЯ
СЛОВЕНИЯ
СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
СУДАН
СЬЕРРА-ЛЕОНЕ
ТАДЖИКИСТАН
ТАИЛАНД
ТУНИС
ТУРЦИЯ
УГАНДА
УЗБЕКИСТАН
УКРАИНА
УРУГВАЙ
ФИЛИППИНЫ
ФИНЛЯНДИЯ
ФРАНЦИЯ
ХОРВАТИЯ
ЦЕНТРАЛЬНОАФРИКАНСКАЯ РЕСПУБЛИКА
ЧАД
ЧЕРНОГОРИЯ
ЧЕШСКАЯ РЕСПУБЛИКА
ЧИЛИ
ШВЕЙЦАРИЯ
ШВЕЦИЯ
ШРИ-ЛАНКА
ЭКВАДОР
ЭРИТРЕЯ
ЭСТОНИЯ
ЭФИОПИЯ
ЮЖНАЯ АФРИКА
ЯМАЙКА
ЯПОНИЯ

Устав Агентства был утвержден 23 октября 1956 года на Конференции по выработке Устава МАГАТЭ, которая состоялась в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке. Устав вступил в силу 29 июля 1957 года. Центральные учреждения Агентства находятся в Вене. Главной целью Агентства является достижение “более скорого и широкого использования атомной энергии для поддержания мира, здоровья и благосостояния во всем мире”.

Серия норм по безопасности, № NS-G-1.3

СИСТЕМЫ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

Руководство по безопасности

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2008 ГОД

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Группа продажи и рекламы
Издательская секция
Международное агентство по атомной энергии
Wagramer Strasse 5
P.O. Box 100
1400 Vienna, Austria
факс: +43 1 2600 29302
тел.: +43 1 2600 22417
эл. почта: sales.publications@iaea.org
веб-сайт: http://www.iaea.org/books

Напечатано МАГАТЭ в Австрии
Апрель 2008

СИСТЕМЫ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ
МАГАТЭ, ВЕНА, 2008
STI/PUB 1116
ISBN 978–92–0–403108–9
ISSN 1020–5845

ПРЕДИСЛОВИЕ

Мохамед ЭльБарадей
Генеральный директор

Одна из уставных функций МАГАТЭ сводится к тому, чтобы устанавливать или применять нормы безопасности для охраны здоровья, жизни и имущества в деятельности по освоению и применению ядерной энергии в мирных целях, а также обеспечивать применение этих норм как в своей собственной работе, так и в работе, в которой оказывается помощь, и, по требованию сторон, в деятельности, проводимой на основании любого двустороннего или многостороннего соглашения, или, по требованию того или иного государства, к любому виду деятельности этого государства в области ядерной энергии.

Наблюдение за разработкой норм безопасности осуществляют следующие консультативные органы: Консультативная комиссия по нормам безопасности (ККНБ); Комитет по нормам ядерной безопасности (НУССК); Комитет по нормам радиационной безопасности (РАССК); Комитет по нормам безопасности перевозки (ТРАНССК); и Комитет по нормам безопасности отходов (ВАССК). Государства-члены широко представлены в этих комитетах.

Чтобы обеспечить широчайший международный консенсус, нормы безопасности направляются также всем государствам-членам для замечаний перед их одобрением Советом управляющих МАГАТЭ (в случае Основ безопасности и Требований безопасности) или, от имени Генерального директора, Комитетом по публикациям (в случае Руководств по безопасности).

Нормы безопасности МАГАТЭ не имеют юридически обязательной силы для государств-членов, но они могут приниматься ими по их собственному усмотрению для использования в национальных регулирующих положениях, касающихся их собственной деятельности. Эти нормы обязательны для МАГАТЭ в отношении его собственной работы и для государств в отношении операций, в которых МАГАТЭ оказывает помощь. Любое государство, желающее вступить в соглашение с МАГАТЭ, касающееся его помощи в связи с выбором площадки, проектированием, строительством, вводом в эксплуатацию, эксплуатацией или снятием с эксплуатации ядерной установки или любой другой деятельностью, должно будет выполнять те части норм безопасности, которые относятся к деятельности, охватываемой соглашением. Однако следует помнить, что ответственность за принятие окончательных решений и юридическая ответственность в любых процедурах лицензирования возлагается на государства.

Нормы безопасности устанавливают важнейшие основы для безопасности, однако может также потребоваться включение более детальных требований, отражающих национальную практику. Кроме того, будут включаться, как правило, специальные вопросы, которые должны оцениваться на индивидуальной основе.

Физическая защита делящихся и радиоактивных материалов и АЭС в целом упоминается в надлежащих случаях, но не рассматривается подробно; к обязательствам государств в этом отношении следует подходить на основе соответствующих договорно-правовых документов и публикаций, разработанных под эгидой МАГАТЭ. Нерадиологические аспекты техники безопасности на производстве и охраны окружающей среды также прямо не рассматриваются; признано, что государства должны выполнять свои международные обязательства и обязанности относительно них.

Требования и рекомендации, изложенные в нормах безопасности МАГАТЭ, возможно, не полностью соблюдаются на некоторых установках, построенных в соответствии с принятыми ранее нормами. Решения о том, как нормы безопасности должны применяться на таких установках, будут приниматься государствами.

Внимание государств обращается на тот факт, что нормы безопасности МАГАТЭ, не являясь юридически обязательными, разработаны с целью обеспечения того, чтобы мирные применения ядерной энергии и радиоактивных материалов осуществлялись таким образом, который дает возможность государствам выполнять свои обязательства в соответствии с общепринятыми принципами международного права и правилами, касающимися охраны окружающей среды. Согласно одному такому общему принципу территория государства не должна использоваться так, чтобы причинить ущерб в другом государстве. Государства, следовательно, обязаны проявлять должную осмотрительность и соответствующую меру заботливости.

Гражданская ядерная деятельность, осуществляемая в рамках юрисдикции государств, как и любая другая деятельность, подпадает под действие обязательств, которые государства могут принимать согласно международным конвенциям в дополнение к общепринятым принципам международного права. Государствам надлежит принимать в рамках своих национальных правовых систем такое законодательство (включая правила) и другие нормы и меры, которые могут быть необходимы для эффективного выполнения всех взятых на себя международных обязательств.

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Дополнение, если оно включено, представляет собой неотъемлемую часть норм и имеет тот же статус, что и основной текст. Приложения, сноски и списки литературы, если они включены, содержат дополнительную информацию или практические примеры, которые могут оказаться полезными для пользователя.

Формулировка "должен, должна, должно, должны" используется в нормах безопасности в случаях, когда речь идет о требованиях, обязанностях и обязательствах. Использование формулировки "следует" означает рекомендацию желательного варианта.

Официальным текстом является английский вариант.

Настоящая публикация была заменена публикацией SSG-39.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1. Настоящее Руководство по безопасности было подготовлено в рамках программы МАГАТЭ по разработке норм безопасности для атомных электростанций. Оно дополняет публикацию в Серии норм безопасности, № NS-R-1, «Безопасность атомных электростанций: проектирование» [1] (Требования к проектированию), в которой устанавливаются проектные требования для обеспечения безопасности атомных электростанций. Настоящее Руководство по безопасности указывает, как эти требования следует выполнять применительно к системам контрольно-измерительных приборов и управления (КИПиУ), важным для безопасности.

1.2. Данная публикация представляет собой пересмотр двух предыдущих Руководств по безопасности: Серий изданий по безопасности, №№ 50-SG-D3 и 50-SG-D8, в объединенном документе, и настоящее новое Руководство по безопасности заменяет эти предыдущие руководства.

1.3. При пересмотре были учтены разработки в области систем КИПиУ, важных для безопасности, появившиеся после опубликования в 1980 и 1984 годах, соответственно, предыдущих Руководств по безопасности. Основные изменения сводятся к следующему:

— В настоящем Руководстве по безопасности учитываются разработки в использовании компьютеризованных систем КИПиУ, важных для безопасности.
— При пересмотре публикаций Серии изданий по безопасности, №№ 50-SG-D3 и 50-SG-D8, рассматриваются все системы КИПиУ, важные для безопасности. Упорядочены и представлены руководящие материалы, касающиеся требований и критериев, изложенных в [1].
— Настоящее Руководство по безопасности рассчитано на использование вместе и в увязке с Требованиями к проектированию [1] и соответствующими руководствами по безопасности, касающимися программного обеспечения [2] и обеспечения качества ([3], Руководства по безопасности Q3 и Q10).
— Приведены руководящие материалы по классификации систем КИПиУ, важных для безопасности, на основе других международных стандартов.

ЦЕЛЬ

1.4. Настоящее Руководство по безопасности содержит руководящие материалы по проектированию систем КИПиУ, важных для безопасности атомных электростанций, включая все элементы КИПиУ от датчиков механических систем до исполнительного оборудования, интерфейсы оператора и вспомогательное оборудование.

1.5. В настоящем Руководстве по безопасности излагаются главным образом проектные требования, предъявляемые к системам КИПиУ, которые являются важными для безопасности. Оно дополняет положения пунктов документа [1], касающиеся систем КИПиУ, важных для безопасности.

1.6. Настоящая публикация предназначена для использования прежде всего разработчиками проектов атомных электростанций, а также владельцами и/или операторами (эксплуатирующими организациями) и регулирующими органами атомных электростанций.

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.7. Настоящее Руководство по безопасности содержит общие руководящие материалы по важным для безопасности системам КИПиУ, предназначенным для широкого использования применительно ко многим АЭС. Более детальные требования и ограничения в отношении безопасной эксплуатации конкретных типов станции следует разрабатывать и вводить в действие в процессе проектирования. Руководящие материалы данной публикации содержат принципы проектирования систем, важных для безопасности, которые требуют особого внимания, и их следует применять как при проектировании новых систем КИПиУ, так и при модернизации существующих систем. Приводятся также руководящие материалы по тому, как следует применять принципы проектирования и по основам метода классификации систем в зависимости от их важности для безопасности.

1.8. Согласно определениям, данным в [1], системы КИПиУ, важные для безопасности, это – системы КИПиУ, которые являются частью группы безопасности и систем КИПиУ, неисправность или отказ которых может привести к радиационному облучению персонала на площадке или лиц из населения. Примерами таких систем являются:

— система защиты реактора;

— системы управления реактивностью;
— системы мониторинга и контроля нормального охлаждения реактора;
— системы мониторинга и контроля аварийного энергоснабжения;
— системы изоляции защитной оболочки.

1.9. Серия технических докладов МАГАТЭ, № 387 [4], содержит общий обзор концепций и примеров систем, рассматриваемых в настоящем Руководстве по безопасности, и может служить полезным справочным материалом для некоторых пользователей.

СТРУКТУРА

1.10. Содержание настоящей публикации построено в соответствии с требованиями и критериями документа [1] и включает руководящие принципы по системам КИПиУ, важным для безопасности.

1.11. В разделе 2 приводится определение функций и систем КИПиУ в рамках содержания настоящего Руководства по безопасности, а также дана классификация функций и систем, обеспечивающих безопасность или связанных с обеспечением безопасности. Раздел 3 содержит определение проектных основ для систем КИПиУ, важных для безопасности. В разделе 4 даны руководящие материалы по проектированию систем КИПиУ, важных для безопасности. В него включены руководящие материалы, которые применяются ко всем системам КИПиУ, важным для безопасности, а также руководящие материалы, которые применяются только к системам безопасности. Применение руководящих материалов к этим двум классам разъясняется в тексте и иллюстрируется таблицей I. В разделе 5 представлены дополнительные руководящие материалы, предназначенные для определенных систем КИПиУ, а именно, систем защиты, источников энергоснабжения и цифровых компьютерных систем. Руководящие материалы для этих систем включают общие руководящие материалы, приведенные в разделе 4, и конкретные руководящие материалы, изложенные в разделе 5. Раздел 6 дополняет руководящие материалы, приведенные в разделе 4 применительно к вопросам взаимодействия человек-машина. Раздел 7 дополняет руководящие материалы, изложенные в разделе 4 в отношении процессов проектирования применительно к обеспечению качества.

1.12. Содержание разделов 4, 5, 6 и 7, как правило, строится с учетом значимости каждой темы для безопасности и с точки зрения Требований к

проектированию. По каждой теме приводятся конкретные руководящие материалы.

2. СИСТЕМЫ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ И УПРАВЛЕНИЯ, ВАЖНЫЕ ДЛЯ БЕЗОПАСНОСТИ

2.1. В соответствии с Требованиями к проектированию все системы и элементы КИПиУ (включая программное обеспечение для систем КИПиУ), которые являются узлами, важными для безопасности, первоначально должны быть определены, а затем классифицированы на основе их функций и значимости с точки зрения безопасности (см. [1], пункт 5.1).

ОПРЕДЕЛЕНИЕ СИСТЕМ КИПиУ

2.2. Принадлежность к системам КИПиУ, важным для безопасности, устанавливается на основе определения необходимых функций безопасности, выполняемых системами КИПиУ, и определения систем, которые выполняют определенные сочетания этих функций. В данном разделе рассматривается типичный процесс определения систем, важных для безопасности.

Функции станции, важные для безопасности

2.3. Существует ряд важнейших функций, которые должны выполняться с целью обеспечения безопасной и эффективной эксплуатации атомной электростанции, и это может включить использование систем КИПиУ. В публикации [1] пункт 4.6 определяет следующие главные функции безопасности, которые требуется выполнять для обеспечения безопасности:

— управление реактивностью;
— отвод тепла из активной зоны, и
— локализация радиоактивных материалов и контроль эксплуатационных сбросов, а также ограничение аварийных выбросов.

2.4. Для определения систем, конструкций и элементов, необходимых для выполнения этих функций безопасности после постулируемого исходного события (ПИС), следует применять системный подход.

2.5. Указанные главные функции безопасности подробно рассматриваются ниже с целью более полного описания функций, которые требуется выполнять для обеспечения безопасности. В этот дополненный набор функций входят функции, необходимые для предотвращения аварийных условий, а также функции, необходимые для смягчения последствий аварийных условий. Они могут выполняться в надлежащих случаях с использованием конструкций, систем и элементов, предусматриваемых для нормальной эксплуатации, с целью исключения того, чтобы ожидаемые при эксплуатации события приводили к аварийным условиям, или смягчения последствий аварийных условий.

Функции безопасности для управления реактивностью:

— обеспечение нормального управления реактивностью в безопасных пределах;
— предотвращение неприемлемых переходных изменений радиоактивности;
— останов реактора, когда это необходимо, с тем чтобы воспрепятствовать тому, чтобы ожидаемые при эксплуатации события приводили к условиям проектных аварий;
— останов реактора для смягчения последствий аварийных условий; и
— поддержание реактора в режиме безопасного останова после всех действий, направленных на останов;

Функции безопасности для отвода тепла из активной зоны:

— отвод тепла из активной зоны во время работы на мощности;
— отвод остаточного тепла в соответствующих эксплуатационных состояниях и условиях проектных аварий с неповрежденным контуром теплоносителя реактора;
— поддержание достаточного запаса теплоносителя для охлаждения активной зоны в нормальных эксплуатационных состояниях и после любых ПИС;
— удаление тепла из активной зоны после отказа контура теплоносителя реактора с целью ограничения повреждения топлива; и
— передача тепла конечному поглотителю тепла от промежуточных теплоотводов, используемых для отвода тепла из активной зоны.

Функции безопасности для локализации радиоактивных материалов и ограничения аварийных выбросов, а также для ограничения аварийных выбросов:

— сохранение целостности оболочек твэлов в активной зоне реактора;
— сохранение целостности контура теплоносителя реактора; и
— ограничение выброса радиоактивных материалов и сведение к минимуму облучения населения и персонала.

2.6. Следует обеспечивать, чтобы указанные выше функции, важные для безопасности, выполнялись за счет применения инженерно-технических систем, в том числе систем КИПиУ. В случае систем КИПиУ в число типичных первичных функций, важных для безопасности, входят:

— функции защиты;
— функции управления;
— функции контроля и индикации; и
— функции проведения испытаний.

2.7. Кроме того, существуют функции обслуживания, также важные для безопасности, выполнение которых следуют обеспечивать в поддержку первичных функций. Примеры таких функций обслуживания включают обеспечение подачи электро-, пневмо- или гидроэнергии, передачу данных, а также функции контроля и проведения испытаний, которые поддерживают системы, выполняющие первичные функции.

2.8. Первичные функции систем КИПиУ, важные для безопасности, можно охарактеризовать следующим образом:

Функции защиты

2.9. Функции защиты обеспечивают «оборонительную» линию против отказов в других системах станции. Они входят в число наиболее важных функций безопасности и имеют прямое отношение к ядерной безопасности в плане защиты персонала и населения в случае серьезного отказа.

Функции управления

2.10. Функции управления обеспечивают уверенность в том, что станция будет управляться и ее состояние будет поддерживаться в пределах рабочих режимов при нормальных и ненормальных условиях. Функции управления могут также

смягчать последствия переходных режимов станции или ПИС, тем самым способствуя обеспечению ядерной безопасности путем сведения к минимуму потребностей в срабатывании функций защиты.

Функции контроля и индикации

2.11. Функции контроля и индикации обеспечивают взаимосвязь между станцией и персоналом, осуществляющим эксплуатацию и техническое обслуживание. Эти функции являются важными для безопасности, поскольку они позволяют персоналу станции определять переходные режимы и поддерживать состояние станции в пределах рабочих режимов безопасной эксплуатации.

Функции проведения испытаний

2.12. Функции проведения испытаний обеспечивают уверенность в готовности к срабатыванию и эффективности других функций, важных для безопасности, и позволяют подтверждать отсутствие их деградации.

Примеры систем КИПиУ, важных для безопасности

2.13. Приведенный ниже список, составленный с учетом соответствующих функций станции, важных для безопасности, содержит примеры систем КИПиУ, важных для безопасности.

2.14. Системы КИПиУ, предусматриваемые для осуществления функций, связанных с управлением реактивностью, включают:

— системы, которые обеспечивают запуск останова реактора (аварийное отключение);
— системы, используемые для контроля или поддержания параметров станции в рамках:
  • эксплуатационных пределов, важных для безопасности (такие, как системы контроля температуры теплоносителя),
  • пределов, принятых в качестве начальных условий в анализе безопасности (такие, как системы контроля пределов мощности реактора);
— системы, неисправность или отказ которых могут посылать соответствующие сигналы на системы, обеспечивающие функции защиты, такие, как системы управления реактивностью;

— системы, которые выполняют функции, важные для поддержания условий безопасного останова, например, средства вычисления запаса до критичности;
— системы, которые выполняют функции, важные для предотвращения, прекращения или смягчения последствий ожидаемых при эксплуатации событий или условий проектных аварий, например, системы снижения мощности реактора до заданного уровня; и
— системы, предусматриваемые непосредственно для обеспечения неодинакового резервирования систем, выполняющих функции защиты, например, системы, которые смягчают последствия ожидаемых переходных режимов без срабатывания аварийной защиты или систем, которые компенсируют возможные ошибки в проектировании.

2.15. Системы КИПиУ, предусматриваемые для осуществления функций, связанных с отводом тепла из активной зоны, включают:

— такие системы, как системы защиты реактора, и системы обслуживания (исполнительные системы) инженерно-технических средств безопасности, которые автоматически включают соответствующие системы для обеспечения того, чтобы установленные в проекте пределы не превышались в результате ожидаемых при эксплуатации событий, для определения условий проектных аварий и смягчения их последствий или для отмены небезопасных действий системы управления; и
— системы, контролирующие условия окружающей среды на станции, которые являются необходимыми для надлежащего функционирования оборудования станции, важного для безопасности, и пребывания персонала на станции.

2.16. Системы КИПиУ, предусматриваемые для осуществления функций локализации радиоактивных материалов и ограничения аварийных выбросов, а также ограничения аварийных выбросов, включают:

— системы, неисправность или отказ которых может приводить к выбросу радиоактивного материала в окружающую среду и для которых системы безопасности не предусматриваются, например, системы, которые используются для управления обращением с отходами и охлаждением отработавшего топлива;
— системы, используемые для обнаружения и измерения утечек из системы теплоносителя реактора;

— системы, используемые для контроля природных или техногенных явлений или управления ими, которые могут отрицательно влиять на безопасность, например, сейсмические мониторы; и
— системы, используемые для аварийного мониторинга и оценки, например, системы, которые контролируют и регистрируют при необходимости давление в защитной оболочке, активность в защитной оболочке, параметры охлаждения активной зоны реактора, радиоактивные выбросы в окружающую среду и метеорологическую информацию.

2.17. Системы КИПиУ, предусматриваемые для поддержки осуществления других функций, важных для безопасности, включают:

— системы, которые обеспечивают выполнение вспомогательной функции для нескольких систем КИПиУ, важных для безопасности, например, систем передачи цифровых данных, которые осуществляют передачу сигналов между системами и между элементами систем;
— системы, используемые для контроля состояния систем безопасности, например, системы, которые контролируют отказ каналов безопасности и дефекты в трубопроводах, клапанах или насосах систем безопасности;
— системы, которые могут использоваться в процессе эксплуатации систем безопасности, например, для испытания системы защиты; и
— другие специальные применения КИПиУ, важные для безопасности, например, для обеспечения связи, обнаружения и тушения пожаров, а также контроля доступа.

Типы систем КИПиУ, важных для безопасности

2.18. На основе определения требующихся функций безопасности предусматриваются системы КИПиУ, которые должны выполнять функции, важные для безопасности. Обычно используются следующие типы систем.

Системы защиты

2.19. Системы защиты – это тип систем КИПиУ, важных для безопасности, которые имеют особое значение. Требования к проектированию предписывают (см. [1], пункт 6.80): “Система защиты должна проектироваться с таким расчетом, чтобы она:

(1) автоматически приводила в действие соответствующие системы, включая, если требуется, системы останова реактора, с тем чтобы предотвратить

превышение установленных проектных пределов для ожидаемых при эксплуатации событий;

(2) обнаруживала проектные аварии и приводила в действие системы, требующиеся для уменьшения последствий таких аварий в рамках основы проекта;

(3) была в состоянии подавлять небезопасные действия системы контроля и управления.”

2.20. Следует отметить, что термин 'система защиты' используется не во всех государствах-членах, и существуют некоторые допустимые расхождения в детальной структуре системы или систем, которые выполняют функции защиты. Например, в некоторых государствах-членах для выполнения функций детектирования и приведения в действие систем безопасности, которые перечислены выше, вместо общей системы защиты применяются подсистемы КИПиУ независимых специальных систем обеспечения безопасности. В таких случаях руководящие материалы, приведенные в настоящем Руководстве по безопасности, применяются к группам соответствующих систем КИПиУ.

Системы блокировки

2.21. Системы блокировки предотвращают возникновение небезопасных режимов или небезопасные операции, обеспечивают защиту персонала и предотвращают опасности. Блокировки предотвращают действия, которые могут приводить к возникновению опасности для станции или к повреждению станции, или же к усугублению этих ситуаций, и обычно не включают действия, направленные на исправление ситуации. Функции блокировки могут быть активными функциями, которые поддерживают непрерывное действие, препятствующее развитию данного состояния, или пассивными функциями, которые предотвращают какое-либо действие.

2.22. Функции блокировки могут обеспечиваться механическими средствами или же административными методами и электрическими средствами. Механические и административные функции блокировки не входят в сферу применения настоящего Руководства по безопасности.

Системы управления

2.23. В состав систем управления входят все виды оборудования и элементы, используемые в автоматическом и ручном режиме для управления параметрами станции, от средств связи с датчиками процессов до исполнительных

устройств, которые оказывают прямое воздействие на физические процессы, влияющие на значения параметров, управление которыми осуществляется.

2.24. Системы управления поддерживают параметры процесса в пределах, принятых в анализе безопасности станции. Для того, чтобы допущения, принимаемые в анализе безопасности, соблюдались, определенные параметры должны удерживаться в пределах, установленных для начальных условий ожидаемого при эксплуатации события или проектной аварии. Вероятность того, что данные параметры будут оставаться в рамках этих установленных пределов, зависит от надежности систем управления, которые поддерживают параметры, и от надежности контрольно-измерительных систем, которые контролируют эти параметры и направляют сигналы о любых отклонениях оператору для принятия корректирующих мер.

2.25. Отказы в системе управления могут потребовать срабатывания системы защиты; т.е. отказ системы управления может составлять ПИС. Следует обеспечивать, чтобы любые отказы в системах автоматического управления автоматически включали переход на ручное управление. Следует предусматривать, чтобы при отказе системы автоматического управления, который приводит к автоматическому переходу на ручное управление, оператору направлялся соответствующий сигнал-предупреждение об изменении режима управления.

Информационные системы

2.26. В состав информационных систем входят оборудование и элементы, такие, как датчики, оборудование, которое преобразует сигналы, поступающие от датчиков, в сигналы, пригодные для индикации или регистрации, передатчики звуковых сигналов, световые индикаторы, контрольно-измерительные приборы, видеомониторы, регистраторы, принтеры и твердотельные индикаторные устройства (устройства отображения информации).

2.27. Информационная система снабжает операторов станции информацией о режиме безопасности систем или станции, которую операторы могут использовать для определения действий, выполняемых вручную, которые необходимы для обеспечения безопасности станции. В условиях нормальной эксплуатации операторы постоянно контролируют состояние станции с помощью индикаторов (устройств отображения информации), а также сигнализаторов или устройств визуального отображения, которые находятся в помещении центрального щита управления.

2.28. Информационная система также обеспечивает специалистов по безопасности на площадке и за ее пределами информацией о состоянии станции в аварийных условиях. Помещение центрального щита управления является информационно-оперативным центром станции для операторов в условиях нормальной эксплуатации, ожидаемых при эксплуатации событий, проектных аварий и тяжелых аварий. Оно может также использоваться в качестве первичного центра для управления действиями за пределами площадки на начальной стадии в случае аварийной ситуации.

2.29. В случае аварийной ситуации на площадке может находиться значительное количество специалистов. Если для размещения специалистов выделяются отдельные помещения (центр технической поддержки, аварийный эксплуатационный центр или центр аварийного реагирования), эти помещения следует оснащать информационными системами (устройствами визуального отображения, эксплуатационными регламентами, руководствами по эксплуатации систем) для того, чтобы дать возможность специалистам выполнять свои функции. В составе информационных систем могут быть линии прямой связи со специалистами, которым разрешается находиться в помещении центрального щита управления.

2.30. Информационная система регистрирует или отображает на экране или в виде распечаток краткосрочные и долгосрочные тенденции развития параметров процессов, важных для безопасности, в целях выполнения срочного или последующего анализа, а также для представления отчетов внутри эксплуатирующей организации и внешним компетентным органам. Регистрационные записи или распечатки хранятся в помещении центрального щита управления и рядом с ним (и возможно на компьютерном жестком диске для облегчения доступа) и содержат аналоговые параметры процессов и двоичные сигналы для того, чтобы обеспечить доступ к хронологической информации о функционировании и поведении станции. Эта информация необходима в качестве: 1) резервной информации для дежурных операторов (отображение краткосрочных и долгосрочных тенденций), 2) общей эксплуатационной информации для административного руководства станции и 3) материала для долгосрочного анализа эксплуатации и аварий.

Системы ограничения

2.31. В состав систем ограничения входят все виды оборудования и элементы, предназначенные для снижения частоты возникновения ПИС, которые в этой связи включаются в анализ безопасности станции, если это признается обоснованным. Функциями, иногда осуществляемыми системами ограничения,

являются, например, блокировка регулирующих стержней и снижение мощности реактора.

2.32. Некоторые государства-члены прямо включают системы ограничения в свои регулирующие положения и проекты. В других государствах-членах функции ограничения могут предусматриваться в нормальных системах управления.

Системы снижения риска

2.33. В состав систем снижения риска входят все виды оборудования и элементы, предусматриваемые специально для снижения вероятности повреждения активной зоны в случае последовательности многократных отказов, а также для предотвращения возникновения исходного события (например, путем приведения в действие дополнительной специализированной системы останова или дополнительного средства включения аварийной системы подачи питательной воды), а не для смягчения последствий события (например, использование неодинаковых генераторов в случае обесточивания станции).

2.34. Некоторые государства-члены прямо включают системы снижения риска в свои регулирующие положения и проекты. В других государствах-членах функции снижения риска могут предусматриваться в нормальных системах управления.

2.35. Следует отметить, что типичные функции КИПиУ редко являются взаимоисключающими в системе; например, системы управления часто служат в качестве источника данных, используемых информационными системами, и в состав систем блокировки редко включаются отдельные системы.

КЛАССИФИКАЦИЯ СИСТЕМ КИПиУ

2.36. В пунктах 2.13–2.35 системы КИПиУ, важные для безопасности, связаны с выполнением главных функций безопасности, определенных в Требованиях к проектированию [1]. Однако это не подразумевает наличие градаций в важности для безопасности этих систем КИПиУ; конкретная система КИПиУ может обеспечивать выполнение одной или нескольких главных функций безопасности. Вместе с тем градация важности для безопасности этих систем КИПиУ необходима и обеспечивается посредством классификации систем

КИПиУ, важных для безопасности. Проведение такой классификации требуется в [1], пункт 5.1.

2.37. В частности, Требования к проектированию предусматривают (см. [1], пункт 5.2), что метод классификации конструкций, систем или элементов на основе их значимости для безопасности прежде всего должен быть основан на детерминированных методах, дополненных при необходимости вероятностными методами и инженерно-техническими заключениями, с учетом таких факторов, как:

— выполняемые функции безопасности;
— последствия отказа системы КИПиУ;
— вероятность того, что от данной системы КИПиУ потребуется выполнение функции безопасности;
— время после ПИС или период, в течение которого от системы КИПиУ потребуется действие.

2.38. В методе классификации в дополнение к учету указанных выше факторов, как это требуется в [1], при определении класса системы КИПиУ следует также учитывать перечисленные ниже факторы. Критерии, изложенные при описании этих факторов для иллюстративных целей, следует выбирать таким образом, чтобы обеспечивалась количественная и/или качественная индикация относительной важности для безопасности классифицируемой системы КИПиУ:

— вероятность ПИС и потенциальная тяжесть их последствий, если происходит отказ системы КИПиУ (например, высокая, средняя или низкая вероятность, с большими, средними или малыми последствиями (например, радиологическими последствиями));
— потенциал самой системы КИПиУ приводить к возникновению ПИС (т.е. определенных видов отказа системы КИПиУ), средства, предусматриваемые в системах безопасности или в других системах КИПиУ, на которые распространяется настоящее Руководство по безопасности, для учета такого ПИС (т.е. средства для обнаружения отказа системы КИПиУ) и сочетание расчета вероятности и последствий такого ПИС (т.е. частота отказов и радиологических последствий);
— период времени, в течение которого требуется функционирование системы КИПиУ после срабатывания функции безопасности (например, мене 12 ч, более 12 ч);
— своевременность и надежность, с которой могут быть предприняты альтернативные действия (например, срочно/низкая надежность, свыше 30 мин/высокая надежность); и

— своевременность (например, менее 12 ч, свыше 12 ч) и надежность, с которой может быть обнаружен и устранен любой отказ в системе КИПиУ.

2.39. После рассмотрения каждого из факторов для каждой системы КИПиУ следует принимать решение в отношении классификации системы КИПиУ.

2.40. Системы КИПиУ подразделяются в целом на два класса: системы, выполняющие функции, которые являются важными для безопасности, и системы, выполняющие функции, которые не являются важными для безопасности (см. рис. 1). Системы КИПиУ, важные для безопасности, – это системы, используемые для выполнения основных функций, важных для безопасности, как указывалось ранее в данном разделе. Класс «системы КИПиУ, важные для безопасности» подразделяется на два основных подкласса следующим образом:

— «системы безопасности КИПиУ», представляющие собой системы КИПиУ, важные для безопасности, которые выполняют первичные функции безопасности, как определено в Требованиях к проектированию; т.е. они гарантируют безопасный останов реактора или отвод остаточного тепла из активной зоны, либо ограничивают последствия ожидаемых при эксплуатации событий и проектных аварий;
— «связанные с обеспечением безопасности системы КИПиУ», которыми являются системы КИПиУ, важные для безопасности, выполняющие другие функции, важные для безопасности, которые не выполняются системами безопасности КИПиУ.

2.41. В состав систем безопасности КИПиУ входят системы, которые обеспечивают функции защиты. Эти функции обычно обеспечивает система, известная как система защиты реактора, или подсистемы КИПиУ специальных систем безопасности, таких, как системы останова реактора, система аварийного охлаждения активной зоны реактора и система изоляции защитной оболочки. Системы безопасности КИПиУ могут также выполнять функции послеаварийного контроля и вспомогательные функции (например, системы передачи важных данных для систем защиты или специальных систем безопасности).

2.42. Типичные примеры систем КИПиУ, связанных с обеспечением безопасности, включают системы управления, системы контроля и индикации, а также другие системы, за исключением систем, включенных в класс систем безопасности или относящихся к этому классу, системы ограничения или системы снижения риска.

РИС. 1. Примеры систем КИПиУ, важных для безопасности. (Примеры приводятся для иллюстрации. Некоторые системы показаны в одной колонке, хотя фактически они могут быть также отнесены к другой колонке, например, КИПиУ помещения щита управления.)

2.43. Следует обеспечивать, чтобы классификация необходимых сервисных систем (электрических, пневматических или гидравлических источников энергоснабжения, систем смазки) соответствовала классификации функций безопасности, которые они поддерживают.

2.44. В случае всех систем КИПиУ и оборудования, выполняющих функции, важные для безопасности, между системами и оборудованием различных классов следует предусматривать соответствующим образом спроектированные границы раздела для обеспечения того, чтобы любой отказ в системе, относящейся к более низкому классу, не распространялся на систему более высокого класса. Оборудование, выполняющее функцию предотвращения распространения отказа, следует относить к более высокому классу.

2.45. Проектирование, конструирование и техническое обслуживание всех систем КИПиУ и оборудования следует осуществлять с таким расчетом, чтобы технические данные, результаты верификации и валидации, обеспечения качества, контроля качества и надежность этих систем и оборудования соответствовали их классификации.

3. ПРОЕКТНЫЕ ОСНОВЫ

3.1. В проектных основах станции определяются необходимые потенциальные возможности станции функционировать в определенном диапазоне эксплуатационных состояний и условий проектных аварий в соответствии с установленными требованиями радиационной защиты. Проектные основы, как правило, включают спецификацию для нормальной эксплуатации, условия, возникающие в результате ПИС, важные допущения и в некоторых случаях конкретные методы анализа.

3.2. Следует также учитывать функционирование станции в случае некоторых событий, для которых проект станции не рассчитан, т.е. в условиях запроектных (или тяжелых) аварий. Системы КИПиУ, важные для безопасности, играют важную роль в таких случаях, так как может потребоваться, чтобы они обеспечивали получение критической информации о состоянии станции или работали за пределами проектных диапазонов механических систем станции.

3.3. Требования к проектированию определяют деятельность, которая влияет на проектные основы систем КИПиУ, важных для безопасности. Эта

деятельность рассматривается ниже. (Руководящие материалы, имеющие отношение к этим требованиям, предъявляемым к проектированию систем КИПиУ, приведены в разделах 4, 5 и 6 настоящего Руководства по безопасности.)

КАТЕГОРИИ СОСТОЯНИЙ СТАНЦИИ

3.4. В Требованиях к проектированию содержится требование о том, что состояния станции должны быть определены и включены в ограниченное число категорий в соответствии с вероятностью их возникновения (см. [1], пункт 5.7). Эти категории обычно охватывают нормальную эксплуатацию, ожидаемые при эксплуатации события, проектные аварии и тяжелые аварии.

Эксплуатационные состояния

3.5. Согласно Требованиям к проектированию (см. [1], пункт 5.25) при проектировании должна учитываться потенциальная возможность возникновения аварий в режиме работы на малой мощности или в состоянии останова, например при пуске, перегрузке топлива и проведении работ по техническому обслуживанию, когда готовность некоторых систем безопасности КИПиУ может быть пониженной, и должны быть определены соответствующие ограничения в отношении неготовности систем безопасности КИПиУ (см. разделы 4 и 5).

3.6. При проектировании следует рассматривать безопасную нормальную эксплуатацию атомной электростанции, охватывающую все штатные режимы эксплуатации. В процессе проектирования следует определять набор требований и ограничений для нормальной эксплуатации системы КИПиУ, которые необходимы для безопасной эксплуатации станции. В эти требования следует включать (см. [1], пункт 5.26):

— информацию, необходимую для определения уставок систем безопасности;
— ограничения систем управления и процедурного характера, действующие в отношении параметров процесса и других важных параметров;
— требования в отношении проведения работ по техническому обслуживанию, испытаний и инспекций на станции с целью обеспечения уверенности в том, что конструкции, системы и элементы функционируют как предусмотрено; и

— четко определенные эксплуатационные конфигурации, в том числе эксплутационные ограничения в случае отключений системы безопасности.

3.7. Эти требования и ограничения служат основой для установления эксплуатационных пределов и условий, согласно которым разрешается эксплуатировать станцию.

Постулируемые исходные события

3.8. Согласно Требованиям к проектированию должно быть признано при проектировании станции, что на всех уровнях глубокоэшелонированной защиты могут возникать проблемы, и должны предусматриваться проектные меры, обеспечивающие выполнение необходимых функций безопасности и достижение целей безопасности (см. [1], пункт 5.8). Системы КИПиУ предусматриваются для определения начала развития проблемы в случае ПИС и инициирования действий, необходимых для обеспечения выполнения заданных функций безопасности и, таким образом, исключения превышения пределов, определенных в проектных основах.

3.9. С целью определения соответствующих возможностей систем КИПиУ по обнаружению ситуаций, обработке информации и инициированию действий, необходимых для выполнения функций безопасности, в проектные основы станции следует включать определенный список ПИС. В этом списке следует учитывать место расположения станции, прогнозируемую частоту появления событий и последствия, возникающие в результате отсутствия защитных действий.

3.10. В анализе безопасности станции эти ПИС рассматриваются индивидуально. Кроме того, исходное событие вследствие своего характера может приводить к каскадной цепи происшествий или отказов. Любые такие последующие происшествия или отказы, рассматриваемые в анализе безопасности станции, следует включать в проектные основы. Для последствий ПИС следует устанавливать приемлемые пределы.

3.11. Эти ПИС и приемлемые пределы их последствий образуют основы вводимых параметров в анализе безопасности, которые, в свою очередь, определяют в количественном выражении общие требования в отношении рабочих характеристик систем, которые требуются для выполнения задачи обеспечения безопасности.

3.12. Эти требования в отношении рабочих характеристик затем применяются к соответствующим системам КИПиУ, важным для безопасности. В настоящем Руководстве по безопасности такой анализ безопасности конкретно не рассматривается и не дается информация о средствах оценки адекватности полученных требований, предъявляемых к рабочим характеристикам. Однако здесь определяются входные данные, необходимые для последующего проектирования системы защиты. Ниже приводится типичная последовательность проведения указанного анализа безопасности, который может неоднократно повторяться в процессе разработки проекта:

— определение ПИС применительно к каждому режиму эксплуатации станции и оценка частоты их возникновения;
— определение приемлемых пределов для каждого такого события;
— выбор пределов условий на станции с целью исключения с достаточным запасом превышения приемлемых пределов, установленных для последствий ПИС (см. раздел 5 документа [1]);
— определение требующихся задач обеспечения безопасности в целях поддержания условий на станции в рамках этих приемлемых пределов, а также определение требующейся целостности процесса выполнения этих задач; и
— определение с учетом физической конфигурации станции диапазонов условий окружающей среды, в которых должны работать элементы системы защиты; они включают условия, которые могут привести к функциональной деградации элементов системы защиты и в отношении которых должны быть предусмотрены такие средства, как физические барьеры, с целью сохранения способности элементов системы защиты выполнять требующиеся задачи обеспечения безопасности.

Проектные основы для проектных аварий

3.13. Согласно Требованиям к проектированию в случаях, когда в ответ на ПИС требуется принимать оперативные и надежные действия, должно предусматриваться автоматическое срабатывание требующейся системы безопасности с целью предотвращения развития ситуации в более тяжелую стадию, которая может представлять угрозу для следующего барьера. Руководящие материалы по проектированию, касающиеся автоматического срабатывания систем защиты, приводятся в разделе 5.

3.14. В Требованиях к проектированию указано, что, если оперативные действия не требуются, то может разрешаться ручное включение систем или выполнение оператором других действий при условии, что необходимость

осуществления действий будет выявляться достаточно заблаговременно и будут определены надлежащие процедуры для обеспечения надежности таких действий. Руководящие материалы по проектированию, касающиеся взаимодействия человек-машина для обеспечения оператора надлежащей достоверной информацией, приводятся в разделе 6.

Проектные основы для запроектных аварий

3.15. В анализе безопасности рассматривается возможность возникновения тяжелых аварий, в случае которых некоторые весьма маловероятные события могут угрожать целостности многих или всех барьеров, препятствующих выбросу радиоактивных материалов. Анализ безопасности определяет последовательности развития тяжелых аварий, для которых могут устанавливаться разумно осуществимые на практике профилактические или смягчающие последствия меры. Стратегии и процедуры управления авариями разрабатываются для таких условий в соответствии с разделом 5 документа [1].

Проектные требования для систем КИПиУ

3.16. Проектные основы для систем КИПиУ, важных для безопасности, следует разрабатывать на основе проектных основ станции с целью оформления документации для соответствующих систем и характеристик. Проектные основы для систем КИПиУ следует документировать согласно руководящим материалам, содержащимся в разделе 7 настоящего Руководства по безопасности. При проектировании систем КИПиУ следует учитывать требования, предъявляемые к рабочим характеристикам, к готовности системы и условиям окружающей среды (в том числе условиям, возникающим во время и после аварии), в которых системы КИПиУ должны функционировать.

3.17. Функциональные требования и требования к рабочим характеристикам систем КИПиУ следует устанавливать в соответствии с требованиями эксплуатирующей организации, возможностями персонала станции, требованиями безопасности и результатами анализа безопасности атомной электростанции. Следует определять требования к рабочим характеристикам, таким, как диапазон измеряемого параметра, точность, время реакции, ширина полосы и уровни выходного сигнала. При проектировании связанных с обеспечением безопасности систем КИПиУ следует принимать во внимание воздействие кратковременных и нормальных изменений характеристик источника питания, таких, как колебания напряжения и частоты и перепады давления воздуха в приборах, в той мере, в какой это необходимо для

обеспечения того, чтобы системы КИПиУ надлежащим образом выполняли заданные им функции безопасности.

3.18. Согласно Требованиям по проектированию для эксплуатационных состояний и проектных аварий должен конкретно определяться набор проектных пределов, соответствующих основным физическим параметрам каждой конструкции, системы или элемента. В случае систем КИПиУ, важных для безопасности, в их число следует включать спецификацию условий окружающей среды, которые система должна будет выдерживать, и ожидаемую продолжительность эксплуатации в таких условиях, во время эксплуатационных состояний и в условиях проектных аварий. Следует учитывать условия окружающей среды, такие, как максимальные и минимальные значения температуры, давления, влажности, интенсивности ионизирующих излучений, электромагнитных помех, колебаний напряжения источника питания, вибрации, коррозии, усталости и напряжения.

4. ОБЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ

4.1. Для систем КИПиУ, важных для безопасности, определен ряд ключевых атрибутов или существенно важных аспектов. Ниже приводятся общие руководящие принципы, касающиеся этих атрибутов. Применительно к каждому атрибуту приводится обоснование руководящих принципов, служащее в качестве своевременного напоминания разработчикам проекта о вопросах или факторах, в связи с которыми были разработаны атрибуты. После каждого рассмотрения обоснования руководящие принципы группируются и представляются на основе классификации систем по важности для безопасности (см. раздел 2) в двух уровнях. Первый уровень включает руководящие принципы, предназначенные для всех систем, важных для безопасности. Они применяются одинаково ко всем системам в независимости от того, являются ли они системами безопасности или связанными с обеспечением безопасности системами. Руководящие принципы второго уровня применяются к системам безопасности и дополняют первый уровень. Несмотря на то, что для каждого атрибута предусмотрено два возможных уровня руководящих принципов, в некоторых случаях руководящие принципы не могут быть определены как применимые только к системам безопасности, либо к связанным с обеспечением безопасности системам. Применимость руководящих принципов к этим двум классам систем оговаривается в тексте пояснения и иллюстрируется таблицей I.

ТАБЛИЦА I. ПРИМЕНЕНИЕ ПУНКТОВ РАЗДЕЛА 4 К СВЯЗАННЫМ С ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ СИСТЕМАМ ИЛИ СИСТЕМАМ БЕЗОПАСНОСТИ

Пункты	Тема	Применение	
		Связанные с обеспечением безопасности системы	Системы безопасности
4.1–4.2	Общие принципы проектирования	да	да
4.3–4.7	Требования к рабочим характеристикам	да	да
4.8–4.13	Обеспечение надежности при проектировании	да	да
4.14	Обеспечение надежности при проектировании	нет	да
4.15	Критерий единичного отказа	да	да
4.16	Критерий	да	да
4.17–4.21	Применение критерия единичного отказа к системам КИПиУ, важным для безопасности	да	да
4.22	Резервирование	да	да
4.23–4.30	Неодинаковость	да	да
4.31	Неодинаковость	нет	да
4.32–4.34	Оценка надежности	да	да
4.35	Надежность программного обеспечения	да	да
4.36–4.48	Независимость	да	да
4.49–4.50	Виды отказов	да	да
4.51–4.53	Контроль доступа к оборудованию	да	да
4.54–4.60	Уставки	да	да
4.61	Взаимодействие человек-машина	да	да
4.62–4.65	Аттестация оборудования	да	да
4.66–4.69	Программа аттестации оборудования	да	да
4.70	Программа аттестации оборудования	нет	да
4.71–4.73	Методы аттестации	да	да
4.74–4.76	Качество	да	да
4.77–4.78	Обеспечение электромагнитной совместимости при проектировании	да	да

ТАБЛИЦА I. ПРИМЕНЕНИЕ ПУНКТОВ РАЗДЕЛА 4 К СВЯЗАННЫМ С ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ СИСТЕМАМ ИЛИ СИСТЕМАМ БЕЗОПАСНОСТИ (продолж.)

Пункты	Тема	Применение	
		Связанные с обеспечением безопасности системы	Системы безопасности
4.79–4.80	Испытания и возможность проведения испытаний	да	да
4.81–4.83	Программа испытаний	да	да
4.84–4.85	Обеспечение испытаний	да	да
4.86–4.87	Обеспечение испытаний	нет	да
4.88–4.89	Обнаружение неисправностей	да	да
4.90	Обнаружение неисправностей	нет	да
4.91–4.92	Демонстрация работы систем	нет	да
4.93	Вывод из работы	да	да
4.94–4.95	Вывод из работы	нет	да
4.96	Контроль за испытаниями и их проведение	нет	да
4.97–4.103	Возможность проведения технического обслуживания	да	да
4.104–4.106	Документация	да	да
4.107–4.108	Определение узлов, важных для безопасности	да	да

4.2. Детальные дополнительные руководящие материалы, предназначенные специально для проектирования некоторых отдельных систем, приводятся в разделе 5. Руководящие материалы раздела 4 и конкретизированные руководящие материалы, изложенные в разделе 5, вместе составляют общий набор руководящих материалов, предназначенных для применения в случае этих отдельных систем.

ТРЕБОВАНИЯ К РАБОЧИМ ХАРАКТЕРИСТИКАМ

4.3. Требования к рабочим характеристикам определяют действия КИПиУ, которые должны выполняться, и основные технические характеристики. Эти требования включают диапазон измеряемых параметров, которые будут использованы, а также точность, время реакции, ширину полосы и уровни выходного сигнала.

4.4. Необходимые требования к рабочим характеристикам и цели надежности как систем КИПиУ, важных для безопасности, так и их вспомогательных средств устанавливаются посредством анализа безопасности, проводимого для конкретной станции, и указываются в проектных основах станции.

4.5. Следует обеспечивать, чтобы системы КИПиУ, важные для безопасности, выполняли функции, указанные в анализе безопасности станции, и чтобы их технические характеристики соответствовали допущениям, принимаемым в анализе безопасности, и проектным требованиям.

4.6. Если система КИПиУ, важная для безопасности, должна работать в определенном диапазоне условий окружающей среды (см. пункты 4.62–4.65), эту систему следует проектировать таким образом, чтобы она соответствовала всем требованиям при воздействии условий в пределах данного диапазона.

4.7. Если оборудование системы используется для различных функций, технические задания в отношении этого оборудования (например, точность и время реакции) следует выбирать такими, чтобы требования для всех этих функций выполнялись.

ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ПРИ ПРОЕКТИРОВАНИИ

4.8. Надежность является важным атрибутом систем, важных для безопасности. В Требованиях к проектированию содержится требование, чтобы все конструкции, системы и элементы, которые являются узлами, важными для безопасности, проектировались таким образом, чтобы их качество и надежность соответствовали их классификации. В частности, надежные системы КИПиУ, важные для безопасности, необходимы для предотвращения появления излишних проблем, связанных с целостностью физических барьеров, и для обеспечения надежности инженерных устройств защиты. В отношении систем защиты пункт 6.81 в [1] содержит конкретное требование в отношении проектирования с обеспечением высокой функциональной надежности.

4.9. В целях обеспечения выполнения требований по надежности, включенных в проектные основы систем КИПиУ, важных для безопасности, следует, как правило, применять соответствующую комбинацию вероятностных и детерминированных критериев проектирования. Для связанных с аппаратными средствами отказов систем следует, как правило, определять количественные показатели надежности. При проектировании систем КИПиУ,

важных для безопасности, при необходимости следует рассматривать такие проектные характеристики, как устойчивость к случайным отказам, устойчивость к отказам по общей причине, отказобезопасность конструкции, независимость оборудования и систем, подбор высококачественного оборудования, возможность проведения испытаний и возможность проведения технического обслуживания.

4.10. На практике для оптимизации таких целей, как сведение к минимуму времени простоя на ремонт и уменьшение частоты испытаний, может потребоваться принятие в определенной степени компромиссных решений в отношении некоторых из этих факторов. Независимо от того, каким образом оптимизирована система КИПиУ, следует обеспечивать, чтобы она удовлетворяла требованиям в отношении надежности.

4.11. Чем выше надежность отдельных компонентов системы КИПиУ, тем выше надежность всей этой системы. Существуют, однако, практические пределы уровня надежности отдельных компонентов. Высокая надежность достигается за счет применения принципов резервирования или неодинаковости. Например, может оказаться возможным контролировать мощность реактора с помощью нескольких каналов или путем применения неодинаковых средств, таких, как измерение потока нейтронов или температуры и расхода или давления жидкости. Применение резервирования обеспечивает защиту от случайных отказов. Использование принципа неодинаковости обеспечивает защиту от определенных отказов по общей причине.

4.12. Надежность, требующаяся для каждой системы, зависит от важности для безопасности функций системы, и ее следует, как правило, указывать в проектных основах. Чем важнее для безопасности система КИПиУ, тем выше надежность следует обеспечивать. Один из подходов, используемых для определения требующейся надежности, сводится к присвоению числового показателю надежности каждому классу, упомянутому в разделе 2. Другой подход состоит в определении критериев детерминированного проектирования для различных классов на основе инженерного опыта путем присвоения системам классов, а затем установления набора требований, применяемых к каждому классу. Все системы одного класса затем сравниваются с типовыми системами. В большинстве случаев применяется определенное сочетание детерминированных и вероятностных критериев.

4.13. В некоторых государствах-членах используются прямые требования надежности. В других государствах-членах надежность является лишь одним из

аспектов подтверждения рабочих характеристик, требующихся для систем безопасности и соответствующего оборудования. В практике государств устанавливаются цели обеспечения рабочих характеристик системы защиты, которые превышают требование применения критерия единичного отказа. Такое повышение надежности иногда достигается благодаря использованию двойной защиты от отказов в некоторых секциях системы защиты и/или за счет использования оборудования с повышенным проектным запасом.

4.14. Следует обеспечивать, чтобы конструкция систем безопасности удовлетворяла критерию единичного отказа, а также следует учитывать возможность отказов по общей причине. В некоторых случаях могут применяться минимальные требования по резервированию, ниже которых эксплуатация не будут разрешаться. При проектировании систем безопасности следует тщательно определять и изучать потенциальные причины отказов с целью определения целесообразности применения принципа неодинаковости на данном участке системы.

Критерий единичного отказа

4.15. Критерий единичного отказа представляет собой детерминированный подход к обеспечению минимального резервирования системы или группы составных частей оборудования. Он базируется на общем опыте, который свидетельствует о том, что даже в случае элементов и оборудования, которые изготовлены в соответствии с высокими стандартами качества, иногда могут происходить отказы, которые до некоторой степени и иногда носят случайный и непредсказуемый характер. Если система проектируется так, что связанные с безопасностью функции этой системы обеспечиваются несмотря на возникновение такого случайного отказа компонента, уровень ее надежности будет повышенным.

Критерий

4.16. Согласно Требованиям к проектированию соблюдение критерия должно считаться достигнутым, если было доказано, что каждая группа безопасности будет выполнять свои функции безопасности при соблюдении следующих условий (см. [1], пункт 5.37):

— допускается, что могут иметь место любые потенциально вредные последствия ПИС для группы безопасности; и
— допускается наличие наихудшей допустимой конфигурации систем безопасности, выполняющих требующуюся функцию безопасности, с

учетом проведения работ по техническому обслуживанию, проверок, испытаний, инспекций и ремонта, а также допустимых периодов отключения оборудования.

При применении данной концепции ложное срабатывание следует рассматривать как один из видов отказа. Никогда не предполагается, что происходит более чем один отказ.

Применение критерия единичного отказа к системам КИПиУ, важным для безопасности

4.17. Согласно определению критерия единичного отказа, данному в Требованиях к проектированию, этот критерий должен применяться к каждой группе безопасности, включаемой в проект станции. «Группа безопасности» определяется как набор оборудования (часто называемый «цепью»), который выполняет все необходимые действий после возникновения ПИС с целью предотвращения превышения пределов, установленных в проектных основах для этого события (см. [1], пункт 5.34).

4.18. Для систем КИПиУ, к которым применяется критерий, следует сначала определять предписанные функции безопасности систем, а также группу безопасности, которая должна выполнять эти функции. Следует обеспечивать, чтобы это определение также включало все другие системы, связанные с системой КИПиУ, отказ которой может повлиять на выполнение определенных функций безопасности системы. После определения соответствующей группы безопасности следует выполнять указанный ниже анализ:

— в проектных основах следует определять ПИС, которые соответствуют предписанным функциям безопасности. Следует определять вероятность развития ПИС. Если эти события считаются вероятными, то следует определять последствия этих ПИС;
— следует определять функции безопасности, системы безопасности и вспомогательные средства, которые требуются в случае возникновения ПИС (такие, как ввод регулирующих стержней или закрытие отсечных клапанов защитной оболочки). В их число следует включать альтернативные «пути достижения успеха», посредством которых можно добиться выполнения функций безопасности;
— следует принимать допущение относительно единичного отказа в системе и определять последствия единичного отказа;
— следует подтверждать, что функции безопасности могут выполняться;

— при определении последствий следует проверять выполнение требований по обеспечению независимости в группах безопасности (см. [1], пункт II.11). В этот процесс следует включать проверку того, чтобы, насколько это практически возможно, группы безопасности не имели никакого совместно используемого оборудования или точек уязвимости;
— если устанавливается, что системы независимого резервирования и цепи необходимых систем являются защищенными от единичного отказа, то для этих систем не требуется далее проводить детальный анализ для определения потенциальных отказов согласно критерию единичного отказа;
— если в исключительных случаях критерий единичного отказа не может быть применен, то в проект вносятся изменения для обеспечения соблюдения критерия, или же при наличии обоснования принимается соответствующее исключение. Затем следует обеспечить, чтобы надежность систем поддерживалась на очень высоком уровне путем проведения надлежащих инспекций в процессе эксплуатации, технического обслуживания и применения эксплуатационных процедур (регламентов) таким образом, чтобы их отказ в процессе эксплуатации стал невозможным;
— если единичный отказ может препятствовать достижению достаточного уровня надежности системы безопасности, то следует обеспечивать наличие других систем в целях предотвращения неприемлемых последствий;
— при применении критерия единичного отказа принимается косвенное допущение относительно возможности обнаружения отказов. Однако могут возникать отказы, которые невозможно обнаружить путем испытаний, в результате срабатывания сигнализации или индикации нештатных режимов. Системы следует анализировать на предмет выявления таких необнаруживаемых отказов. Предпочтительным подходом в этом случае является изменение конструкции системы или методов испытаний для того, чтобы обеспечить возможность обнаружения отказов. Если это не представляется возможным, то следует принять допущение, что такие необнаруженные отказы произошли, а затем, кроме того, следует принять допущение относительно единичного отказа. Следует обеспечивать, чтобы в таких условиях могли выполняться функции безопасности;
— следует определять действия оператора, которые предписывается выполнять в случае конкретных последовательностей событий. Следует выполнить анализ связанных с этим последствий неправильного выполнения или невыполнения отдельных случайно выбранных предписываемых действий, которые должен предпринимать оператор.

Следует обеспечивать, чтобы в таких условиях выполнялись функции безопасности;

— в некоторых государствах-членах критерий единичного отказа не применяется, когда одна из резервных цепей выводится из эксплуатации вследствие проведения испытаний или работ по техническому обслуживанию. Для таких случаев следует определять допустимые периоды вывода из эксплуатации, которые обеспечивают требующуюся надежность;
— отказы по общей причине обычно не включаются в анализ. Вероятные отказы по общей причине следует оценивать отдельно детерминированными методами или с помощью метода вероятностного анализа безопасности, или же путем применения сочетания этих методов. Следует предусматривать достаточную независимость и неодинаковость в целях обеспечения разумной уверенности в том, что функции безопасности могут выполняться в случае отказов по общей причине.

4.19. Хотя определенные элементы систем КИПиУ (кабели, печатные платы или корпусы) можно рассматривать в качестве пассивных элементов, в редких случаях необходимо или возможно эффективно использовать это обстоятельство для облегчения анализа единичных отказов.

4.20. Несоблюдение критерия единичного отказа может быть обосновано для:

— очень редких ПИС;
— весьма маловероятных последствий ПИС;
— случаев вывода из эксплуатации определенных элементов для целей проведения технического обслуживания, ремонта или периодических испытаний в течение ограниченных периодов времени;
— средств предотвращения или смягчения последствий тяжелых аварий; и
— элементов, вероятность отказа которых можно определить как достаточно низкую, чтобы ею можно было пренебречь.

4.21. Дополнительные руководящие материалы по применению критерия единичного отказа и стратегиям обеспечения соблюдения этого критерия приводятся в [5].

Резервирование

4.22. Резервирование обычно используется в системах КИПиУ, важных для безопасности, для достижения целей надежности системы и/или обеспечения соблюдения критерия единичного отказа. Чтобы резервирование было

полностью эффективным, следует обеспечивать независимость систем (см. пункты 4.36–4.48). Резервирование, взятое в отдельности, повышает надежность действий по обеспечению безопасности или связанных с обеспечением безопасности действий, но оно также увеличивает и вероятность ложного срабатывания. Для получения правильного соотношения между надежностью и исключением ложного срабатывания обычно используется метод совпадения сигналов от резервного оборудования или схемы отклонения ложных сигналов, работа которых основана на взаимном сравнении сигналов от резервного оборудования.

Неодинаковость

4.23. Неодинаковость в системах КИПиУ – это принцип контроля различных параметров с использованием разных технологий, разных логических схем или алгоритмов, или же разных исполнительных устройств с тем, чтобы обеспечить возможность обнаруживать значительное событие и реагировать на него несколькими разными способами. Неодинаковость обеспечивает защиту от отказов по общей причине, дополняет принцип глубокоэшелонированной защиты и повышает вероятность выполнения задачи обеспечения безопасности, когда это необходимо. Способы защиты на разных уровнях ее глубины также могут быть неодинаковыми и отличаться друг от друга. Принцип неодинаковости, применение которого может рассматриваться, включает неодинаковость разного типа: неодинаковость операторов, неодинаковость конструкции, неодинаковость программного обеспечения, функциональную неодинаковость, неодинаковость сигналов, неодинаковость оборудования и неодинаковость систем.

4.24. Следует предусматривать дополнительный уровень консерватизма в тех случаях, когда получение требующегося подтверждения надежности системы не представляется возможным, например, когда надежность нескольких резервных систем ограничивается такими факторами, как отказы по общей причине или неопределенности при проектировании. Например, особые трудности могут возникнуть при подтверждении надежности компьютерных систем. Неодинаковость – это способ применения консерватизма для компенсации сложности подтверждения требуемого уровня надежности.

4.25. Адекватность неодинаковости, обеспечиваемой в связи с упомянутыми выше критериями, следует обосновывать. Следует рассматривать масштаб применения и тип неодинаковости. Обеспечение желательного уровня консерватизма может не требовать расширения масштаба применения принципа неодинаковости с целью охвата весьма маловероятных ПИС или ПИС

с малыми последствиями, так как риск возникновения таких событий может быть приемлемым несмотря на возможность отказа по общей причине.

4.26. Как правило, применяется неодинаковость разных типов. Особенно эффективным может быть сочетание функциональной неодинаковости (системы, обеспечивающие различные физические функции, которые перекрывают друг друга в своем воздействии на безопасность) и неодинаковости сигналов (использование различных контролируемых параметров для инициирования защитного действия).

4.27. В любом случае следует уделять внимание обеспечению того, чтобы неодинаковость реально достигалась в завершенном проекте и сохранялась в течение всего жизненного цикла станции. Разработчику проекта следует тщательно анализировать проект с целью исключения возможного появления признаков одинаковости при обеспечении неодинаковости применительно к таким компонентам, как материалы, элементы конструкции, аналогичные процессы изготовления, аналогичное программное обеспечение или неявное сходство в принципах работы или общих вспомогательных средствах.

4.28. Следует обеспечивать, чтобы обоснование неодинаковости оборудования или неодинаковости программного обеспечения систем КИПиУ, таких, как операционная система, работающая в режиме реального времени, охватывала элементы оборудования для обеспечения реального наличия неодинаковости. Например, различные изготовители могут использовать одинаковые процессоры или производить по лицензии одинаковые операционные системы, что является потенциальным источником общих отказов. Подтверждение неодинаковости, основанное только на различии в названиях изготовителей, является недостаточным без учета этой возможности.

4.29. Что касается неодинаковости программного обеспечения, то опыт показывает, что независимость видов отказов не может быть достигнута, если несколько версий программного обеспечения были разработаны в соответствии с одной и той же спецификацией требований к программному обеспечению. В частности, возможно, что независимо разработанные версии программ могут быть подвержены отказам по общей причине. Использование таких типов неодинаковости, как функциональная неодинаковость и неодинаковость сигналов, может быть наиболее эффективным способом преодоления этого ограничения.

4.30. Для обеспечения дополнительного повышения надежности сверх уровня, достигаемого только за счет соблюдения критерия единичного отказа,

используется метод расширенного применения таких принципов, как резервирование, неодинаковость, использование апробированного оборудования, обеспечение возможности проведения испытаний, непрерывный мониторинг и обеспечение возможности проведения технического обслуживания.

4.31. В некоторых государствах-членах в дополнение к критерию единичного отказа к системе защиты применяются требования надежности. Такое повышение надежности иногда достигается благодаря использованию двойной защиты от отказов в некоторых секциях системы защиты и/или за счет использования оборудования с повышенным проектным запасом. В некоторых государствах-членах устанавливается общая цель надежности в числовом выражении, и для проверки выполнения этой цели системой защиты используются аналитические методы и испытания.

Оценка надежности

4.32. Для всех систем, важных для безопасности, такие компоненты, как степень резервирования, неодинаковость, возможность проведения испытаний и устойчивость, следует обосновывать с точки зрения их адекватности для обеспечения требующейся надежности функций безопасности, выполняемых системами. Такое подтверждение может быть основано на сочетании детерминированных критериев и количественного анализа надежности.

4.33. При оценке надежности цифровых систем КИПиУ следует рассматривать последствия возможных отказов аппаратных средств и программного обеспечения, а также применения проектных решений, предназначенных для предотвращения или ограничения этих последствий. В рассматриваемые условия отказов аппаратных средств следует включать отказы частей самого компьютера и отказов частей систем связи. Следует учитывать как устойчивые отказы, так и переходные отказы.

4.34. Вклад отказа компонента в неготовность системы КИПиУ следует определять до соответствующей степени уверенности, например, посредством определения доверительного уровня при использовании вероятностного подхода.

Надежность программного обеспечения

4.35. Неисправности программного обеспечения – это систематические неисправности, вызываемые ошибками проектирования, и поэтому в анализе

надежности аппаратных средств относительно них не принимается допущение о случайном характере возникновения отказов. Следовательно, для оценки ненадежности, вносимой аппаратными средствами и программным обеспечением, могут потребоваться различные методы. Например, надежность компьютерных систем можно подтверждать посредством проведения качественной оценки, учитывающей сложность проекта, качество верификации, валидации и испытаний процесса разработки в широком диапазоне вводимых условий, а также на основе накопленного эксплуатационного опыта.

НЕЗАВИСИМОСТЬ

4.36. Независимость позволяет предотвращать: 1) распространение отказов от системы к системе или 2) распространение отказов между резервными элементами в пределах систем и 3) отказы по общей причине из-за общих внутренних опасностей на станции. Независимость также важна для обеспечения эффективности принципов резервирования и неодинаковости, применяемых для достижения высокой надежности систем, важных для безопасности.

4.37. Применение принципа независимости следует рассматривать с целью предотвращения распространения отказов:

— между элементами системы вследствие возникновения ПИС;
— между системами, имеющими одинаковую важность для безопасности; и
— от систем более низкой важности к системам более высокой важности для безопасности.

4.38. Следует обеспечивать, чтобы системы безопасности не зависели от связанных с обеспечением безопасности систем и систем, не связанных с безопасностью. Системы более низкой важности для безопасности могут быть связаны с системой безопасности при условии, что между этими системами поддерживается независимость и что независимость резервных групп безопасности при этом не ухудшается.

4.39. Следует обеспечивать независимость друг от друга резервных групп безопасности систем КИПиУ, важных для безопасности.

4.40. Следует предусматривать независимость между резервными элементами связанных с обеспечением безопасности систем.

4.41. Соответствующую независимость следует предусматривать между неодинаковыми функциями. Следует обосновывать адекватность обеспечиваемой независимости.

4.42. Независимость достигается посредством электрической изоляции, физического разделения и независимости связи между системами.

4.43. Электрическая изоляция необходима для исключения или предотвращения нежелательного воздействия оборудования и элементов друг на друга, причинами которого являются электромагнитная индукция, скопление электростатического электричества, короткие замыкания, разрыв цепей, заземление, приложение максимально возможного напряжения (переменного или постоянного тока) и механическое взаимодействие. Примерами средств электрической изоляции являются устройства, в которых используется электрическая и оптическая развязка, экранирование кабелей, внутренние механические конструкции или аналогичные устройства. Если разъединительные устройства используются между системами различной важности для безопасности, следует обеспечивать, чтобы они были связаны с системой более высокой важности.

4.44. Следует обеспечивать, чтобы ни один вероятный отказ на не связанной с безопасностью стороне разъединительного устройства не препятствовал любой части системы безопасности выполнять минимальные требования, предъявляемые к рабочим характеристикам, во время и после любого ПИС, которое требует выполнения функции безопасности.

4.45. Физическое разделение систем друг от друга достигается за счет расстояния, с помощью барьеров или сочетания этих двух методов и может использоваться для уменьшения вероятности возникновения отказов по общей причине в результате отказов вследствие ПИС (таких, как пожары, летящие предметы, затопление или разрывы трубопроводов с большим выделением энергии). Такое физическое разделение дополнительно снижает вероятность случайных неправильных действий в процессе эксплуатации или технического обслуживания применительно к более чем одной части этих систем.

4.46. Выбор методов физического разделения дистанцированием, с помощью барьеров или сочетанием этих методов может быть различным и зависит от места расположения в конструкции атомной электростанции. Он будет зависеть от необходимости обеспечения защиты от всех учитываемых в проектных основах ПИС, включая воздействие пожаров, химические взрывы, падения

летательных аппаратов и летящие предметы. В [6–9] содержатся дополнительные руководящие материалы.

4.47. Определенные участки станции отличаются той особенностью, что они являются естественным скоплением резервного оборудования или проводок. Следует тщательно определять, в какой степени после определенных ПИС может быть потеряна независимость на этих участках, и полученные результаты использовать в качестве основы при разработке общего проекта, удовлетворяющего требованиям и целям в отношении надежности. К таким местам скопления относятся, например, проходки в защитной оболочке, пульты управления электродвигателями, помещения распределительных устройств, распределительные помещения кабелей, машинные залы, помещение щита управления и ЭВМ управления технологическими процессами станции.

4.48. Обеспечение независимости средств связи является необходимым только в случае конструкций, в которых используются системы передачи данных. Независимость связи достигается за счет подбора соответствующей архитектуры систем и протоколов передачи данных таким образом, чтобы неправильное срабатывание логической схемы или программного обеспечения в одной системе не могло отрицательно повлиять на связанные системы. Независимость связи обеспечивается посредством принятия адекватных мер для буферизации данных (в том числе применения аппаратной логика и/или логики программного обеспечения для поддержки коммутации данных, обнаружения и устранения ошибок в передаче, регулирования расхода или управлении передачей, или же для управления протоколами) таким образом, чтобы неисправности модулей передачи и приема данных не приводили к нарушению функционирования модулей обработки данных.

ВИДЫ ОТКАЗОВ

4.49. Одним из методов борьбы с ожидаемыми отказами систем или элементов является конструирование этих систем и элементов таким образом, чтобы возникающие отказы приводили к известным видам отказов. Следует обеспечивать, чтобы возникающие отказы сводились не только к прогнозируемым видам отказов, но также и к видам отказов, которые переводят систему в безопасное состояние. В требованиях к проектированию содержится требование, чтобы принцип отказобезопасного проектирования в надлежащих случаях учитывался и применялся при проектировании систем и элементов станции, важных для безопасности станции(см. [1], пункт 5.40).

4.50. В целях облегчения проектирования систем безопасности в целом следует обеспечивать, чтобы оборудование, насколько это практически возможно, характеризовалось прогнозируемым и известным видом отказов. Следует обеспечивать, чтобы более вероятные виды отказов в системе, важной для безопасности, насколько это практически возможно, переводили эту систему в безопасное состояние. Следует принимать во внимание использование таких средств обеспечения отказобезопасности, как «обесточивание для срабатывания» или «сторожевые таймеры» в конструкции систем КИПиУ (см. [1], пункт 5.40). Однако, если такая практика применяется, она не устраняет необходимость выполнения требований безопасности в отношении отказов, которые могут произойти в самих проектных средствах обеспечения отказобезопасности.

КОНТРОЛЬ ДОСТУПА К ОБОРУДОВАНИЮ

4.51. Доступ к оборудованию в системах, важных для безопасности, следует соответствующим образом ограничивать ввиду необходимости предотвращения как несанкционированного доступа, так и возможности совершения ошибок имеющим соответствующий доступ персоналом. Эффективные методы включают соответствующие сочетания мер физической безопасности (запираемые ограждения, запираемые помещения, сигнализация на панельных дверцах) и административных мер с учетом степени наблюдения за оборудованием в месте его расположения.

4.52. Особого внимания требуют два момента, связанных с контролем доступа, – это корректировки уставок и калибровок вследствие их важности с точки зрения предотвращения ухудшения работы систем из-за возможных ошибок при эксплуатации или проведении работ по техническому обслуживанию.

4.53. Для контроля доступа к цифровым компьютерным системам следует использовать средства, ограничивающие электронный доступ к программному обеспечению и данным. Эти ограничения следует применять в отношении доступа через сетевые связи и оборудование, используемое для ремонта и технического обслуживания.

УСТАВКИ

4.54. Атомная электростанция должна проектироваться с таким расчетом, чтобы обеспечивалась безопасная эксплуатация в определенном диапазоне

параметров таким образом, чтобы радиологическая опасность для населения и окружающей среды находилась в пределах нормативных пределов (см. [1], пункт 5.24). Состояние станции изменяется в ответ на исходные события, однако при этом режим станции может приблизиться к такому состоянию, которое выходит за пределы параметров безопасной эксплуатации. Происходит срабатывание определенных систем, важных для безопасности, которое инициирует действия, необходимые для возврата станции в безопасное состояние. Эти системы срабатывают при достижении контролируемым параметром заданной уставки.

4.55. Для конкретного контролируемого параметра (например, давления в первом контуре, давления в защитной оболочке) или расчетного параметра (например, мощности реактора, коэффициента критического теплового потока) на основе критериев безопасности устанавливается предел безопасности. В качестве такого предела следует применять значение параметра, при отклонении от которого можно ожидать возникновения неприемлемых последствий для безопасности (см. рис. 2).

4.56. Аналитический предел[1] – это теоретическая величина, полученная на основании результатов анализа безопасности. Анализом безопасности следует подтверждать, что после исходного события предел безопасности не будет достигаться, если смягчающее действие включается при подходе к аналитическому пределу. В этом анализе принимается допущение относительно конфигурации «как было спроектировано» для систем и оборудования и соответствующим образом постулированных отказов. Благодаря этому разность предела безопасности и аналитического предела будет компенсировать неопределенности в моделировании и возможные погрешности в поведении приборов, вызванные переходными процессами.

4.57. Номинальная уставка является значением, которое задается для функции аварийного срабатывания. Запас между номинальной уставкой и аналитическим пределом следует выбирать таким, чтобы смягчающее действие завершалось до достижения аналитического предела.

[1] Аналитический предел – это теоретическая величина, полученная на основании результатов анализа безопасности, при которой, если после исходного события включается смягчающее действие при подходе к аналитическому пределу, предел безопасности не достигается.

РИС. 2. Пример соотношений между уставками и пределами.

4.58. .«Допустимый предел» используется применительно к приборам, которые требуют проведения периодических испытаний и контроля. Запас между допустимым пределом и номинальной уставкой охватывает случайные неопределенности в калибровке приборов, случайные инструментальные погрешности и ошибки из-за дрейфа приборов. Если уставка выходит за границы допустимого предела, следует обеспечивать, чтобы включались срочные корректирующие действия.

4.59. Основы для номинальных уставок и допустимых пределов следует документировать и соответствующим образом обосновывать.

4.60. В некоторых случаях контролируемый параметр не идентичен параметру, используемому для определения предела безопасности. Примерами таких случаев являются:

— не поддающаяся контролю максимально допустимая температура оболочки твэлов после аварии с потерей теплоносителя. Вместо этого контролируется давление теплоносителя реактора, так как снижение давления может служить индикатором аварии, которая будет угрожать целостности твэлов;
— осевой поток нейтронов, температуры горячих и холодных ниток и давление в первом контуре, которые контролируются в реакторе, охлаждаемом водой под давлением, так как вместе они могут обеспечить индикацию кризиса пузырькового кипения – параметра, который не может быть измерен прямо.

ВЗАИМОДЕЙСТВИЕ ЧЕЛОВЕК-МАШИНА

4.61. Средства эффективного взаимодействия человека и машины для систем, важных для безопасности, необходимы для обеспечения оператора точной, полной и своевременной информацией о состоянии станции, а также для обеспечения надежного функционирования систем, которыми управляют системы КИПиУ. Согласно Требованиям к проектированию в процесс проектирования должен включаться систематический анализ человеческих факторов и взаимодействия человек-машина (см. [1], пункт 5.50). Следует обеспечивать, чтобы средства взаимодействия человек-машина для систем КИПиУ, важных для безопасности, соответствовали руководящим материалам, изложенным в разделе 6 настоящего Руководства по безопасности.

АТТЕСТАЦИЯ ОБОРУДОВАНИЯ

4.62. Следует обеспечивать, чтобы системы, важные для безопасности, были способны выполнять заданные им функциям безопасности, когда это требуется, при нормальной эксплуатации, внешних событиях и ожидаемых эксплуатационных условиях, а также в условиях проектных аварий и после них. Это имеет фундаментальное значение для предотвращения выбросов радиоактивных материалов, а также для предотвращения или смягчения радиологических последствий для здоровья человека и окружающей среды, если эти выбросы происходят.

4.63. Примерами опасных условий окружающей среды, являющихся результатом условий проектных аварий, которые могут приводить к отказу оборудования, являются радиационная обстановка и параметры пара, связанные с разрывами трубопроводов, включая разрывы в системе

теплоносителя реактора. Примеры режимов потенциально опасных процессов включают высокоскоростной двухфазный поток, высокие уровни вибрации или насыщенные обломками технологические жидкости. В дополнение к событиям, связанным с потенциально опасными процессами, следует учитывать такие эффекты, как перегрев, электромагнитные наводки, электростатические разряды и колебания параметров источника питания, которые также могут приводить к отказам по общей причине.

4.64. Согласно Требованиям к проектированию должна быть утверждена процедура аттестации для подтверждения того, что оборудование будет отвечать в течение установленных для них проектных сроков эксплуатации требованиям в отношении выполнения предписываемых им функций безопасности в случае необходимости в условиях воздействия внешней среды (вибрация, температура, давление, ударная сила струи, электромагнитные помехи, облучение, влажность или любое вероятное их сочетание) (см. [1], пункт 5.45). Аттестация представляет собой процесс определения опасностей в среде, в которой оборудование может эксплуатироваться, а также выполнения программы испытаний и/или анализа с целью определения и документального подтверждения способности оборудования удовлетворительно выполнять свою функцию безопасности в регламентированных рабочих условиях. Аттестация – это один из методов сведения к минимуму возможности того, что события или последствия, связанные с изменением условий окружающей среды, приведут к отказу оборудования по общей причине.

4.65. Следует обеспечивать, чтобы аттестация оборудования подтверждала способность оборудования функционировать в данных рабочих и окружающих условиях. В сочетании с другими руководящими материалами по аттестации, приведенными, например, в [10], следует применять указанные ниже рекомендации, касающиеся проектирования систем, важных для безопасности.

Программа аттестации оборудования

4.66. Следует обеспечивать выполнение аттестационной программы с целью подтверждения того, что оборудование, важное для безопасности, будет способно отвечать до конца своего проектного ресурса требованиям, предъявляемым к включенным в проектные основы рабочим характеристикам (таким, как диапазон, точность и время реакции) для осуществления предписываемой задачи обеспечения безопасности в данных условиях окружающей среды (таких, как температура, давление, облучение, влажность или едкие аэрозоли), когда это оборудование потребуется.

4.67. В эти условия окружающей среды следует включать ожидаемые сочетания условий при нормальной эксплуатации, во время ожидаемых при эксплуатации событий и в случае проектных аварий и после них. В программе аттестации оборудования не требуется учитывать условия тяжелой аварии. Однако следует подтверждать с достаточной степенью достоверности и в той мере, в какой это представляется возможным, что оборудование, предусматриваемое для реагирования на тяжелые аварии, будет функционировать в ожидаемых условиях тяжелой аварии (см. [1], пункт 5.46).

4.68. В тех случаях, когда оборудование подвергается воздействию таких внешних событий, как природные явления или другие внешние факторы, и должно выполнять задачу обеспечения безопасности во время такого события или после него, в аттестационную программу следует включать условия, налагаемые на оборудование воздействием этих внешних событий. В аттестационную программу следует включать, кроме того, любые необычные условия окружающей среды, которые могут быть обоснованно спрогнозированы и стать следствием конкретных условий эксплуатации, например, условий, которые могут возникнуть во время проведения периодических проверок скорости утечки из защитной оболочки.

4.69. В программу следует включать план, обеспечивающий аттестацию оборудования в течение предполагаемого периода его использования и при необходимости его своевременную переаттестацию или замену. Следует принимать во внимание комбинированное воздействие различных внешних факторов, а также суммарное воздействие факторов обычной окружающей среды в течение требуемого срока службы оборудования. В соответствующих случаях следует предусматривать дополнительный уровень консерватизма с целью учета непредвиденных механизмов старения. Следует предусматривать соответствующие меры для осуществления контроля, испытаний и проверок оборудования станции с целью определения непредвиденного поведения или ухудшения характеристик (см. [1], пункт 5.47).

4.70. При аттестации оборудования системы безопасности следует проверять пригодность предпочтительно всего комплекса оборудования, а не только тех частей, которые непосредственно связаны с данной задачей обеспечения безопасности.

Методы аттестации

4.71. Для осуществления целей, указанных выше, следует использовать соответствующие сочетания следующих методов аттестации:

— проведение испытаний типового оборудования, которое будет поставляться;
— проведение испытаний фактически поставляемого оборудования;
— использование соответствующего прошлого опыта применения аналогичного оборудования; и/или
— анализ, основанный на приемлемой технической экстраполяции результатов испытаний или опыта эксплуатации в сходных условиях.

4.72. Следует обеспечивать, чтобы выбранный метод аттестации позволял достигать степени уверенности, соответствующей важности оборудования для безопасности системы, как описано в разделе 2. Следует предусматривать испытания для проверки аттестации оборудования, и их следует проводить, когда это представляется практически возможным, в случае оборудования, обеспечивающего безопасность.

4.73. Когда для изолирования оборудования от возможных воздействий окружающей среды предусматриваются защитные барьеры, следует предусматривать аттестационную программу для этих барьеров с целью подтверждения их пригодности.

КАЧЕСТВО

4.74. Обеспечение высокого качества проектирования и изготовления необходимо для того, чтобы можно было подтвердить, что системы, важные для безопасности, удовлетворяют предъявляемым к ним требованиям безопасности. Проектирование и изготовление с обеспечением надлежащего уровня качества – это важные условия выполнения требований, изложенных в [1], пункт 5.1.

4.75. Следует обеспечивать, чтобы элементы и модули систем, важных для безопасности, имели качество, которое отвечает цели сведения к минимуму необходимости проведения технического обслуживания и интенсивности отказов.

4.76. Для систем, важных для безопасности, следует подбирать оборудование по возможности апробированной конструкции, которое соответствуют целям надежности, а также облегчает выполнение требований, предъявляемых к калибровке, испытаниям, техническому обслуживанию и ремонту. При подборе оборудования следует учитывать как возможность ложного срабатывания, так и

опасные отказы (например, отказ, препятствующий быстрой остановке в случае ее необходимости).

ОБЕСПЕЧЕНИЕ ЭЛЕКТРОМАГНИТНОЙ СОВМЕСТИМОСТИ ПРИ ПРОЕКТИРОВАНИИ

4.77. Оборудование и системы КИПиУ, включая соединительные кабели, следует проектировать и монтировать таким образом, чтобы они выдерживали электромагнитную обстановку на атомных электростанциях.

4.78. При проектировании следует предусматривать соответствующие средства обеспечения заземления, экранирования и развязки от помех. Следует применять соответствующие методы монтажа и технического обслуживания, обеспечивающие надлежащее использование этих средств при выполнении работ по монтажу и техническому обслуживанию. В [11] приводятся дополнительные руководящие материалы по заземлению. В [4] приводятся примеры типичных методов заземления и экранирования.

ИСПЫТАНИЯ И ВОЗМОЖНОСТЬ ПРОВЕДЕНИЯ ИСПЫТАНИЙ

4.79. Эксплуатационные испытания обеспечивают уверенность в том, что системы, важные для безопасности, остаются пригодными к эксплуатации и способными к выполнению предписанных им задач обеспечения безопасности. Частоту проведения испытаний следует устанавливать на основе требований, предъявляемых к готовности и надежности системы. Возможность проведения испытаний, т.е. возможность выполнения проверок системы, следует обеспечивать непосредственно в самом проекте. При проектировании доступной для испытаний системы следует уделять внимание: 1) правильному размещению оборудования, 2) обеспечению соответствующего доступа, 3) легкости обнаружения неисправностей в оборудовании и 4) возможности подтверждения сохранения способности функционировать таким образом, чтобы безопасность действующей станции не подвергалась опасности.

4.80. Возможность проведения испытаний – это необходимый элемент проектирования применительно как к обеспечению надежности систем, как указано в пунктах 5.32–5.42 Требований к проектированию, так и к проведению испытаний, инспекций и контроля во время эксплуатации, как это предписывается в пунктах 5.43–5.44 Требований к проектированию. Кроме того, следует обеспечивать, чтобы система защиты отвечала специальным

требованиям по надежности и возможности проведения испытаний, как указано в пунктах 6.81–6.84 Требований к проектированию.

Программа испытаний

4.81. При проектировании систем КИПиУ, важных для безопасности, следует определять программу испытаний и калибровок в соответствии с требованиями, предъявляемыми к их готовности.

4.82. Посредством этой программы испытаний следует обеспечивать сохранение функциональной способности систем и элементов, важных для безопасности. В нее следует включать периодическое подтверждение выполнения таких проектных требований, как требования, предъявляемые к точности, времени реакции и уставкам.

4.83. Следует обеспечивать, чтобы испытания систем КИПиУ, важных для безопасности, были, насколько это практически возможно, комплексными проверками (от датчиков до исполнительных механизмов), которые можно проводить на месте с минимальными усилиями. Допустимо, чтобы программы испытаний включали отчасти дублирующие друг друга испытания, которые все вместе позволяют провести проверку всего канала. Следует проводить проверку всех выходных функций, важных для безопасности, таких, как сигналы систем сигнализации, управляющие действия и срабатывание исполнительных устройств.

Обеспечение испытаний

4.84. Во все системы, важные для безопасности, следует включать средства, позволяющие проводить необходимые испытания, включая в соответствующих случаях встроенные испытательные устройства. Следует обеспечивать, чтобы они позволяли проводить проверки регулярно для обеспечения непрерывной правильной работы. В тех случаях, когда проверяемое оборудование не может быть размещено в безопасном месте, следует предусматривать средства, позволяющие проводить испытания дистанционно вне зоны повышенной опасности.

4.85. Если предусматриваются испытательные устройства, при проектировании следует обеспечивать, чтобы систему нельзя было случайно оставить в испытательном режиме. Когда для проведения периодических испытаний предусматриваются стационарные испытательные устройства, в интерфейсных устройствах применяется блокировка аппаратных средств для обеспечения

того, чтобы взаимодействие с испытательной системой было не возможным без специального ручного вмешательства.

4.86. Для систем безопасности идеальным методом испытаний является единичный тест без вывода из работы, проводимый для каждой функции, который должен охватывать все элементы от датчиков до исполнительных механизмов. Однако такие испытания не всегда практически осуществимы. В таких случаях следует предусматривать, чтобы программа испытаний объединяла испытания без вывода из работы (для эксплуатационных состояний, в которых функция безопасности требуется или может требоваться) и испытания с выводом из работы (для эксплуатационных состояний, в которых функция безопасности не требуется) в серии отчасти дублирующих друг друга этапов испытаний в той степени, в какой это необходимо для достижения целей испытаний. Следует подтверждать приемлемость использования отчасти дублирующих друг друга этапов испытаний.

4.87. Проект систем безопасности и условия их испытаний следует предусматривать такими, чтобы они обеспечивали безопасность станции во время фактических испытаний и в идеальном случае сводили к минимуму возможность ложного инициирования любого действия по обеспечению безопасности и любого другого отрицательного воздействия испытаний на степень готовности станции. Следует обеспечивать, чтобы осуществление программы испытаний не приводило к ухудшению состояния какого-либо элемента станции сверх уровня, предусмотренного проектом.

Обнаружение неисправностей

4.88. Следует обеспечивать, чтобы проведение периодических испытаний позволяло получить объективную информацию о состоянии систем и – в соответствующих случаях – данные о тенденциях, с тем оказать помощь в обнаружении ухудшения состояния системы, а также тех условий, которые указывают на начальные признаки отказа в системе. Насколько это практически возможно, при проектировании систем, важных для безопасности, следует применять средства самопроверки. Средства самопроверки, однако, следует применять сбалансировано с учетом обеспечения требующейся простоты.

4.89. Насколько это практически осуществимо, для каждого датчика измеряемых параметров следует предусматривать отдельные испытания, например, путем:

— возмущения контролируемого параметра;

— подведения к датчику и соответствующего изменения заменяющего входного сигнала того же рода, что и измеряемый параметр; или
— перекрестной (взаимной) проверки параметров, которые связаны известной зависимостью между собой и для которых имеются показания.

4.90. Следует обеспечивать, чтобы требующиеся испытания позволяли обнаруживать неисправности в системах безопасности во всей цепи от датчиков до исполнительных механизмов. Следует предусматривать испытания, которые будут обеспечивать обнаружение неисправностей в каждом резервном элементе этих систем. Если в канале предусматривается резервное оборудование, следует обеспечивать, чтобы испытания позволяли проводить проверку эксплутационной готовности каждого резервного элемента.

Подтверждение рабочих характеристик систем

4.91. Периодические испытания и средства обеспечения калибровки следует выбирать с таким расчетом, чтобы можно было подтвердить рабочие характеристики, определенные в проектных основах для резервных каналов в системе защиты, системах обслуживания устройств безопасности и вспомогательных устройствах систем безопасности. Испытания и калибровки следует, как правило, проводить с разной периодичностью.

4.92. В тех случаях, когда для формирования сигнала для системы защиты применяются сочетания параметров, следует проводить проверку и калибровку всех используемых параметров.

Вывод из работы

4.93. В тех случаях, когда требование полноты периодических испытаний не согласуется с требованием обеспечения надежности группы безопасности (например, когда канал выводится из эксплуатации для испытаний и в то же время он должен быть надлежащим образом возвращен в эксплуатацию для обеспечения безопасности), следует добиваться, чтобы используемый метод испытаний обеспечивал удовлетворительное достижение обеих задач. Например, когда датчик выводится из эксплуатации с целью проведения периодических испытаний, следует использовать визуальную перекрестную проверку с резервными датчиками (или другими эквивалентными средствами) для проверки последующего возврата данного датчика в эксплуатацию. Кроме того, следует проверять состояние оборудования, работа которого была нарушена для проведения периодических испытаний (например, положение корневой задвижки для приборов, ремонтные байпасы), чтобы обеспечить их

возврат в первоначальное рабочее состояние. В этой связи следует обращать должное внимание на возможные ошибки человека.

4.94. При проектировании систем безопасности следует обеспечивать, чтобы во время проведения периодических испытаний остающиеся в эксплуатации части системы могли выполнять требующуюся задачу по обеспечению безопасности. В случае системы безопасности следует обеспечивать, чтобы вывод из работы какого-либо одного элемента или канала не приводил к утрате требуемого резервирования в случаях, когда приемлемый уровень надежности работы системы не может быть соответствующим образом подтвержден (см. [1], пункт 6.81). Следует обеспечивать, чтобы избранный метод испытаний сводил, насколько это практически возможно, к минимуму период времени, в течение которого оборудование выведено из эксплуатации. Предпочтительным методом вывода из эксплуатации является перевод выхода выведенного канала в определенное безопасное состояние.

4.95. Следует обеспечивать, чтобы правила проведения периодических испытаний систем безопасности КИПиУ не требовали и не допускали применения передвижных испытательных установок, временных соединительных проводов, удаления плавких предохранителей или размыкания выключателей. Временные соединения испытательного оборудования могут использоваться в тех случаях, когда подлежащее испытаниям оборудование системы безопасности обеспечено устройствами, специально предназначенными для подсоединения этого испытательного оборудования. Эти устройства следует считать частью системы безопасности, и следует обеспечивать, чтобы они соответствовали всем рекомендациям настоящего Руководства по безопасности, независимо от того, будет ли портативное испытательное оборудование разъединено с этими устройствами или останется подсоединенным к ним.

Контроль за испытаниями и их проведение

4.96. Следует обеспечивать, чтобы проведение испытаний не нарушало независимость систем безопасности и не приводило к отказам по общей причине.

ВОЗМОЖНОСТЬ ПРОВЕДЕНИЯ ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ

4.97. Ряд факторов, присущих системам КИПиУ атомных электростанций, обусловливает необходимость проектирования этих систем таким образом,

чтобы обеспечивалось надежное и эффективное техническое обслуживание. К таким факторам относятся:

— продолжительный жизненный цикл атомной электростанции по сравнению с типичной длительностью жизненных циклов различных аппаратных компонентов систем КИПиУ;
— неизбежный дрейф параметров, деградация или ухудшение характеристик контрольно-измерительных приборов; и
— износ аппаратных средств систем КИПиУ (т.е. интенсивность отказов элементов, которая делает неизбежной замену элементов как минимум один раз на протяжении жизненного цикла станции).

4.98. В случае систем, важных для безопасности, особое внимание следует уделять облегчению проведения работ по техническому обслуживанию при сохранении пригодности системы для работы в условиях окружающей среды, в которой эта система должна работать. Сведение к минимуму времени, необходимого для выполнения ремонта, является фактором, повышающим общую надежность и готовность. Возможность проведения технического обслуживания является важным элементом реализации принципов глубокоэшелонированной защиты, изложенных в пунктах 2.9–2.11 документа [1].

4.99. Системы КИПиУ, важные для безопасности, следует проектировать и размещать с расчетом облегчить проведение осмотра и технического обслуживания, обеспечить своевременный доступ и в случае возникновения отказов или ошибок обеспечить свободное проведение диагностики и ремонта.

4.100. Системы КИПиУ, важные для безопасности, следует проектировать с учетом возможностей и ограничений человека в выполнении требующихся работ по техническому обслуживанию. Когда это представляется практически возможным, системы КИПиУ следует располагать так, чтобы сводился к минимуму риск для эксплуатационного персонала и облегчалось проведение технического обслуживания оборудования. Вокруг оборудования следует оставлять достаточно места для выполнения персоналом, проводящим техническое обслуживание, своих функций в нормальных рабочих условиях. По возможности оборудование не следует располагать в местах, где имеется опасность значительного облучения (см. [12]) или где обычно существуют условия с экстремальной температурой или влажностью.

4.101. Системы, в которых используются устройства, расположенные в недоступных местах, следует тщательно изучать с целью определения

целесообразности применения других стратегий в устранении возможных отказов. Примеры таких стратегий включают использование запасных резервных устройств, применение устройств для дистанционного монтажа, а также переход станции на работу на пониженной мощности, если происходит отказ оборудования и оно не может быть незамедлительно отремонтировано или заменено. Во время работы на мощности расположение некоторых элементов может препятствовать проведению их регулярной калибровки. В этом случае особое внимание следует уделять обеспечению долгосрочной точности и устойчивости работы отобранных устройств, и следует предусматривать средства, позволяющие проводить сравнение с применением других устройств, например, сравнение интенсивности нейтронного потока с тепловой мощностью.

4.102. В системах, к которым применяется критерий единичного отказа, если канал шунтируется во время эксплуатации станции для целей проведения технического обслуживания, испытаний, ремонта или калибровки, следует обеспечивать, чтобы оставшиеся действующие каналы системы продолжали отвечать критерию единичного отказа, если не обосновывается иное, как указано в пунктах 4.15–4.21 настоящего Руководства по безопасности.

4.103. Средства обеспечения технического обслуживания систем КИПиУ, важных для безопасности, следует проектировать таким образом, чтобы любые воздействия на безопасность станции были допустимыми. Типичными примерами таких решений являются отключение одного канала в системе с резервными каналами и обеспечение средств для альтернативных действий, выполняемых вручную.

ДОКУМЕНТАЦИЯ

4.104. Уверенность в конструкции систем, важных для безопасности, в значительной степени зависит от правильности применяемых процессов. Документация играет важную роль в укреплении уверенности в конструкции и в подтверждении этой уверенности. Следует обеспечивать, чтобы документация, которая готовится при проектировании и создании систем, важных для безопасности, была ясной и точной.

4.105. Следует разрабатывать и хранить комплекты документов, с тем чтобы можно было отслеживать развитие концепции проектирования. Соответствующие документы следует готовить на каждом этапе процесса разработки, и при поставке системы следует прилагать комплект документов

системы. Детали, касающиеся области применения, типа и содержания документации, рассматриваются ниже в разделе 7. Для всех документов, относящихся к системам, важным для безопасности, следует обеспечивать выполнение условий, указанных ниже:

— следует обеспечивать, чтобы документация была понятной и ясной для людей с разным уровнем образования и опыта, которые могут принимать участие в проектировании, строительстве, вводе в эксплуатацию, эксплуатации, техническом обслуживании и лицензировании установки;
— следует использовать ясный стиль изложения с четко определенной терминологией; и
— во всей документации следует использовать унифицированные системы обозначений, терминологию, тексты и схемы.

4.106. Документацию следует составлять в соответствии с требованиями удобства и простоты использования, т.е. ее следует составлять с учетом потребностей пользователей следующим образом:

— следует обеспечивать, чтобы требования, спецификации и описания проекта допускали исключительно однозначную интерпретацию каждого отдельного требования, каждой спецификации или каждого описания;
— следует обеспечивать возможность поиска с переходом от документов более высокого уровня к проектной документации для проведения проверок полноты документации;
— следует обеспечивать возможность поиска с переходом от проектной документации к документам более высокого уровня для проведения проверок наличия излишних элементов документации;
— следует обеспечивать, чтобы документы не содержали каких-либо противоречащих друг другу или непоследовательных положений;
— для каждого элемента информации следует предусматривать единое, легко определяемое место в документации, и следует обеспечивать, чтобы этот элемент не повторялся и не дробился на несколько частей;
— каждое требование или каждый проектный модуль следует снабжать идентификационным обозначением (которое также помогает проводить поиск);
— требования и информацию о конструкции следует представлять так, чтобы можно было проводить проверки того, что системы, важные для безопасности, отвечают требованиям и выполнены в соответствии с проектом;
— следует обеспечивать, чтобы структура и стиль изложения документов были такими, чтобы можно было легко вносить любые необходимые

изменения с обеспечением требующейся полноты и последовательности; и

— следует обеспечивать, чтобы документация была понятной для пользователей, которым она предназначается.

ИДЕНТИФИКАЦИЯ УЗЛОВ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ

4.107. Узлы, важные для безопасности, следует идентифицировать с целью обеспечения того, чтобы требования, предъявляемые к системам, важным для безопасности, применялись при проектировании, строительстве, техническом обслуживании и эксплуатации станции. Такую идентификацию следует проводить с целью обеспечения выполнения требований в отношении классификации безопасности, изложенных в пунктах 5.1–5.3 документа [1].

4.108. Для систем безопасности и их элементов следует предусматривать однозначную маркировку, например, путем прикрепления соответствующей бирки или цветового кодирования. Кроме того, в составе самой системы безопасности следует соответствующим образом маркировать резервные каналы в целях уменьшения вероятности случайного выполнения работ по техническому обслуживанию, испытаниям, ремонту или калибровке не на том канале. Следует обеспечивать, чтобы такая идентификация не требовала использования чертежей, руководств или других справочных материалов. Следует обеспечивать, чтобы используемые способы идентификация отличались от опознавательной маркировки, применяемой для других целей. Аналогичную практику следует также применять для связанных с обеспечением безопасности систем. Элементы или модули, установленные в оборудовании или сборках, которые имеют четкую маркировку, не нуждаются в дополнительной идентификации. Методы управления конфигурацией обычно являются достаточными для обеспечения идентификации таких элементов, модулей и встроенного программного обеспечения ЭВМ.

5. ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ СИСТЕМ

5.1. Изложенные в настоящем разделе конкретные руководящие материалы применяются *в дополнение к* общим руководящим материалам, приведенным в разделе 4.

СИСТЕМЫ БЕЗОПАСНОСТИ

5.2. Система защиты представляет собой ту часть системы безопасности, которая выявляет отклонения от приемлемых условий работы станции и инициирует действия, направленные на предотвращение возникновения небезопасных или потенциально небезопасных условий. Для достижения этой цели используются различные конфигурации системы, и термин ‘система защиты’ не является универсальным во всех государствах-членах. Руководящие материалы, приведенные в разделе, посвященном системам защиты, применяются к системам, выполняющим эти функции.

СИСТЕМЫ ЗАЩИТЫ

5.3. Система защиты призвана поддерживать безопасность в ситуациях, когда системы управления не способны поддерживать переменные параметры работы станции в рамках определенных пределов. Такие ситуации могут возникать вследствие неисправности в системе управления или из-за того, что произошло событие, вызвавшее настолько быстрое изменение параметров процесса, что системы управления оказались не в состоянии надлежащим образом реагировать на это, или ввиду отказа узла, важного для безопасности. В таких ситуациях требуются быстрые действия, с тем чтобы воспрепятствовать превращению этой ситуации в возможную аварию.

5.4. Как правило, действие, необходимость которого вызывается конкретной ситуацией, а именно, задача обеспечения безопасности в такой ситуации, влечет за собой координированное срабатывание многочисленных узлов станции. Вместе с исполнительными системами безопасности и вспомогательными устройствами систем безопасности система защиты предназначена для выполнения всех предписанных задач обеспечения безопасности.

5.5. Система защиты контролирует соответствующие переменные параметры станции. Это могут быть технологические параметры процесса, такие, как скорость изменения флюенса (интегральной плотности потока) нейтронов[2] или уровни температуры теплоносителя и давления, или они могут представлять собой параметры, характерные для ожидаемых при эксплуатации событий или

[2] Скорость изменения флюенса ($\perp$) представляет собой приращение числа частиц $d\Phi$ за достаточно малый интервал времени, деленное на величину этого интервала времени: $\perp = d\Phi/dt$.

условий проектной аварии, такие, как скорости изменения параметров процесса, уровни влажности, изменение положения оборудования или радиационные уровни. Следует обеспечивать, чтобы измеряемые параметры станции – единичные или в отдельных сочетаниях – позволяли выявлять все ситуации, в которых должна быть решена задача, выполняемая в рамках обеспечения безопасности.

Назначение системы защиты

5.6. Требования к проектированию содержат требование ([1], пункт 6.80) о том, чтобы система защиты была спроектирована с таким расчетом, чтобы она могла:

— автоматически приводить в действие соответствующие системы, включая при необходимости системы остановки реактора, с тем чтобы предотвратить превышение установленных проектных пределов для ожидаемых при эксплуатации событий;
— обнаруживать проектные аварии и приводить в действие системы, необходимые для ограничения последствий таких аварий рамками, предусмотренными в проектных основах;
— быть в состоянии подавлять небезопасные действия системы управления.

5.7. Как правило, требуется, чтобы система защиты:

— обнаруживала, что параметр станции достиг уставки;
— определяла ситуацию, в которой необходимы защитные действия;
— инициировала в правильной последовательности выполнение всех действий по обеспечению безопасности, требуемых соответствующей задачей обеспечения безопасности в рамках самой системы защиты, исполнительных систем безопасности и вспомогательных устройств систем безопасности; и
— в некоторых государствах-членах контролировала параметры станции и обеспечивала их отображение, с тем чтобы оператор мог воспользоваться этими данными при выполнении ручного защитного действия.

5.8. Системой защиты инициируются следующие общие функции безопасности, которые определены в проектных основах:

— безопасная остановка реактора;
— поддержание параметров контура теплоносителя реактора в проектных пределах при всех эксплуатационных состояниях;

— отвод остаточного тепла во время ожидаемых при эксплуатации событиях и в аварийных условиях;
— аварийное охлаждение активной зоны в условиях проектной аварии и впоследствии;
— изоляция защитной оболочки реактора в условиях проектной аварии и после нее;
— понижение давления и температуры в защитной оболочке реактора после аварии;
— очистка атмосферы защитной оболочки;
— изоляция выделяющихся радиоактивных отходов; и
— контроль содержания летучих радиоактивных веществ, включая контроль их проникновения на рабочие участки и их выхода в окружающую среду.

5.9. Выполнение защитных действий начинается, когда значение параметра станции достигает заранее определенного значения, а именно, номинальной уставки.

Устройство системы защиты

5.10. Система защиты включает в себя все электрические и механические устройства и цепи, участвующие в формировании сигналов защитных действий на основании измерений параметров процесса. На рис. 3 показаны сопряжения системы с:

— технологическим процессом станции, защита которого осуществляется с помощью датчиков в составе системы защиты;
— исполнительными системами безопасности посредством исполнительных устройств, относящихся к исполнительным системам безопасности;
— любыми средствами отображения информации для оператора, которые не входят в систему защиты, но получают сигналы от этой системы через изолирующие устройства, расположенные в системе защиты; и
— системами управления через изолирующие устройства в системе защиты.

5.11. В целях упрощения на рис. 3 не показаны все возможные точки сопряжения системы защиты и других систем, таких, как мониторинговые информационные системы, вспомогательные устройства систем безопасности и пульты управления на периферийных панелях.

5.12. Система защиты состоит из следующих узлов:

— датчиков, которые могут быть:

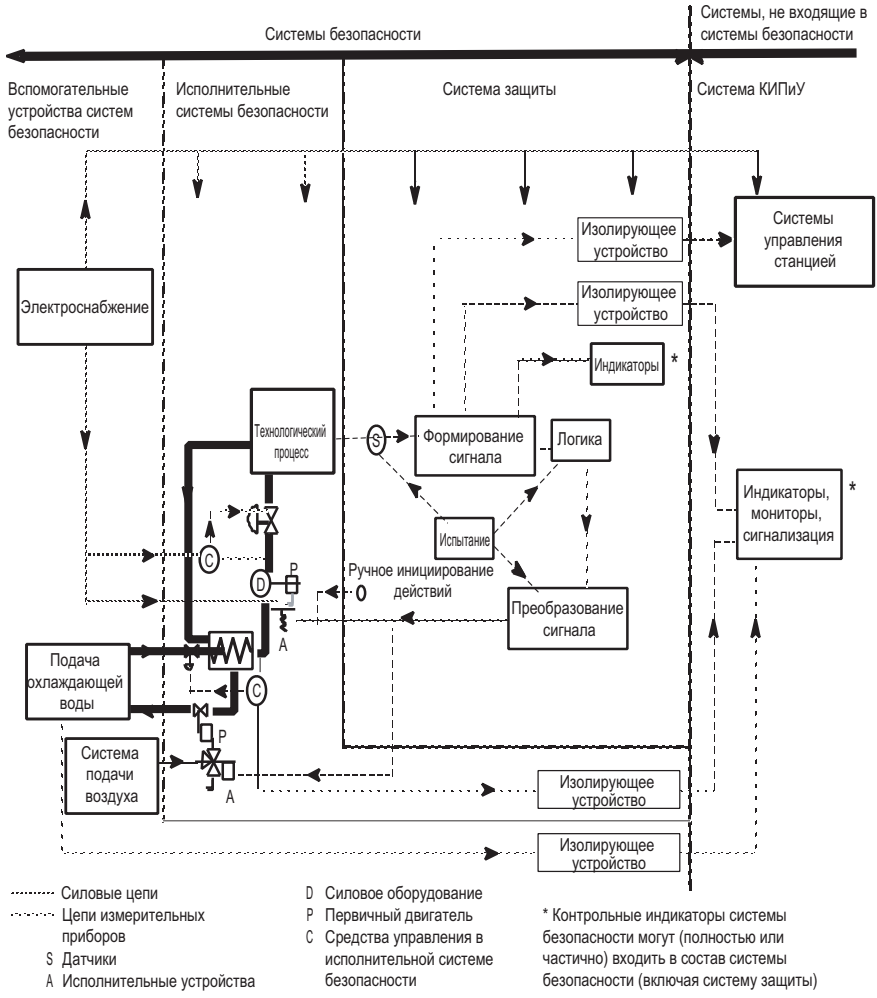

РИС. 3. Типичная структурная схема системы защиты и ее соединений с другими системами.

- связаны с технологическим процессом контрольно-измерительными линиями до преобразователя исходных данных включительно (например, давления, расхода и положения элементов); и
- первичными датчиками, применяемыми для измерения параметров станции (например, термопарами и ионизационными камерами);

— оборудования формирования сигналов для первичных датчиков, включая компараторы отключающих устройств и аналого-цифровые преобразователи сигналов;
— решающих логических устройств, используемых для каждого измеряемого параметра;
— оборудования преобразования сигналов, обеспечивающего подачу выходных сигналов в качестве защитных действий на исполнительные устройства;
— индикаторов, необходимых для ручного инициирования защитных действий;
— изолирующих устройств, сопряженных с информационными дисплеями оператора и системами различной классификации безопасности;
— панелей, стоек и корпусов, содержащих оборудование системы защиты;
— соединительных кабелей и каналов для внутренней прокладки кабелей;
— проходок через защитную оболочку для электрических кабелей и кабелей контрольно-измерительных приборов; и
— любого другого промежуточного оборудования, расположенного между выходом сигнала процесса и входными клеммами исполнительного устройства.

5.13. Руководящие материалы в этом разделе также применимы к другому оборудованию систем безопасности, которое должно работать с целью обеспечения выполнения функций системы защиты. Такое другое оборудование систем безопасности включает:

— исполнительные устройства, получающие выходные сигналы от системы защиты;
— оборудование первичных двигателей, срабатывающее от исполнительных устройств; и
— силовое оборудование, приводимое в действие оборудованием первичных двигателей.

Датчики

5.14. Систему защиты следует использовать для контроля параметров станции и выявления отклонений от установленных для них пределов, с тем чтобы могли выполняться предписанные функции безопасности. Следует обеспечивать соответствие измерений параметров станции требованиям, предъявляемым к рабочим характеристикам, определенным в проектных основах. Насколько это практически осуществимо, соответствующие условия на станции следует контролировать путем проведения непосредственных

измерений, а не получать эти данные на основе других измерений более косвенного характера.

5.15. При выборе диапазона измерений каждого подлежащего контролю параметра следует принимать во внимание точность, скорость реакции и степень выхода за пределы регулирования, необходимые для конкретной функции, и любую необходимую способность выполнения контроля после аварии. Если для надлежащего охвата всего диапазона изменения контролируемого параметра требуется несколько датчиков, следует предусматривать достаточное перекрытие диапазонов в каждой точке перехода от одного датчика к другому, с тем чтобы эффекты насыщения или наложения не препятствовали выполнению необходимой защитной функции.

5.16. Уставки параметров могут быть фиксированными или переменными, в зависимости от некоторых других параметров или условий на станции. В случае переменных уставок, устройства, используемые для задания уставок, классифицируются как часть системы защиты, и следует обеспечивать, чтобы они соответствовали предъявляемым к ней требованиям. В проекте системы следует предусматривать средства, позволяющие оператору определять значения уставок для каждого канала системы защиты.

«Фиксация состояния» системы защиты

5.17. При инициировании системой защиты определенного действия следует обеспечивать фиксацию состояния[3]. Фиксацию состояния не следует отключать, кроме случаев выполнения оператором действий вручную после завершения действия по обеспечению безопасности, или путем срабатывания системы защиты с целью предотвращения превышения пределов, установленных в проектных основах. После фиксации состояния по завершении действия следует продолжить выполнение необходимой последовательности операций до тех пор, пока не будет выполнена задача обеспечения безопасности. Следует предусматривать, чтобы после фиксации состояния по завершении действия система защиты автоматически контролировала условия на станции, осуществляя действия по обеспечению безопасности, диктуемые условиями на станции, и предоставляя информацию в поддержку любых допустимых действий оператора. Следует предусматривать,

[3] «Фиксация состояния» – это свойство элемента, заставляющее его выходной сигнал принять новое состояние и оставаться в этом состоянии после того, как входной сигнал или сигналы, инициировавшие это новое состояние, возвратились к своим прежним значениям.

чтобы выполнение функции безопасности не препятствовало инициированию системой защиты других защитных действий, которые могут потребоваться в связи с возникшими впоследствии условиями на станции.

5.18. Следует предусматривать, чтобы дополнительные элементы, обеспечивающие выполнение функций фиксации состояния, не снижали надежности действий по обеспечению безопасности до уровня ниже приемлемого.

Ручные действия по обеспечению безопасности

5.19. Действия оператора включают в себя:

— дублирование действий по обеспечению безопасности;
— непосредственное инициирование или прекращение некоторых действий по обеспечению безопасности; и
— возвращение в исходное состояние системы защиты после ее срабатывания.

5.20. При проектировании управляемых вручную установок следует предусматривать достаточную гибкость, с тем чтобы имелась возможность инициирования в аномальных ситуациях действий по обеспечению безопасности и была обеспечена долгосрочная послеаварийная эксплуатация.

5.21. Требования к большинству защитных действий таковы, что потребуется автоматическое инициирование действий. Кроме того, следует предусматривать возможность ручного инициирования остановки реактора и инициирования действий на уровне систем, таких, как изоляция защитной оболочки. Это не исключает вмешательства оператора в более детальной форме. Если предусматривается ручное управление, следует обеспечивать, насколько это практически осуществимо, его независимость от оборудования автоматической системы защиты.

5.22. В случае непреднамеренного ручного инициирования действия по обеспечению безопасности следует обеспечивать защиту станции путем автоматического срабатывания системы защиты. Ручное инициирование или прекращение действий по обеспечению безопасности может использоваться само по себе при условии, что может быть показано, что приемлемые пределы превышены не будут. Примерами таких выполняемых вручную действий являются:

— инициирование выполнения некоторых задач по обеспечению безопасности после завершения автоматических последовательностей операций;
— перевод остановленной станции в наиболее благоприятное состояние в долгосрочном плане после аварии; и
— инициирование некоторых действий по обеспечению безопасности, выполнение которых не требуется в течение значительного времени после ПИС.

5.23. При принятии решения о том, что одно лишь ручное действие приемлемо, следует подтверждать, что:

— оператор располагает достаточной и четко представленной информацией о классе безопасности, позволяющей ему делать обоснованные оценки и инициировать требуемые действия по обеспечению безопасности;
— оператор получил письменные инструкции и подготовку, которые могут оказать ему помощь;
— оператор имеет достаточно средств для осуществления требуемых действий;
— оператору дается достаточно времени для оценки состояния станции и завершения требуемых действий; и
— каналы связи между операторами, выполняющими действия, обеспечивают правильное выполнение этих действий.

5.24. В разных государствах-членах на выполнение оператором запланированного действия после начала ожидаемого при эксплуатации события или возникновения условий проектной аварии отводится различное время – от 10 до 30 мин. Отводимое время зависит от таких факторов, как сложность решения, имеющиеся средства визуальной индикации, необходимость дифференцировать различные ПИС и последствия принятия неправильного решения.

5.25. Следует обеспечивать, чтобы проектирование и компоновка помещения щита управления облегчали выполнение ручных действий по обеспечению безопасности. Следует обеспечивать, чтобы все органы управления, индикаторы и средства сигнализации, необходимые для безопасной эксплуатации, остановки реактора и отвода от реактора остаточного тепла, а также для выполнения функций системы защитной оболочки, были легко доступны и ясным образом представляли информацию оператору.

5.26. Следует предусматривать, чтобы информация о важных для безопасности действиях, предпринятых операторами вне помещения центрального щита управления, незамедлительно появлялась в помещении щита управления, кроме тех ситуаций, когда помещение щита управления повреждено или покинуто персоналом. В этом случае следует обеспечивать наличие необходимой информации в помещении резервного щита управления.

5.27. В Требованиях к проектированию содержится требование ([1], пункт 6.84) о том, что в проекте должно обеспечиваться сведение к минимуму вероятности того, что действия оператора могут привести к снижению эффективности системы защиты при нормальной эксплуатации и ожидаемых при эксплуатации событиях, но исключать отмену правильных действий оператора в условиях проектной аварии.

Ложное срабатывание

5.28. Ложное инициирование может происходить по многочисленным причинам, в частности, вследствие отказов оборудования, неправильных пределов отключения по некоторым параметрам в связи с изменениями, происходящими при нормальной эксплуатации, или ошибок человека при выполнении мер вмешательства. Они могут быть результатом:

— неправильного учета реакции станции на эксплуатационные помехи и последующих изменений контролируемых параметров;
— неправильных допусков на точность приборов, погрешностей калибровки и дрейфа или ошибок при выборе уставки отключения;
— неправильной трактовки шумов сигнала; или
— сочетания этих факторов.

5.29. Следует предусматривать, чтобы основным требованием к системе защиты было надлежащее выполнение предписанных для нее задач обеспечения защиты. Вместе с тем число ложных инициирований следует сводить к минимуму, насколько это практически осуществимо, так как они могут приводить к:

— появлению излишней нагрузки на оборудование;
— необходимости выполнения других действий по обеспечению безопасности;
— снижению уверенности оператора в правильной работе оборудования, что может впоследствии потенциально приводить к игнорированию действительных сигналов; и

— потере станцией производственной мощности.

5.30. Поэтому систему защиты следует проектировать так, чтобы она удовлетворяла соответствующим требованиям и чтобы в то же самое время сводилось к минимуму число ложных инициирований. Следует обеспечивать, чтобы ложный выходной сигнал системы защиты не мог инициировать событие, способное повлиять на безопасность. Если ложное инициирование в системе защиты может приводить к состоянию станции, в котором станция требует защиты, то следует предусматривать, чтобы условия безопасности поддерживались с помощью действий, инициируемых и осуществляемых незатронутыми частями системы защиты, исполнительных систем безопасности и вспомогательных устройств систем безопасности.

5.31. К эффективным мерам снижения числа ложных инициирований относятся фильтрация сигнала в реальном времени, валидация параметров, выбор одного из резервных сигналов и использование его для приведения в действие оборудования.

Взаимодействие между системой защиты и другими системами

5.32. Следует оценивать возможные взаимодействия между системой защиты и системами управления. В Требованиях к проектированию содержится требование о том, что должно предотвращаться взаимовлияние системы защиты и систем контроля и управления путем исключения взаимосвязей или применения соответствующего функционального разделения ([1], пункт 6.86). Если сигналы используются совместно системой защиты и какой-либо системой управления, то должно быть обеспечено соответствующее разделение (например, путем введения соответствующих развязок).

5.33. Если отказ системы управления может привести к условию на станции, которое вызывает необходимость выполнения действия по обеспечению безопасности и может одновременно блокировать один канал в группе безопасности, осуществляющей защиту от этого условия, то следует обеспечивать дальнейшее выполнение требований безопасности в случае совпадающего единичного отказа где-либо в этой группе безопасности. Если разрешается эксплуатация с каналом, байпасированным или выведенным из работы для целей испытаний или технического обслуживания, то его байпас или вывод из работы следует рассматривать в качестве допущения при анализе.

5.34. Если ПИС может вызывать такое срабатывание системы управления, которое приводит к условию на станции, требующему выполнения действия по

обеспечению безопасности, то следует обеспечивать, чтобы то же самое ПИС не препятствовало надлежащей работе группы безопасности, предусмотренной для защиты от воздействия этого условия на станции. К эффективным мерам предотвращения взаимодействия этого типа относятся:

— введение в группу безопасности дополнительного оборудования с целью решения потенциальных проблем взаимодействия;
— введение на станции барьеров и/или альтернативных мер, направленных на ограничение ущерба в результате ПИС; или
— применение этих способов в сочетании таким образом, чтобы проект группы безопасности и/или станции обеспечивал поддержание условий на станции в допустимых пределах.

5.35. В случае, когда отдельное исполнительное устройство, такое, как двигатель насоса или приводной механизм клапана, управляется системой управления станции и системой защиты, следует предусматривать возможность корректировки системой защиты действия, инициируемого системой управления. Например, если система управления требует работы насоса на половинной скорости, а система защиты требует работы насоса на полной скорости, следует обеспечивать, чтобы сигнал системы защиты имел приоритет и насос работал на полной скорости. Точно так же, если система управления требует закрытия клапана, а система защиты требует, чтобы клапан был открыт, следует обеспечивать, чтобы сигнал системы защиты имел приоритет и клапан был открыт.

Технологические байпасы

5.36. Отключения, которые защищают реактор в одном состоянии при нормальной эксплуатации, могут препятствовать переходу в другие эксплуатационные состояния. Например, отключения, которые защищают реактор на малой мощности, будут препятствовать достижению реактором полной мощности. Для того, чтобы осуществить эти переходы, следует не допускать инициирования излишнего и нежелательного защитного действия посредством технологического байпаса (иногда называемого условием отключения). Такую привязку логических условий к сигналам остановки следует интегрировать в систему защиты.

5.37. Следует предусматривать, чтобы всякий раз, когда не выполняются условия, допускающие байпас, системы безопасности автоматически предотвращали активацию технологического байпаса и выполняли одно из следующих действий:

— отменяли активированный технологический байпас,
— переводили станцию в состояние, при котором технологический байпас допустим, или
— инициировали выполнение соответствующих защитных действий.

5.38. Независимо от способа, которым выполняется активация, средства активации технологических байпасов рассматриваются в качестве части системы защиты, и следует обеспечивать, чтобы они соответствовали положениям настоящего руководства по безопасности.

ИСТОЧНИКИ ЭНЕРГОСНАБЖЕНИЯ

5.39. Следует обеспечивать, чтобы энергоснабжение (электропитание и, при необходимости, обеспечение работы пневмо-и гидравлических систем) было совместимо с системой КИПиУ. Следует обеспечивать, чтобы классификация, аттестация, изоляция, возможность проведения испытаний, обслуживания и индикация вывода из эксплуатации энергоснабжения систем КИПиУ, важных для безопасности, соответствовали требованиям надежности систем КИПиУ, работу которых оно обеспечивает.

5.40. Через линии электроснабжения обычно распространяются электрические помехи, источники которых могут находиться вне пределов системы КИПиУ или которые могут возникать в других системах КИПиУ, непосредственно или косвенно подключенных к тем же линиям электроснабжения. Следует предусматривать, чтобы конструкция источников энергоснабжения и систем КИПиУ обеспечивала ограничение таких эффектов помех, с тем чтобы они не ухудшали выполнение функций системы КИПиУ. Это следует подтверждать путем испытаний, анализа или с помощью другого соответствующего способа оценки комплексных систем КИПиУ, важных для безопасности, и связанных с ними систем электроснабжения (см. также раздел 4).

5.41. Системы КИПиУ, важные для безопасности, к которым предъявляется требование постоянной готовности в эксплуатационных состояниях или условиях проектной аварии, следует подключать к источнику бесперебойного электропитания. Следует обеспечивать, чтобы требования к рабочим характеристикам источников бесперебойного питания соответствовали требованиям, предявляемым к системе, питание которой они обеспечивают.

5.42. В тех случаях, когда это оправдано условиями эксплуатации, системы КИПиУ, важные для безопасности, могут быть переключены операторами

станции или устройствами автоматической коммутации с нормального электропитания на питание от резервных источников питания, при условии, что функции систем КИПиУ допускают связанное с этим прерывание электропитания. Систему переключения следует в большинстве случаев рассматривать в качестве части системы электроснабжения.

ЦИФРОВЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ

5.43. Цифровые компьютерные системы используются в системах КИПиУ, важных для безопасности, при выполнении функций защиты, сбора данных, расчетов, мониторинга управления и индикации. При правильном проектировании они обеспечивают повышенную надежность, точность и расширенные функциональные возможности по сравнению с аналоговыми системами. Компьютерные системы могут быть самыми разнообразными – от мощных процессоров, обеспечивающих выполнение многих функций до широкой сети малых процессоров, решающих конкретные прикладные задачи.

5.44. Компьютерные системы могут с успехом использоваться для обнаружения и контроля неисправностей внутреннего и внешнего характера по отношению к системам станции и оборудованию, важному для безопасности.

5.45. Аппаратные средства и программное обеспечение компьютерных систем следует конфигурировать так, чтобы в условиях вероятных отказов аппаратных средств и программного обеспечения обеспечивался заранее определенный безопасный режим работы системы.

5.46. При использовании компьютеров возможно выполнение одним комплексом оборудования нескольких функций системы. Недостаток этого подхода состоит в том, что при выходе из строя одного компонента может одновременно прекратиться выполнение сразу нескольких функций. Поэтому данный фактор следует учитывать при проектировании и анализе систем.

5.47. Если использование компьютера связано с выполнением двух или более функций, относящихся к различным классам безопасности, то следует предусматривать, чтобы компьютерная система удовлетворяла требованиям более высокого класса безопасности.

5.48. При запуске и перезапуске цифровой системы (например, после временной потери электропитания) следует обеспечивать возвращение системы

в заранее определенное состояние, обеспечивающее дальнейшую безопасную эксплуатацию.

5.49. Следует обеспечивать, чтобы программное обеспечение цифровой системы было укомплектовано надлежащей документацией и было разработано в рамках контролируемого инженерного процесса разработки.

5.50. Дополнительные руководящие материалы по использованию цифровых компьютерных систем приведены в руководстве по безопасности МАГАТЭ [2].

Техническое обслуживание

5.51. На протяжении всего срока службы станции следует сохранять надлежащий экспертно-технический потенциал в области первоначальной технологии аппаратных средств и программного обеспечения. В отличие от остальных систем станции, техническое обслуживание компьютерных систем представляет собой нестандартную задачу. Персоналу технического обслуживания следует обладать глубокими знаниями в области компьютеризованных систем и процесса разработки, используемого при модернизации цифровых систем.

Модернизация цифровых систем

5.52. Следует учитывать тот факт, что компьютеризованные системы КИПиУ на новых станциях будут также подвергаться физическому и моральному старению и в конечном счете потребуют замены. Поскольку поставщики цифрового оборудования часто меняют выпускаемые модели, возникают трудности с поставками запасных частей в течение всего срока службы станции. Пользователь должен хранить на складе значительное количество цифровых компонентов, и при этом следует учитывать возможное ухудшение характеристик электронной продукции, хранящейся в течение длительного промежутка времени.

Передача данных

5.53. Передача данных, как она определена для целей настоящего Руководства по безопасности, представляет собой передачу из одного места в другое двух или более сигналов или сообщений по одиночному каналу передачи данных с использованием методов временного разделения, частотного разделения, импульсного кодирования или подобных методов. Реализация передачи данных возможна с использованием широкого диапазона технических решений: от

простых аппаратных решений, обеспечивающих только мультиплексный режим, и до сложных самокорректирующихся многоуровневых коммуникационных протоколов, контролируемых программным обеспечением.

5.54. Следует обеспечивать, чтобы каналы передачи данных, важные для безопасности, соответствовали рекомендациям относительно независимости, изложенным в разделе 4, в частности, в пунктах 4.36-4.48.

5.55. При проектировании системы передачи данных следует предусматривать обнаружение и, насколько это практически осуществимо, исправление ошибок и индикацию состояния данных в передаваемой информации.

5.56. Проверка передачи данных может проводиться периодически в качестве автоматической функции самопроверки. Следует обеспечивать, чтобы выбранная частота этой самопроверки соответствовала использованию данных и частоте запросов на выполнение системой функции безопасности. Функции обнаружения и исправления ошибок могут использоваться для повышения надежности передачи сигнала с целью обеспечения соответствия целям надежности.

5.57. Следует выбирать и соответствующим образом конфигурировать коммуникационную технологию, с тем чтобы она удовлетворяла требованиям в отношении времени реакции во всех возможных условиях загрузки данных.

5.58. В случаях, когда весьма важно обеспечивать надежность данных и канала передачи данных, следует выбирать соответствующую коммуникационную технологию. Выбор и использование более сложной технологии могут обеспечивать определенные функциональные преимущества, но могут также привести к появлению дополнительных видов отказов и трудностей в проведении валидации. Следует уделять надлежащее внимание использованию резервирования в канале передачи данных, надлежащему уровню надежности самого канала передачи данных в целом и способности передающих и принимающих систем выдерживать все возможные виды отказов. Следует обеспечивать, чтобы использование передачи данных не нарушало физического или функционального группирования элементов обработки данных или логических элементов в архитектуре системы.

5.59. Как правило, следует избегать, насколько это практически возможно, потоков данных от систем более низкого класса безопасности к системам более высокого класса безопасности. В тех случаях, когда такие потоки данных необходимы, следует принимать меры (такие, как валидация данных или

проверки принадлежности к диапазону данных) с целью обеспечения того, чтобы данные от системы низшего класса не создавали угрозы выполнению функций, важных для безопасности.

6. ВЗАИМОДЕЙСТВИЕ ЧЕЛОВЕК-МАШИНА

6.1. Мониторинг систем, важных для безопасности, и управление ими осуществляются в виде сочетания функций автоматического измерения и управления и операций мониторинга и управления, осуществляемых человеком. На современных атомных станциях широко используются автоматическое управление и автоматическое приведение в действие систем безопасности, однако общее управление работой станции по-прежнему осуществляется операторами станции.

6.2. При проектировании следует стремиться к достижению основной цели – разработке конструкции, совместимой с сильными сторонами и ограничениями, присущими человеку-оператору. При проектировании с учетом взаимодействия человек-машина следует уделять внимание должностным обязанностям и функциям персонала станции с целью обеспечения эффективного взаимодействия эксплуатационного персонала и станции. При этом следует уделять внимание не только операторам, но также и ремонтникам, инспекторам и административному и аварийному персоналу станции.

6.3. В целях облегчения выбора проектных принципов в отношении представления информации и органов управления оператор рассматривается как лицо, исполняющее двойную роль: системного администратора, отвечающего в том числе и за управление авариями, и оператора оборудования.

6.4. В Требования к проектированию содержится требование ([1], пункт 5.54) о том, чтобы оператор в роли системного администратора получал информацию, позволяющую ему:

— оперативно оценивать общее состояние станции, в каком бы режиме она ни находилась, будь то нормальная эксплуатация, ожидаемое при эксплуатации событие или аварийные условия, и получать подтверждение того, что предусмотренные в проекте автоматические действия по обеспечению безопасности осуществляются; и

— определять соответствующие инициируемые оператором действия по обеспечению безопасности, которые должны быть предприняты.

6.5. Требования к проектированию содержат требование ([1], пункт 5.55) о том, чтобы оператор в роли оператора оборудования получал достаточную информацию о параметрах, относящихся к отдельным системам и оборудованию станции, для подтверждения того, что может быть эффективно начато осуществление необходимых действий по обеспечению безопасности.

6.6. В целом, ввиду большого числа параметров станции и оборудования, инструментальное измерение которых и управление которыми обычно осуществляются на современной атомной станции, следует уделять серьезное внимание проектированию с учетом взаимодействия человек-машина с целью обеспечения того, чтобы вся необходимая информация была доступна оператору, когда это необходимо, и при любых обстоятельствах. В то же самое время следует обеспечивать, чтобы оператор не был перегружен большими объемами данных, которые трудно осмысливать вследствие ограниченных возможностей восприятия, познания и памяти человека. Подобным же образом при проектировании систем, включающих инициируемые оператором управляющие воздействия, особое внимание следует уделять снижению вероятности ошибки человека и обеспечению устойчивости системы к воздействию ошибок, которые могут быть допущены.

6.7. Требования к проектированию содержат требование ([1], пункт 5.50) о том, чтобы на раннем этапе разработки проекта в процесс проектирования включался систематический анализ человеческих факторов и взаимодействия человек-машина, который должен проводиться в течение всего процесса проектирования с целью обеспечения надлежащего и четкого разграничения функций между эксплуатационным персоналом и предусматриваемыми автоматическими системами.

6.8. Следует обеспечивать, чтобы операторы станций и лица, выполняющие работы по техническому обслуживанию, получали информацию, дающую им представление о состоянии станции и позволяющую им выполнять свои обязанности. Эффективным методом достижения этой цели является осуществление инженерно-технической программы, учитывающей человеческие факторы, начиная с наиболее ранних стадий проектирования (см. пункты 7.6–7.10).

6.9. В комплексном цикле проектирования следует рассматривать вопросы проектирования, подготовки кадров, эксплуатационных процедур и

организации работы групп специалистов в связи с системами КИПиУ (таким образом, чтобы, например, могли быть проанализированы последствия использования компьютеризованного взаимодействия человек-машина для поведения оператора). Детальное рассмотрение этих соображений выходит за рамки настоящего Руководства по безопасности. В других нормах безопасности будут представлены руководящие материалы по общему процессу учета человеческих факторов.

6.10. Интерфейсы оператора со станцией расположены прежде всего в помещении центрального щита управления, центре технической поддержки, помещениях резервного щита управления и аварийном центре управления. К этим техническим средствам относятся связанные с безопасностью индикаторы, связанные с безопасностью органы управления, системы аварийного мониторинга, устройства аварийной сигнализации и системы регистрации исторических данных. В настоящем разделе приводятся руководящие материалы по проектированию этих технических средств и систем.

ПОМЕЩЕНИЕ ЦЕНТРАЛЬНОГО ЩИТА УПРАВЛЕНИЯ

6.11. Управляющие воздействия, связанные с безопасностью, осуществляются прежде всего из помещения центрального щита управления. В Требованиях к проектированию содержится требование ([1], пункт 6.71) о том, что должно быть предусмотрено помещение щита управления, из которого можно было бы безопасно управлять АЭС во всех ее эксплуатационных состояниях и из которого можно было бы принимать меры по поддержанию станции в безопасном состоянии или по возвращению ее в это состояние после возникновения ожидаемых при эксплуатации событий, проектных аварий и тяжелых аварий. Кроме того, из помещения щита управления могут приниматься меры по смягчению последствий тяжелых аварий.

6.12. В Требованиях к проектированию содержится требование ([1], пункт 6.73) о том, что размещение контрольно-измерительных приборов и способ представления информации должны давать эксплуатационному персоналу соответствующую полную картину состояния и характеристик АЭС. При проектировании помещения щита управления необходимо учитывать эргономические факторы.

6.13. Основные цели функционального проектирования помещения щита управления направлены на обеспечение оператора точной, полной и

своевременной информацией о состоянии оборудования и систем станции во всех эксплуатационных состояниях и условиях проектной аварии и оптимизацию деятельности оператора при мониторинге станции и управлении ее работой. При проектировании помещения центрального щита управления, которое является центром, где сосредоточены связанные с КИПиУ элементы систем безопасности, связанные с безопасностью системы и системы, не важные для безопасности, следует учитывать требования по функциональной изоляции и физическому разделению, а также эргономические принципы.

6.14. При проектировании помещения щита управления следует учитывать факторы инженерной психологии, такие, как рабочая нагрузка, возможность ошибки человека, время реакции оператора и сведение к минимуму физических и умственных усилий оператора, с тем чтобы облегчить выполнение эксплуатационных процедур, предписанных для обеспечения безопасности во всех эксплуатационных состояниях и после возникновения условий проектной аварии. Следует предусматривать необходимые меры по обеспечению удовлетворительных условий работы, включая условия освещения, температуры и влажности, и предотвращению возникновения опасных условий, таких, как неприемлемые уровни излучения, или наличие в воздухе дыма или токсических веществ. Поскольку связанные с безопасностью индикаторы, сигнализаторы и органы управления обычно используются во всех условиях эксплуатации станции, при проектировании помещения щита управления следует сбалансированным образом рассматривать все принятые в допущениях условия. Во многих случаях следует использовать автоматическое срабатывание связанных с безопасностью органов управления, с тем чтобы не налагать на оператора чрезмерного бремени по выполнению функций безопасности. Учет человеческого фактора приводит к формулированию нескольких проектных целей, наиболее важные из которых указаны ниже:

— представление информации посредством индикаторов и контрольно-измерительных приборов следует осуществлять в рамках комплексной согласованной системы, с тем чтобы оптимизировать понимание оператором состояния станции и оптимизировать деятельность, необходимую для управления станцией;
— в тех случаях, когда информация об управляемом процессе поступает на резервные или неодинаковые индикаторы в качестве средства подтверждения основной информации, эти альтернативные источники информации следует, насколько это практически осуществимо, располагать и конфигурировать так, чтобы оператор при принятии решений мог пользоваться обоими источниками с минимальными

усилиями, не ставя под угрозу требуемую независимость источников информации;
— индикаторы в помещении щита управления следует располагать таким образом, чтобы оператор мог легко наблюдать за ними и определять состояние любой системы;
— управляющие устройства и функционально связанные с ними индикаторы следует, насколько это практически возможно, располагать так, чтобы это облегчало действия оператора;
— следует обращать внимание на необходимость обеспечения для операторов возможности иметь эффективное общее представление о состоянии станции, а также обеспечения согласованности информации, представляемой различному персоналу в помещении щита управления;
— некоторые индикаторы могут показывать параметры, измеряемые контрольно-измерительными приборами различных уровней аттестации (т.е. надежности); в этих случаях следует предоставлять на индикаторе четкую информацию для оператора, указывающую различия в уровне аттестации.

ПОМЕЩЕНИЯ РЕЗЕРВНОГО ЩИТА УПРАВЛЕНИЯ

6.15. Помимо помещения центрального щита управления используются различные типы помещений резервного щита управления и посты управления. Перечень и распределение функций в различных государствах-членах неодинаковы, но к числу других помещений щита управления и постов управления относятся:

— помещение аварийного щита управления,
— зона вспомогательных органов управления,
— панель безопасного останова,
— помещения резервного щита управления, и
— другие локальные пункты управления.

Дополнительная информация содержится в [4]. Ниже приведены руководящие материалы по проектированию.

6.16. В Требованиях к проектированию содержится требование ([1], пункт 6.75) о том, что предпочтительно в одном помещении, физически и электрически отделенном от основного помещения щита управления, должно быть также размещено достаточное количество контрольно-измерительных приборов и оборудования для управления, с тем чтобы можно было остановить реактор и

поддерживать его в этом состоянии, отводить остаточное тепло и контролировать важнейшие параметры станции, если будет потеряна возможность осуществлять эти важнейшие функции безопасности из помещения основного щита управления. Эти контрольно-измерительные приборы обычно располагаются в помещении резервного щита управления.

6.17. В проектных основах станции следует определять условия, при которых не представляется более возможным выполнять функции управления из помещения центрального щита управления вследствие его враждебного захвата, пожара или других причин, в силу которых может возникнуть необходимость покинуть помещение центрального щита управления.

6.18. Следует надлежащим образом предусматривать возможность передачи приоритета управления на другой пост и изоляции оборудования в помещении центрального щита управления всякий раз, когда персонал покидает помещение центрального щита управления.

6.19. Проектные основы атомной станции обычно таковы, что утрата возможности работы в помещении щита управления вследствие ПИС является весьма редким событием. Поэтому нет необходимости постулировать ситуацию, при которой второе ПИС произойдет в условиях, когда работа в помещении центрального щита управления невозможна, а требуемые функции безопасности выполняются из помещения резервного щита управления.

6.20. Если проектные основы требуют учитывать повреждение оборудования в помещении щита управления, то следует применять требования по обеспечению независимости в отношении электрических схем, обеспечивающих электропитание этих зон, с тем чтобы отказы, вызываемые ПИС в одной зоне, например короткие замыкания, обрывы цепей и высокие напряжения, не препятствовали выполнению требующихся задач обеспечения безопасности в другой зоне. В зависимости от характера события и проекта станции может оказаться необходимым предусматривать для каждой зоны резервные измерительные каналы, логические каналы и другую аппаратуру, обеспечивающую безопасность работы. При использовании общего исполнительного оборудования в системах безопасности в проектных основах следует предусматривать приоритет сигналов пункта управления.

6.21. При проектировании помещений резервного щита управления следует предусматривать соответствующие меры по предотвращению несанкционированного доступа и использования.

6.22. Ручное управление из помещения резервного щита управления следует, как правило, осуществлять посредством выполнения простых действий, таких, как приведение в действие переключателя или нажатие кнопки. Следует обеспечивать, чтобы в той степени, в какой это возможно, индикаторы и органы управления были аналогичны индикаторам и органам управления в помещении центрального щита управления.

6.23. При проектировании помещения центрального щита управления и помещений резервного щита управления следует предусматривать, чтобы никакое ПИС не могло одновременно оказать воздействие на помещение центрального щита управления и помещения резервного щита управления в такой степени, что станет невозможным выполнение функций безопасности.

6.24. Следует также обеспечивать, чтобы необходимый приоритет при инициировании конкретной функции безопасности мог передаваться помещению центрального щита управления, либо помещению резервного щита управления.

6.25. При проектировании помещений резервного щита управления следует принимать во внимание сведения, изложенные в соответствующих частях других разделов настоящего руководства по безопасности, и надлежащим образом учитывать различия в назначении и использовании помещений резервного щита управления и помещения центрального щита управления.

6.26. В зависимости от характера ПИС, следует рассматривать возможность введения измерительных каналов, независимых от каналов в помещении центрального щита управления. При необходимости следует также рассматривать особые потребности во вспомогательных средствах для системы безопасности.

6.27. При проектировании следует также должным образом рассматривать возможность обеспечения подходящего маршрута доступа, позволяющего операторам, покидающим помещение центрального щита управления, безопасно и удобно перейти в помещения резервного щита управления.

6.28. На протяжении выбранного маршрута доступа от помещения центрального щита управления к помещениям резервного щита управления следует предусмотреть надлежащую индикацию потенциальных опасностей (таких, как дым) и применение защитных мер (такие, как респираторы).

6.29. Помещения резервного щита управления следует располагать и конфигурировать так, чтобы операторы могли приступать к выполнению своих обязанностей на новом месте в рамках приемлемого предельного срока.

6.30. Если анализ безопасности показывает, что потребуется продолжительное пребывание, следует обеспечивать необходимые условия работы, например, посредством вентиляции. Следует также предусматривать надлежащее размещение персонала, средства для ведения записей, доступ к документам и рабочие поверхности для работы с документами.

СРЕДСТВА АВАРИЙНОГО РЕАГИРОВАНИЯ

6.31. Помещение центрального щита управления является для операторов станции информационным центром и центром по принятию мер в эксплуатационных состояниях и в условиях проектной аварии. Оно может также использоваться в качестве основного центра по руководству начальными стадиями деятельности за пределами площадки в случае аварийной ситуации. Однако следует обеспечивать, чтобы операции аварийного реагирования за пределами площадки не ухудшали способность персонала помещения щита управления выполнять процедуры управления авариями. Поэтому следует предусматривать меры по быстрейшему выводу из помещения щита управления не связанных с эксплуатацией операций по аварийному реагированию, таких, как руководство действиями групп или оповещение и координация действий за пределами площадки, и по ограничению доступа в помещение щита управления в случае аварийной ситуации.

6.32. В Требованиях к проектированию содержится требование ([1], пункт 6.87) о том, что на площадке станции отдельно от помещения щита управления станции должны предусматриваться аварийный центр управления, в котором мог бы собираться аварийный персонал для работы в случае аварийной ситуации. Следует обеспечивать, чтобы в этот центр поступала информация о важных параметрах станции и о радиационной обстановке на станции и в непосредственной близости от нее. В центре следует предусматривать средства связи с помещением щита управления, помещениями резервного щита управления и другими важными пунктами станции, а также с организациями аварийного реагирования на площадке и за ее пределами. Необходимо предпринимать надлежащие меры по защите лиц, находящихся в этом помещении в течение продолжительного периода времени, от опасностей, возникающих при тяжелой аварии.

6.33. Помимо локальных мероприятий по управлению аварией некоторые государства-члены считают целесообразным размещать на удалении от площадки аварийный вспомогательный центр по координации получаемых от экспертов рекомендаций. Подобным же образом следует предусматривать соответствующие информационно-коммуникационные системы в связи с такими средствами.

6.34. Дополнительная информация относительно средств аварийного реагирования содержится в [4, 13].

СРЕДСТВА УПРАВЛЕНИЯ

6.35. Если оборудованием, важным для обеспечения безопасности, можно управлять из помещения щита управления и из мест, находящихся вне помещения щита управления, то следует обеспечивать автоматическую визуальную индикацию фактического источника управляющих действий (с помощью сигнализаторов, контролепригодных световых индикаторов, позиций ручных переключателей) на каждом посту управления.

6.36. В помещении щита управления следует предусматривать все органы управления, необходимые для принятия мер в таких аварийных условиях, в которых:

— осуществление необходимого управления вне помещения щита управления может быть ограничено вследствие аварийных условий, и
— дефицит времени для принятия мер в аварийных условиях может не позволить оператору покинуть помещение щита управления с целью осуществления управления из других мест.

6.37. Следует предусматривать надлежащие функции обслуживания, такие, как освещение и средства связи и пожаротушения, позволяющие эксплуатационному персоналу станции считывать показания контрольных индикаторов и принимать надлежащие меры по обеспечению безопасности после любого ПИС.

6.38. При проектировании средств управления следует принимать во внимание не связанные с КИПиУ аспекты, такие, как вопросы радиологической защиты [12], обеспечения нормальных условий работы [8], защиты от молний, противопожарной защиты [6], доступности и контроля доступа, защиты от

летящих предметов [7, 8] и сейсмостойкости [14], исходя из определенных для станции ПИС внешнего и внутреннего происхождения.

6.39. Речевая связь между помещением центрального щита управления, помещениями резервного щита управления, другими соответствующими местами на станции и аварийными службами за пределами площадки важна для безопасности, особенно в условиях ожидаемых при эксплуатации событий или проектных аварий. Такую связь следует, как правило, обеспечивать посредством двух, предпочтительно неодинаковых каналов связи, совместимых по электромагнитным параметрам с системами КИПиУ (телефоны с автономным питанием, телефоны с питанием от батарей, ручные портативные радиостанции). Эти линии связи следует прокладывать таким образом, чтобы пожары, отказы электрических систем или другие соответствующие ПИС не могли приводить к одновременному выходу из строя обеих систем.

ИНДИКАТОРЫ

6.40. Индикаторы представляют операторам станции информацию о состоянии станции, а также о состоянии систем и оборудования, необходимых для мониторинга, технического обслуживания и эксплуатации систем, важных для безопасности, и поддержания параметров станции в пределах значений, определенных в проектных основах. Индикаторы используются для выполнения одной или нескольких следующих функций:

— информирования операторов станции о состоянии систем и состоянии безопасности станции;
— информирования экспертов по безопасности на площадке и за ее пределами о состоянии безопасности станции в аварийных условиях; и
— представления информации о поведении во времени параметров технологического процесса, важных для безопасности, для целей оперативного или последующего анализа, а также для представления отчетности как эксплуатирующей организации, так и внешним компетентным органам.

6.41. Следует предусматривать сигнализацию об изменениях состояния систем безопасности, а также индикацию их состояния в помещении щита управления.

6.42. При нормальной эксплуатации операторы постоянно контролируют состояние станции с помощью комплекса индикаторов и сигнализаторов или дисплеев, расположенных в помещении центрального щита управления.

Сигнальные или другие устройства сигнализируют об отклонениях от нормальной эксплуатации. Следует предусматривать, чтобы в случае их возникновения операторам предоставлялась информация, необходимая:

— для определения действий, предпринимаемых автоматическими системами;
— для анализа причины нарушения нормальной работы;
— для отслеживания характера поведения станции; и
— для осуществления любых необходимых выполняемых вручную мер противодействия.

6.43. Следует предусматривать, чтобы средства индикации обеспечивали отображение соответствующих переменных параметров в соответствии с допущениями в рамках анализа безопасности и с необходимой оператору информацией об эксплуатационных состояниях и условиях проектной аварии. Следует обеспечивать, чтобы точность и диапазон индикаторов соответствовали допущениям при анализе безопасности.

6.44. В тех случаях, когда для выполнения требований надежности используются резервные индикаторы, следует предусматривать их функциональную изоляцию и физическое разделение с целью обеспечения того, чтобы единичный отказ в этой системе не приводил к полной потере информации о контролируемом параметре; например, путем использования двух клавиатур для работы с несколькими дисплеями.

6.45. В тех случаях, когда отказ одиночного канала отображения информации может быть причиной неоднозначности представляемой информации (например, единичный отказ, приводящий к расхождению данных, представляемых двумя резервирующими друг друга индикаторами), это может приводить к тому, что оператор деактивирует или не приведет в действие требуемую функцию безопасности. Для того чтобы исключить подобные ситуации, следует предусматривать дополнительные средства, позволяющие оператору разрешать такие конфликты при представлении информации. Это может быть достигнуто, например, путем введения третьего канала передачи информации или отображения другого переменного параметра, известным образом связанного с отображаемыми на индикаторах параметрами и обеспечивающего выявление неисправного канала. В тех случаях, когда среднее время обнаружения отказа и восстановления работоспособности или обнаружения отказа и замены меньше, чем допустимый период неработоспособности, приемлемым является использование одноканального индикатора с четкой идентификацией видов отказа.

6.46. В тех случаях, когда информация о тенденции изменения переменного параметра необходима для определения соответствующего действия оператора, следует предусматривать средства индикации этой тенденции.

6.47. Если часть системы, важной для безопасности, была преднамеренно деактивирована с использованием функции, предусмотренной при проектировании конкретно для данной цели, то следует обеспечивать автоматическую индикацию этого состояния в помещении щита управления. Если часть системы, важной для безопасности, была деактивирована с использованием других средств административного контроля, то следует обеспечивать четкую индикацию этого действия в помещении щита управления.

МОНИТОРИНГ АВАРИЙНЫХ УСЛОВИЙ

6.48. Следует предусматривать надежную, легкодоступную и понятную индикацию информации о состоянии станции и тенденциях изменения ключевых параметров станции с целью обеспечения того, чтобы оператор мог предпринимать эффективные меры в аварийных условиях и чтобы вспомогательный персонал, прибывающий для оказания помощи, был надлежащим образом информирован. Ниже приводятся рекомендации относительно проектирования систем и средств аварийного мониторинга.

6.49. Информационные дисплеи для мониторинга аварийных условий на станции следует предусматривать в помещении центрального щита управления и при необходимости в помещениях резервного щита управления.

6.50. При определении характера отображаемой информации следует принимать во внимание, что оператору необходимо:

— выявлять отклонение от нормальных условий;
— определять конкретную аварию и, когда это возможно, ее исходное событие;
— проверять выполнение требуемых функций безопасности;
— отслеживать протекание события или аварии;
— определять ситуации, когда развиваются условия, оправдывающие принятие компетентными органами аварийных мер вне границы станции; и
— разрешать конфликты при представлении информации, которые могут возникнуть в результате резервирования каналов.

6.51. С целью обеспечения возможности определять выполнение требуемых функций безопасности оборудование мониторинга аварийных условий следует проектировать таким образом, чтобы у оператора имелась возможность подтверждения того, что:

— реактор остановлен и остается в состоянии останова;
— остаточное тепло отводится и будет и далее отводиться из активной зоны и от других узлов, важных для безопасности, к конечному поглотителю тепла; и
— любой предусмотренный барьер, предотвращающий выбросы радиоактивных веществ в окружающую среду, функционирует и сохранится в будущем.

6.52. Следует обеспечивать, чтобы параметры станции, контролируемые с целью такого подтверждения, соответствовали проекту и площадке реактора.

6.53. Следует обеспечивать, чтобы оборудование для мониторинга аварийных условий могло функционировать в послеаварийной окружающей среде в случае необходимости и в течение требуемого срока. Следует обеспечивать, чтобы диапазоны измерений выбранных ключевых параметров охватывали значения, которые могут быть достигнуты при событиях, создающих потенциальную угрозу барьерам, препятствующим выбросу радиоактивных материалов из топлива, системе теплопередачи или защитной оболочке, или способных приводить к выбросу радиоактивных материалов с нарушением одного или нескольких этих барьеров.

6.54. Следует обеспечивать, чтобы индикаторы, используемые для послеаварийного мониторинга, отличались от других индикаторов.

6.55. В тех случаях, когда для анализа аварий или аварийных мер требуется информация о прошлых периодах, следует предусматривать возможность регистрации соответствующих данных и последующего доступа к ним.

6.56. На станции следует предусматривать технические средства для передачи соответствующих данных средствам аварийного реагирования, определенным в [13], без необоснованного вмешательства в работы, проводимые в помещении щита управления в условиях аварийной ситуации.

СИСТЕМЫ АВАРИЙНОЙ СИГНАЛИЗАЦИИ

6.57. Системы визуальной и звуковой аварийной сигнализации используются для привлечения внимания операторов к необходимости вмешательства в эксплуатацию станции посредством, например, ручного инициирования функций системы безопасности или инициирования действий по управлению станцией или ее техническому обслуживанию с целью обеспечения того, чтобы состояние станции поддерживалось в пределах, определенных в проектных основах. Приведенные ниже руководящие принципы применяются в случае использования аварийной сигнализации в связи с системами, важными для безопасности.

6.58. Согласно основным требованиям в отношении действий оператора в надлежащих местах следует предусматривать соответствующие визуальные или звуковые аварийные сигнальные устройства, обеспечивающие своевременную подачу сигналов.

6.59. При проектировании аварийных сигнальных систем следует уделять надлежащее внимание обеспечению возможности для операторов выделять существенно важную информацию, особенно в ходе ожидаемых при эксплуатации событий и в аварийных условиях, когда возможно срабатывание большого числа сигнальных устройств. Эта цель может быть достигнута с помощью различных методов, в том числе путем группирования, определения приоритетности и условий срабатывания тревожных сигналов, а также использования звукового или визуального дифференцирования с целью различения тревожных сигналов разных типов и приоритетов.

6.60. Методы предотвращения перегрузки оператора сигнальной информацией не следует применять таким образом, чтобы происходило подавление информации, необходимой для определения места возникновения и возможных последствий неправильного срабатывания.

6.61. Следует предусматривать средства, позволяющие оператору своевременно подтверждать тревожные сигналы по отдельности, либо группами.

6.62. Звуковые аварийные сигналы обычно используются для того, чтобы привлечь внимание оператора к новым тревожным условиям. Следует предусматривать средства подавления этих звуковых сигналов, с тем чтобы избежать перегрузки слуха и облегчить распознавание новых тревожных сигналов, которые могут появляться впоследствии. В случае подавления

тревожных сигналов следует сохранять визуальную индикацию сигнальных условий до тех пор, пока не будут устранены условия отказа, с тем чтобы об этих условиях не возможно было забыть. Для того чтобы отличить сигнальные режимы, получение информации о которых было подтверждено, от сигналов без подтверждения в их получении, следует использовать визуальные средства (изменение цвета индикаторов или изменение режима работы с мигающего на непрерывный). Следует предусматривать, чтобы после возвращения станции в нормальное состояние индикация тревожных сигналов продолжалась до тех пор, пока оператор не выполнит операцию сброса, с тем чтобы сохранялась информация о тревожных сигналах.

СИСТЕМА РЕГИСТРАЦИИ ИСТОРИЧЕСКИХ ДАННЫХ

6.63. Следует предусматривать возможность регистрации, хранения и восстановления данных о важных процессах на станции, посредством которых фиксируется функционирование и история поведения станции. Как правило, такие системы регистрации исторических данных содержат:

— техническую информацию для операторов смен (с указанием краткосрочных и долгосрочных тенденций);
— общую эксплуатационную информацию для административного руководства станции; и
— данные о диагностике и анализе эксплуатации и аварий в краткосрочном и долгосрочном плане.

6.64. Традиционно для реализации этих функций использовались системы, выдающие печатные копии (бумажные распечатки данных). Однако следует рассматривать использование компьютеризованных систем, поскольку они обеспечивают более эффективное хранение, поиск и обработку возникающих обычно больших объемов данных. Как правило, при использовании компьютеризованных систем следует предусматривать удобное расположение принтеров так, чтобы пользователи могли получать печатные копии.

6.65. Терминалы для доступа к исторической информации следует устанавливать в помещении центрального щита управления и при необходимости рядом с ним. Полезными являются удаленные терминалы, удобно расположенные для использования персоналом инженерно-технической поддержки, и следует рассматривать возможность их установки. При принятии решения относительно мест расположения терминалов и при проектировании сопряжений человек-машина для обеспечения доступа к историческим данным

следует учитывать потребности, обязанности и потенциальные возможности пользователей.

7. ПРОЦЕСС ПРОЕКТИРОВАНИЯ СИСТЕМ КИПиУ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ

7.1. Техническое проектирование атомной электростанции – это сложная деятельность, включающая многие технические дисциплины. Для обеспечения соответствия проекта предъявляемым требованиям необходимо обеспечивать своевременное поступление правильной информации по проекту. Для систем, важных для безопасности, следует использовать структурированный процесс разработки, воплощающий консервативные проектные решения и рациональную инженерно-техническую практику с целью обеспечения правильного применения Требований к проектированию [1]. Невыполнение этих требований вследствие плохой организации или неудовлетворительного руководства процессом может поставить под угрозу ядерную безопасность.

ОБЕСПЕЧЕНИЕ КАЧЕСТВА

7.2. Для достижения требуемых стандартов качества важно обеспечивать, чтобы проектирование, изготовление, аттестация, инспектирование, монтаж, эксплуатация, испытания и техническое обслуживание систем КИПиУ, важных для безопасности, осуществлялись в соответствии с программой обеспечения качества, подготовленной теми, кто занимается разработкой проекта, изготовлением или монтажом, и утвержденной соответствующим компетентным органом. Следует обеспечивать, чтобы эта программа соответствовала надлежащему своду положений и руководствам по безопасности ([3], Руководства по безопасности Q3 и Q10).

7.3. Следует предусматривать, чтобы программа обеспечения качества включала все виды деятельности, необходимые 1) для проверки соответствия проекта систем безопасности предъявляемым требованиям и 2) для обеспечения соответствия систем безопасности всем применимым нормам и требованиям.

ПЛАНИРОВАНИЕ ПРОЕКТА

7.4. С целью обеспечения своевременной и коммерчески реализуемой поставки необходимых элементов конструкции следует использовать методы управления проектами и планирования проектов. При осуществлении деятельности по планированию проекта, используемой для осуществления и завершения проекта, следует учитывать требования безопасности проектируемых систем. В графике осуществления проекта следует выделять достаточное время для представления регулирующему органу документации по проектированию систем, важных для безопасности.

КОНТРОЛЬ ИЗМЕНЕНИЙ И УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

7.5. В течение всего процесса проектирования – от разработки концепции до эксплуатации – на любой стадии итерационного процесса следует осуществлять контроль любых предлагаемых модификаций, так, чтобы обеспечивалось управление конфигурацией проекта. Процесс внесения изменений в проект следует документировать, а также следует запрашивать письменное утверждение с целью обеспечения надлежащего рассмотрения предлагаемых изменений и проведения соответствующей оценки независимыми экспертами, не имеющими отношения к разработчику проекта. На ранних стадиях проектирования могут потребоваться многочисленные итерации с целью уточнения требуемого проекта, и зачастую подход к управлению изменениями становится менее формальным. В этом случае следует проводить периодические рассмотрения проекта с целью обеспечения информированности соответствующего не входящего в группу проектировщиков персонала о ходе проектирования и получения подтверждения того, что требования безопасности по-прежнему выполняются. Однако после утверждения проекта следует обеспечивать организацию официального процесса контроля изменений в проекте.

УЧЕТ ЧЕЛОВЕЧЕСКОГО ФАКТОРА

7.6. Ввиду разносторонней и важной роли, которую операторы и другой персонал станции играют в эксплуатации и использовании систем КИПиУ, важных для безопасности (и станции в целом), в общий процесс проектирования следует включать процессы, связанные с учетом человеческого фактора.

7.7. К методам учета человеческого фактора относятся функциональный анализ, анализ заданий и анализ рабочей нагрузки. Они используются при распределении выполняемых функций между людьми и машинами и при проектировании взаимодействия человек-машина. Опубликованы руководящие материалы по инженерному проектированию с учетом человеческого фактора, в частности, по антропометрии, ошибкам человека, проектированию интерфейсов пользователя и различным другим связанным с этим вопросам. В целях использования этих знаний следует применять системный подход к вопросам, связанным с человеческими факторами (см. также раздел 6).

7.8. С целью обеспечения совместимости с пользователями, ясности и эффективности взаимодействия человек-машина следует применять соответствующие принципы проектирования или требования в отношении учета человеческого фактора. Следует обеспечивать, чтобы в процессе проектирования системы учитывались мнения групп пользователей и чтобы в нем предусматривались надлежащие меры по верификации и валидации интерфейсных средств взаимодействия человек-машина. Программу инженерного проектирования с учетом человеческого фактора (как указано в разделе 6) следует включать в общий план проекта. В ходе инженерного проектирования следует систематически документировать анализ и выводы в отношении человеческого фактора в соответствии с имеющимися инженерно-техническими руководствами и справочными материалами по вопросам человеческого фактора.

7.9. Рекомендуется проводить оценку проектных вариантов взаимодействия человек-машина, начиная с первых стадий проектирования и первоначально используя экспериментальные модели и компьютеризованные средства визуализации. На поздних стадиях проектирования для валидации проекта помещения щита управления следует использовать полномасштабный имитатор помещения щита управления.

7.10. При проектировании следует принимать во внимание возможность ошибок человека, связанных как с выполнением, так и с невыполнением соответствующих действий пользователями системы. С целью сведения к минимуму вероятности серьезных неблагоприятных последствий, являющихся результатом пользовательских ошибок, при проектировании следует в максимально возможной степени структурировать взаимодействие человек-машина, с тем чтобы отдельные ошибки оператора не влекли за собой последствий и поддавались обнаружению и корректировке. Ситуации, в которых ошибка человека имеет относительно высокую вероятность возникновения, а в случае возникновения влечет серьезные неблагоприятные

последствия, следует исключать посредством разработки соответствующей структуры системы или проекта интерфейса пользователя, или с помощью средств автоматизации.

ОПИСАНИЕ ПРОЦЕССА ПРОЕКТИРОВАНИЯ

7.11. Разработку систем, важных для безопасности, следует проводить в рамках поэтапного контролируемого процесса. При использовании этого подхода процесс разработки организуется в виде упорядоченного набора конкретных стадий. На каждой стадии используется информация, полученная в ходе более ранних стадий, а итоговая выходная информация используется в качестве исходной на последующих стадиях. Следует иметь в виду, что разработка систем, важных для безопасности, по своему характеру является итерационным процессом. В процессе проектирования ошибки и просчеты, допущенные на более ранних стадиях, становятся очевидными и обусловливают необходимость повторений определенных операций. Существенно важной особенностью этого подхода является то, что результаты каждой стадии разработки следует подвергать верификации на основе требований предыдущей стадии с целью подтверждения правильности проектирования. На некоторых стадиях разработки проводится валидация с целью подтверждения того, что полученный результат (продукт данного конкретного этапа) соответствует всем функциональным и другим требованиям и что непредвиденное поведение не возникает. Следует обеспечивать, чтобы деятельность по верификации и валидации выполнялась независимыми группами, не связанными с разработчиками и проектировщиками.

7.12. Типичные стадии системного процесса разработки и структурная схема процесса, описываемого в настоящем Руководстве по безопасности, показаны на рис. 4. Ячейки отражают виды деятельности по разработке, которые следует выполнять, а стрелки показывают предполагаемую последовательность работ и направление основного потока информации. На рис. 5 показана связь верификации и валидации с требованиями и различными стадиями проектирования и осуществления. Выбор конкретных видов деятельности по разработке и их порядок на этом рисунке и в настоящем Руководстве по безопасности не преследуют цель указать конкретный метод разработки; другие варианты могут в равной степени обеспечивать выполнение рекомендаций относительно принципов и атрибутов.

7.13. Проектирование атомной станции в целом начинается с проектирования механических и технологических систем и элементов станции. Далее на основе

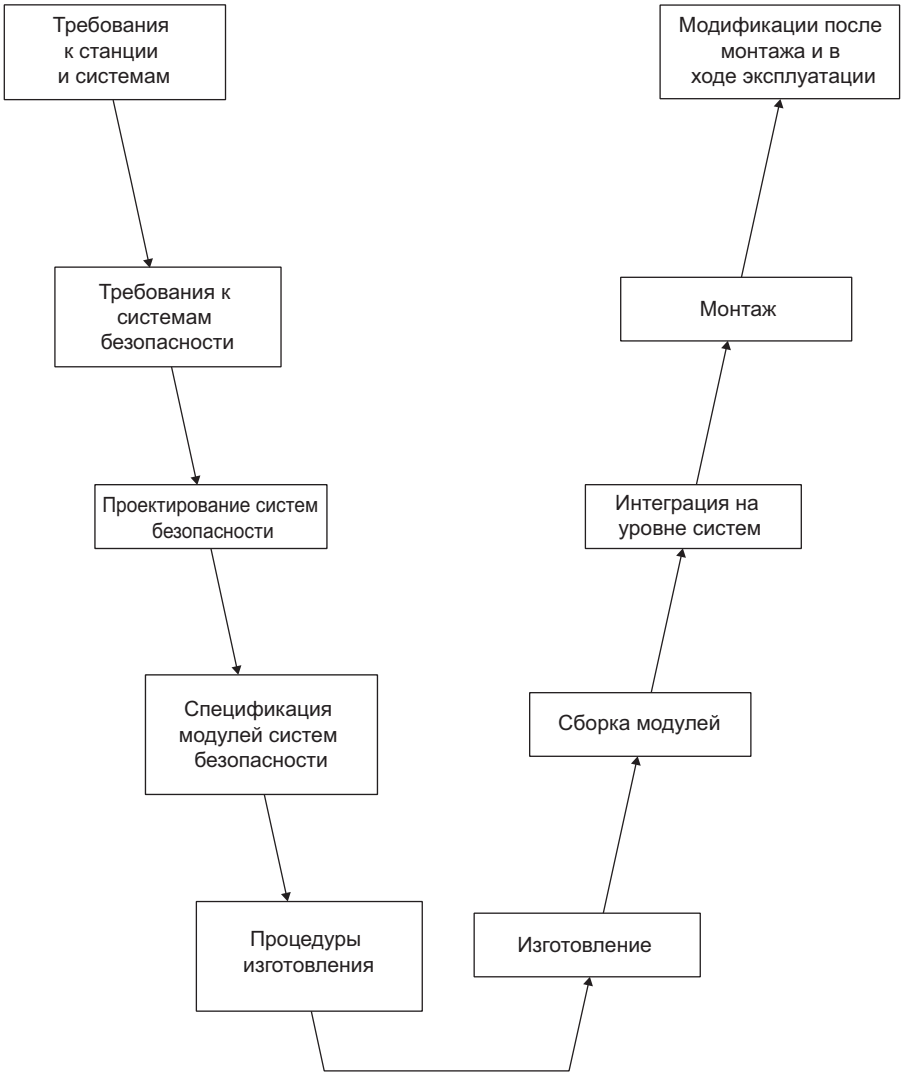

РИС. 4. Разработка системы КИПиУ, важной для безопасности.

результатов (детерминированного и/или вероятностного) анализа безопасности выбранных проектных событий (см. раздел 3) следует разработать проект систем КИПиУ. Следует обеспечивать, чтобы процесс проектирования включал систематический процесс создания перечня выбранных проектных событий, так как упущения могут приводить к неправильному формулированию

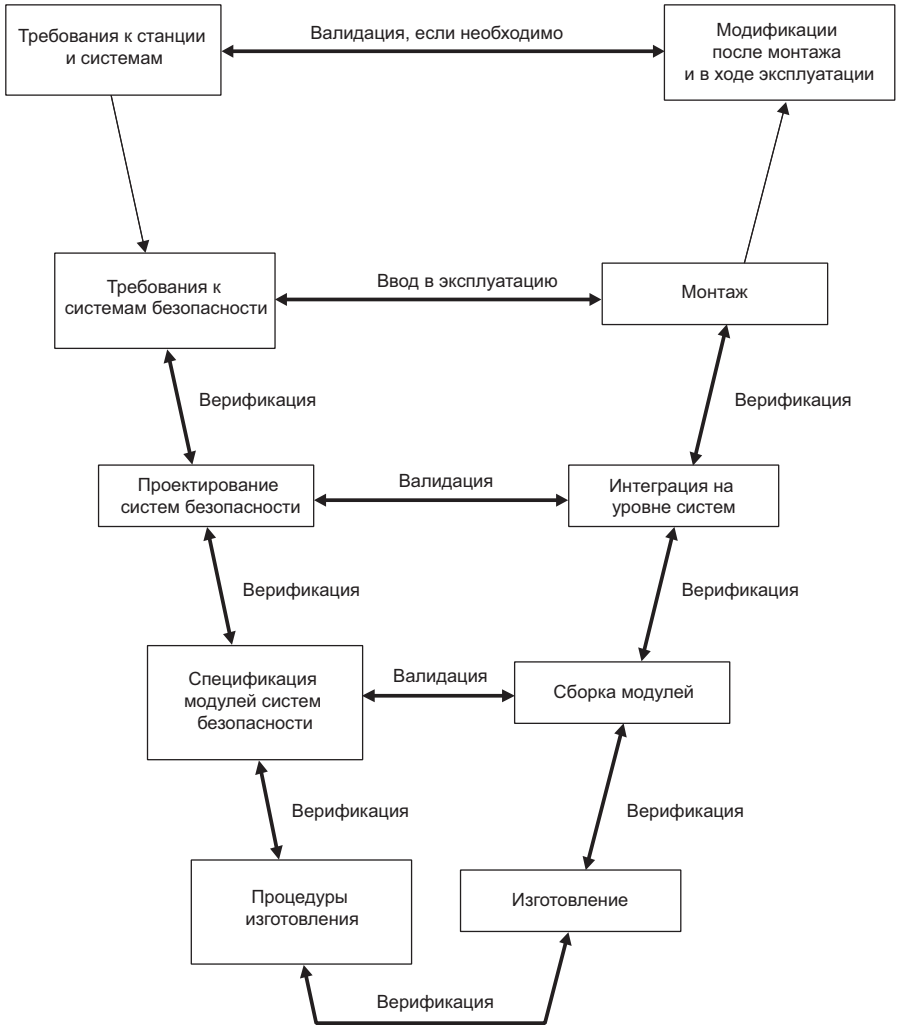

РИС. 5. Процессы верификации, валидации и ввода в эксплуатацию.

требований в отношении мер по обеспечению безопасности, и, тем самым, к небезопасной системе.

7.14. На основе результатов этого анализа выявляются требования к системе безопасности. Специалистам в области ядерной безопасности и других инженерно-технических дисциплин при необходимости следует вносить свой

вклад в определение требований, предъявляемых к системе безопасности. Как правило, в процессе работы возникает необходимость внесения изменений в первоначальный проект и разрабатывается новый вариант проекта, после чего вновь выполняется анализ безопасности. После нескольких циклов повторений достигается конфигурация механических, технологических систем и систем КИПиУ, удовлетворяющая всем современным требованиям ядерной безопасности.

7.15. После того, как разработка проекта достигла стадии, на которой известно, как должны выполняться требования и как будут конфигурированы основные системы и элементы станции, проектную документацию обычно выпускают в виде спецификаций для закупок. При ведении переговоров по контрактам для систем и оборудования станции разработчику проекта следует устанавливать способ связи, который обеспечит возможность продемонстрировать, что осуществление, предложенное поставщиками, удовлетворяет требованиям системы. Разработчику проекта и поставщикам следует обеспечивать эффективное осуществление деятельности по верификации и валидации.

7.16. После определения требований, предъявляемых к системе безопасности КИПиУ, разработчик проекта КИПиУ указывает, как будет выполняться каждое требование, подготавливая проектные требования к системе безопасности КИПиУ. Если предлагается компьютеризованная система, то разработчику проекта следует подготовить требования к компьютерной системе и принять решение относительно архитектуры систем и выполняемых функций. Подобным же образом следует также принимать решение в отношении распределения функций человека и/или машины. На данной стадии проектирования становится понятным, в каких областях проектирования можно полагаться на уже имеющиеся методы, а какие части потребуют специальных усилий по разработке. В тех случаях, когда необходима разработка и требуется макетирование, более эффективными могут оказаться другие модели процессов проектирования, например, спиральная модель.

7.17. По мере осуществления проекта КИПиУ и поступления модулей оборудования, эти модули следует подвергать серии проверок и испытаний с целью подтверждения того, что отдельные модули или подсборки функционируют так, как требуется. Это иллюстрирует рис. 5. Зачастую на этой стадии аттестации оборудования начинаются испытания на уровне модулей или подсборок, и могут проводиться общие или типовые испытания оборудования, которое будет использоваться в нескольких применениях. Затем отдельные модули объединяются в подсистемы с целью выполнения функций, требуемых разработчиком проекта. Следует проводить и другие испытания, специфичные

для конфигурации оборудования, с целью подтверждения совместного функционирования модулей в составе соответствующих подсистем. Впоследствии подсистемы объединяются или интегрируются для обеспечения возможности проведения серии «заводских приемочных испытаний» системы на установках поставщика. Следует обеспечивать, чтобы эти испытания подтверждали правильность реализации функциональных возможностей системы, требуемых разработчиком проекта.

7.18. Если разработчик проекта удовлетворен тем, что система выполняет требующиеся функции на установках поставщика, оборудование отгружается на площадку и монтируется. Собственно операции отгрузки или монтажа могут воздействовать на функционирование оборудования, и поэтому после монтажа следует проводить всеобъемлющие испытания. Следует предусматривать, чтобы эти испытания после монтажа и «завершающие испытания», помимо повторения некоторых из завершающих заводских приемочных испытаний, обеспечивали испытание всей системы в том виде, как она должна работать на практике; например, следует проводить проверку систем с многократным резервированием в условиях реальной совместной работы, а не с использованием моделируемых сигналов. Для системы, требующей длительной программы разводки кабелей, на практике часто представляется нецелесообразным завершать разводку кабелей перед выполнением завершающих испытаний. При таких обстоятельствах, руководствуясь соображениями целесообразности, испытания следует выполнять после того, как сделан репрезентативный выбор всех различных типов соединений с системой. Тем самым будут легко определены и могут быть эффективно решены любые общие проблемы сопряжений. Заключительные испытания следует проводить после полного завершения кабельной разводки системы. На этом этапе система может быть введена в эксплуатацию и может быть продемонстрировано, что она функционирует так, как требуется. Насколько возможно, работы по вводу в эксплуатацию системы КИПиУ и обеспечению ее функционирования следует завершать перед выполнением других работ по вводу в эксплуатацию, для проведения которых может потребоваться функционирование системы КИПиУ.

МОДЕРНИЗАЦИЯ И МОДИФИКАЦИИ

7.19. С целью обеспечения непрерывного и надежного производства электроэнергии на атомных электростанциях и соблюдения на них современных норм безопасности следует периодически проводить модернизацию систем КИПиУ. Атомная промышленность испытывает

проблемы в снабжении запасными частями для аналоговых систем КИПиУ, аппаратные средства которых были разработаны и изготовлены 20–30 лет тому назад. Физическое старение оборудования в сочетании с отсутствием запасных частей привело к повышению интенсивности отказов и затрат на эксплуатацию и техническое обслуживание. Кроме того, ряд поставщиков сократил поддержку аналоговых систем, и есть ряд примеров, когда первоначальный поставщик прекратил свою деятельность. Ввиду значительного повышения надежности цифровой электроники в последние годы, многие атомные энергопредприятия приняли решение о замене старых аналоговых систем КИПиУ компьютеризованными системами.

7.20. Успехи в области цифровой технологии создают следующие дополнительные стимулы к модернизации:

— возможность выполнения более сложных функций;
— возможность достижения большей точности;
— возможность компиляции и использования больших объемов более разнообразной информации;
— интерфейс пользователя может быть сделан более гибким;
— системе легче обнаруживать и устранять ожидаемые внутренние неисправности;
— функциональные изменения могут вноситься без физических изменений или даже физического доступа;
— во многих применениях могут использоваться стандартные процессоры известной надежности.

7.21. В тех случаях, когда компьютеризованная система является составной частью модификации или модернизации, следует рассматривать ее функцию в обеспечении безопасности атомной электростанции. В соответствии с критериями, изложенными в разделе 2, следует выполнить классификацию безопасности системы КИПиУ. Требования по надежности системы, аттестации и обеспечению качества и другие требования определяются в соответствии с классификацией безопасности.

7.22. Исходя их практической целесообразности, в качестве первого шага следует готовить спецификацию имеющейся системы плюс спецификацию новых или измененных системных требований. Проектная документация имеющейся аналоговой системы может быть неполной и неточной. Может оказаться необходимым проведение определенного «инженерного анализа» с целью восстановления технических требований к проектированию и требований в результате осуществления конструктивных решений.

7.23. Выгоды, получаемые при изменении интерфейса оператора и/или стратегий управления, следует сопоставлять с потенциальными затратами. Усовершенствования интерфейса оператора могут потребовать значительной модификации панелей и переподготовки операторов и обслуживающего персонала. Кроме того, перед выбором интерфейса оператора следует проконсультироваться с операторами помещения щита управления, и от них также следует получать информацию для проектной группы на различных стадиях процесса разработки.

7.24. Подробную информацию относительно модернизации КИПиУ можно найти в [15, 16].

АНАЛИЗ, ТРЕБУЮЩИЙСЯ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ

Анализ отказов

7.25. На соответствующих стадиях процесса проектирования следует выполнять анализ систем безопасности с целью проверки того, что комплекс основных подсистем (системы защиты, исполнительных систем безопасности и вспомогательных средств систем безопасности) может на постоянной основе обеспечивать выполнение рекомендаций настоящего Руководства по безопасности в том, что касается единичных отказов (см. раздел 4) и отказов по общей причине, а также любых других требований по надежности систем безопасности. Следует также проводить анализ видов отказов с целью подтверждения требований в отношении отказобезопасного проектирования. Результаты проведенного анализа следует документировать.

Оценка положений об испытаниях

7.26. Следует проводить оценку окончательного проекта с целью проверки адекватности положений по испытаниям системы защиты, исполнительных систем безопасности и вспомогательных средств систем безопасности. Результаты этой оценки следует документировать, и в документации следует определять те области проекта, которые чувствительны либо к отказу оборудования, либо к ошибке человека в любом аспекте испытаний системы и оборудования.

Анализ надежности

7.27. В государстве-члене, в котором принимается решение использовать численные требования по надежности систем безопасности или их частей, следует выполнять соответствующий количественный анализ надежности с использованием достоверных интенсивностей отказов элементов и средних времен восстановления, с тем чтобы:

— учесть случайные отказы оборудования;
— учесть отказы по общей причине, включая ошибки человека;
— установить относительную важность для надежности частей систем безопасности;
— установить первоначальные промежутки между испытаниями в соответствии с применимыми показателями отказов элементов и требованиями к надежности системы;
— подтвердить в ходе эксплуатации станции, что показатели обнаружения отказов соответствуют значениям, принятым в допущениях, и что достигаются целевые показатели надежности;
— определить меры, подлежащие принятию в том случае, если фактические интенсивности отказов превышают интенсивности отказов, принятые в проекте, или оказываются ниже их; например, путем уменьшения или увеличения интервалов между испытаниями или замены тех элементов, которые не позволяют достигнуть целевых показателей надежности.

7.28. Результаты этого анализа, а также результаты периодических испытаний, оценок надежности при эксплуатации и любых принятых восстановительных мер следует документировать.

ВЕРОЯТНОСТНАЯ ОЦЕНКА БЕЗОПАСНОСТИ

7.29. Информацию, полученную в результате проведения вероятностных оценок безопасности (ВОБ), следует учитывать при проектировании с целью обеспечения того, чтобы ни один из факторов не вносил непропорционально большого или неопределенного вклада в совокупный риск. Подробную информацию относительно ВОБ можно найти в [17-20].

ДОПУЩЕНИЯ, ПРИНИМАЕМЫЕ ПРИ АНАЛИЗЕ

7.30. Допущения, сделанные при любом анализе, требуемом для проверки правильности проектирования, следует включать в комплект документации для данного анализа. Каждое допущение следует четко излагать и обосновывать.

ДОКУМЕНТАЦИЯ ДЛЯ СИСТЕМЫ КИПиУ

7.31. Документация по системе КИПиУ имеет следующее назначение: 1) обеспечивать передачу информации между различными стадиями и различными сторонами, участвующими в процессе проектирования; 2) служить документом, показывающим, что требования были правильно интерпретированы и выполнены в установленной системе; 3) предоставлять операторам станции информацию, важную для эксплуатации и связанную с проектированием; и 4) обеспечивать основу для технического обслуживания станции и для будущих возможных пересмотров проекта.

7.32. Для системы КИПиУ, важной для безопасности, в рамках различных видов деятельности, связанных с процессом проектирования, готовится значительное число документов. С целью обеспечения надлежащего учета важности этих документов их следует группировать на основе их роли в процессе проектирования.

7.33. Первичные документы – это документы, являющиеся неотъемлемой частью процесса проектирования и представляющие собой входные и выходные документы для каждой стадии. Ошибка в этих документах может непосредственно привести к неисправности в самой системе. Первичная документация обычно включает документацию по проектным основам для цели анализа безопасности станции, документацию по требованиям к системам безопасности, логические схемы и чертежи изготовителя оборудования.

7.34. Вторичные документы – это те документы, которые связаны с процессом проектирования и используются разработчиком проекта при подготовке входной и выходной документации. Ошибка в этих документах не приводит непосредственно к неисправности в системе, но может затруднить выявление имеющейся неисправности ввиду неправильного представления информации. В других случаях принятие мер в соответствии с неправильными рекомендациями документа может приводить к возникновению неисправности в системе. Как правило, во вторичных документах определены и зафиксированы виды деятельности, связанные с процессом проектирования,

такие, как деятельность по верификации и валидации между стадиями. Регистрационные записи по верификации и валидации используются для определения необходимости изменения документации на связанных с ней стадиях при обнаружении неисправностей.

7.35. Другие документы в программах обеспечения качества, планирования проектов и аттестации оборудования являются вспомогательными для процесса проектирования. Эти вспомогательные документы способствуют принятию организационных, логистических и стратегических решений в связи с процессом проектирования, которые могут оказывать косвенное влияние на проектирование.

7.36. Следует обеспечивать, чтобы к моменту завершения проекта системы КИПиУ, важной для безопасности, была полностью подготовлена вся документация. Следует обеспечивать, чтобы документация была всеобъемлющей, полной, доступной для анализа и поддающейся контролю и подтверждала требующиеся функциональные возможности и совокупную надежность системы. Надлежащая документация облегчит будущие модификации или модернизацию системы.

7.37. Следует обеспечивать, чтобы по окончании проектирования систем КИПиУ окончательный вариант проектной документации включал перечень соответствующих документов по проекту, верификации и валидации проекта, а также конкретные справочные материалы для этих документов.

7.38. Следует обеспечивать постоянное обновление документации для системы КИПиУ и отражать в документации любые модификации системы. В отношении всех документов для системы КИПиУ следует постоянно осуществлять меры по управлению конфигурацией.

Своды положений и нормы

7.39. В начале осуществления проекта следует согласовывать, документировать и в ходе осуществления проекта сообщать соответствующему компетентному органу перечень руководств, сводов положений и норм, применяемых при проектировании системы КИПиУ, важной для безопасности, а также соответствующие показатели соблюдения.

Документирование проектных основ

7.40. Окончательные основы проекта следует документировать. Следует обеспечивать, чтобы эти сведения включали как минимум идентификацию и документирование:

— эксплуатационных состояний станции, в которых должна работать система;
— ПИС с идентификацией соответствующих задач обеспечения безопасности и защиты для систем КИПиУ, наряду с начальными условиями ПИС и допустимыми пределами условий на станции для каждого такого события;
— отдельных параметров или комбинаций параметров, которые должны контролироваться для управления каждым защитным действием вручную или автоматически (либо и в том, и другом режиме одновременно);
— диапазонов и скоростей изменения этих параметров или комбинаций параметров, с которыми должны работать системы КИПиУ, важные для безопасности;
— предельных значений для активации систем безопасности по каждому из этих параметров в каждом применимом режиме эксплуатации станции;
— ограничений для системы управления, связанных с допустимыми значениями параметров процесса и других важных параметров.

7.41. Следует документировать критические точки во времени или критические точки в условиях на станции, которые определяют действия системы после начала проектного события, включая:

— время или условия на станции, при которых требуется инициирование функции безопасности;
— время или условия на станции, при которых требуется запуск автоматического управления функциями безопасности;
— время или условия на станции, определяющие надлежащее завершение выполнения функции безопасности;
— время или условия на станции, при которых возможно возвращение системы безопасности в нормальное состояние готовности.

7.42. Следует документировать методы, используемые при определении того, что надежность конструкции системы безопасности соответствует каждой функции системы безопасности и любым качественным или количественным целям надежности, которые могут задаваться при проектировании системы.

7.43. Следует документировать любые специальные ограничения, связанные с шириной полосы частот (такие, как требуемые частоты выборки и скорости передачи данных), влияющие на проектирование системы.

7.44. Для каждой установленной задачи обеспечения защиты, которая может выполняться вручную с самого начала или после инициирования, следует документировать:

— время и условия на станции, при которых разрешается ручное управление;
— обоснование разрешения на инициирование или управление после инициирования с использованием исключительно ручных средств;
— диапазон окружающих условий, воздействующих на оператора в эксплуатационных состояниях и аварийных условиях станции, в котором требуется выполнение ручных операций;
— упомянутые выше параметры, которые необходимо отображать на индикаторах, с тем чтобы оператор мог учитывать их при выполнении действий вручную.

7.45. Для тех эксплуатационных состояний и аварийных условий на станции, в которых должны функционировать системы, важные для безопасности, следует определять и документировать диапазон переходных и стационарных условий (таких, как напряжение и частота) вспомогательных средств систем безопасности.

7.46. Для эксплуатационных состояний и аварийных условий на станции и для внешних событий следует документировать диапазон переходных и стационарных окружающих условий (таких, как условия излучения, температура, влажность, давление и вибрация), в которых должны функционировать системы, важные для безопасности.

7.47. Следует документировать условия, способные приводить к ухудшению функциональных характеристик систем безопасности, с учетом которых предусматриваются меры по сохранению способности выполнения функций безопасности (например, воздействие летящих предметов, разрывы трубопроводов, пожары, отказ вентиляции, ложное срабатывание систем пожаротушения, ошибки оператора, отказ систем различных классов безопасности).

7.48. Следует указывать те условия на станции, при которых разрешается байпасирование задач обеспечения безопасности. Следует также описывать

средства осуществления таких разрешенных байпасов, наряду с существенно важными индикаторами.

7.49. Следует документировать регламентируемые процессы технического проектирования систем и элементов и определения соответствующих технических условий.

Документирование проекта системы КИПиУ

7.50. Следует документировать проектирование систем КИПиУ, важных для безопасности. Следует обеспечивать, чтобы эта документация включала как минимум следующую информацию:

Функции

7.51. Каждую систему КИПиУ следует классифицировать, как указано в разделе 2.

7.52. Следует документировать основы проекта каждой системы, включая ее связанные с безопасностью функциональные обязанности, сопряжения с другими системами, и ПИС и условия на станции, при которых исполняются связанные с безопасностью функциональные обязанности.

7.53. Следует документировать функции, обеспечиваемые каждым каналом КИПиУ. Это включает документы по характеристикам и в соответствующих случаях по запасам устойчивости индикаторов, тревожных сигналов и органов управления.

7.54. В случае задач обеспечения защиты в документацию следует включать точное и ясное описание условий на станции и индикаторов тех условий, достижение которых определяет выполнение задачи обеспечения защиты.

Характеристики

7.55. Для всей системы и для каждого канала следует приводить описание требуемого диапазона, точности и времени реакции.

7.56. Следует предоставлять документацию, подтверждающую требования к аттестации, функциональным характеристикам и любые другие специальные требования к системе и ее элементам.

7.57. В состав документации следует включать перечень оборудования системы КИПиУ, важной для безопасности, характеристики которого могут не отвечать функциональным требованиям системы в течение полного срока службы станции, в том числе критерии, определяющие окончание срока службы оборудования и ожидаемый срок службы.

7.58. Для систем безопасности (т.е. системы защиты, исполнительной системы безопасности и вспомогательных средств систем безопасности) следует приводить информацию о значениях максимального разрешенного и ожидаемого времени выполнения требующихся функций безопасности.

7.59. Следует приводить описание операций по анализу системы безопасности, определенных в пунктах 7.25–7.28, со ссылкой на соответствующую проектную документацию.

Аттестация

7.60. Следует приводить описание окружающих условий, в которых должен работать каждый элемент, включая нормальные условия, ожидаемые при эксплуатации события и условия проектной аварии.

7.61. Следует указывать источник или источники электропитания, от которых каждая система будет запитываться в нормальных условиях, ожидаемых при эксплуатации событиях и условиях проектной аварии.

7.62. Следует обеспечивать верификацию требований по аттестации каждого элемента или системы.

Испытания и техническое обслуживание

7.63. Следует предусматривать график испытаний, инспекций и периодического технического обслуживания, проводимых с целью обеспечения требуемой готовности оборудования.

7.64. Следует указывать требования, имеющие отношение к испытаниям, техническому обслуживанию и инспекциям, наряду с данными о любом потенциальном ухудшении, риске или деградации, которые могут возникать в результате выполнения такой деятельности.

Эксплуатация

7.65. Следует приводить описание принципов эксплуатации системы во всех эксплуатационных состояниях. В этом описании следует указывать соответствующие сигналы и требуемые автоматические действия или действия, выполняемые оператором.

7.66. Следует обеспечивать наличие инструкций по эксплуатации и инструкций по техническому обслуживанию.

Процедуры и инструкции

7.67. Следует указывать ссылки на инструкции по эксплуатации, вводу в эксплуатацию и техническому обслуживанию, связанные с системой.

Запасные части

7.68. Для каждого элемента следует иметь технические требования на закупку.

7.69. С целью обеспечения использования проектных основ в будущем следует документировать критерии и обоснование выбора запасных частей.

7.70. Следует обеспечивать выполнение требований к документации по обеспечению качества, изложенных в нормах безопасности МАГАТЭ по обеспечению качества. (Дополнительные руководящие материалы см. в [3], Руководствах по безопасности Q3 и Q10.)

Организация документации

7.71. Документацию следует организовывать в соответствии с указанной ниже структурой:

— функции, выполняемые системой, и ее функциональное проектирование;
— проектные решения системы;
— предусмотренные в системе средства испытаний, диагностики и технического обслуживания, и их эксплуатация;
— документирование результатов испытаний;
— аттестация оборудования;
— процесс проектирования и требования к качеству, использованные при проектировании;
— стратегии технического обслуживания;

— стратегии ввода в эксплуатацию;
— методы верификации и валидации проекта;
— эксплуатация системы;
— программы технического обслуживания, надзора и периодических испытаний;
— снабжение запасными частями и/или элементами.

Документация по системе КИПиУ

7.72. По завершении проектирования системы КИПиУ, важной для безопасности, следует документировать данные по ожидаемым эксплуатационным характеристикам и надежности системы. Следует обеспечивать, чтобы эта документация включала как минимум следующую информацию:

— краткое описание проектных основ, обоснование изменений проекта, включая учет результатов рассмотрения опыта эксплуатации (если это применимо), функциональное проектирование системы и важнейшие принципы, лежащие в основе выбора конкретной конструкции;
— полное описание системы, в которое следуют включать информацию обо всех контролируемых переменных (параметрах процесса, сигналах оператора) и регулируемых параметрах (выходных сигналах на исполнительные устройства и индикаторы) для всех эксплуатационных режимов системы. Следует предусматривать, чтобы это описание также включало методы представления данных (например, методы с жесткими алгоритмами или компьютеризованные методы);
— подробные сведения о любой зависимости от эксплуатационных характеристик любой сопряженной системы, исполнительных систем безопасности, прочих вспомогательных средств связанных с безопасностью систем или систем безопасности, включая источники электропитания;
— параметры или комбинации параметров и используемые методы комбинирования, которые подлежат мониторингу для целей принятия защитного действия. Следует обеспечивать, чтобы приводимая информация включала данные о минимальном количестве и местах расположения датчиков, необходимых для надлежащего мониторинга всех важных для безопасности параметров, в том числе тех из них, которые имеют пространственную зависимость (т.е. измеренные величины которых изменяются как функция положения в конкретной зоне, как в случае нейтронного потока). Следует указывать расчетные

диапазоны и скорости изменения упомянутых ранее параметров или комбинаций параметров;
— число каналов системы КИПиУ, их функции и логика обработки сигналов, а также информацию об индикаторах, сигнальных устройствах и регулировочных характеристиках, включая запасы безопасности, рабочие допуска и запасы устойчивости;
— в описании системы следует указывать места расположения (например, на плане станции с указанием отметки высоты, номера помещения или номера зоны) датчиков, стоек, корпусов, панелей, органов управления и индикаторов оператора, а также средств ручной настройки и испытаний системы;
— ПИС с указанием соответствующих задач обеспечения защиты и безопасности;
— параметры или комбинации параметров, которые подлежат мониторингу для целей принятия защитных действий при каждом проектном событии;
— предельные уставки системы безопасности для каждого из перечисленных параметров, в каждом применимом режиме эксплуатации станции, включая все условия технологических и ремонтных байпасов и любые допуски на погрешность калибровки приборов. Следует определять, наряду с соответствующей информацией для интерпретации, запас между уставками системы безопасности и уровнем, который, как считается, отмечает начало небезопасных режимов;
— максимально разрешенные значения времени реакции систем безопасности, необходимые для выполнения всех задач обеспечения защиты и безопасности;
— критерий надежности для каждой задачи обеспечения защиты;
— условия, достижение которых определяет выполнение задачи обеспечения защиты;
— номинальные уставки системы безопасности для каждого параметра или комбинации параметров;
— диапазон, срок службы и ожидаемая точность для каждого узла оборудования системы безопасности;
— анализ проекта согласно пунктам 7.25–7.28;
— документацию по проверке требований к аттестации и функциональным характеристикам и любых других специальных требований к оборудованию систем безопасности;
— перечень такого оборудования в системе безопасности, рабочие характеристики которого могут не соответствовать функциональным требованиям к системе в течение всего срока службы станции. Следует указывать критерии, определяющие окончание срока службы оборудования и предполагаемый срок службы;

— перечень применимых сводов положений и норм для проектирования системы безопасности;
— условия на станции, при которых разрешается байпас определенных задач обеспечения безопасности (применимые разрешающие условия см. в пунктах 5.36–5.38).

Настоящая публикация была заменена публикацией SSG-39.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

[1] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Безопасность атомных электростанций: проектирование, Серия норм безопасности № NS-R-1, МАГАТЭ, Вена (2003).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[3] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Обеспечение качества для безопасности атомных электростанций и других ядерных установок, Свод положений и руководства по безопасности Q1-Q14, Серия изданий по безопасности, № 50-C/SG-Q, МАГАТЭ, Вена (1998).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion, Safety Series No. 50-P-1, IAEA, Vienna (1990).

[6] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Противопожарная защита атомных станций, Серия изданий по безопасности № 50-SG-D2 (Rev. 1), МАГАТЭ, Вена (1998).

[7] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Защита от образующихся в результате аварий летящих предметов и от их вторичных воздействий на атомных электростанциях, Серия изданий по безопасности № 50-SG-D4, МАГАТЭ, Вена (1981).

[8] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Учет внешних событий, связанных с деятельностью человека, при проектировании атомных электростанций, Серия изданий по безопасности № 50-SG-D5 (Rev. 1), МАГАТЭ, Вена (1997).

[9] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Конечный поглотитель тепла и непосредственно связанные с ним системы передачи тепла на атомных электростанциях, Серия изданий по безопасности № 50-SG-D6, МАГАТЭ, Вена (1982).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).

[11] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Системы аварийного энергоснабжения атомных электростанций, Серия изданий по безопасности № 50-SG-D7 (Rev. 1), МАГАТЭ, Вена (1993).

[12] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Вопросы радиационной защиты в проектах атомных электростанций, Серия изданий по безопасности № 50-SG-D9, МАГАТЭ, Вена (1988).

[13] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Готовность и реагирование в случае ядерной или радиационной аварийной ситуации, Серия норм безопасности № GS-R-2, МАГАТЭ, Вена (2003).

[14] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Проектирование и аттестация сейсмостойких конструкций для атомных станций, Серия изданий по безопасности № 50-SG-D15, МАГАТЭ, Вена (1997).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Modernization of Instrumentation and Control in Nuclear Power Plants, IAEA-TECDOC-1016, IAEA, Vienna (1998).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Specifications of Requirements for Upgrades Using Digital Instrumentation and Control Systems, IAEA-TECDOC-1066, IAEA, Vienna (1999).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Series No. 50-P-10, IAEA, Vienna (1995).

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public, Safety Series No. 50-P-12, IAEA, Vienna (1996).

ГЛОССАРИЙ

Для целей настоящей публикации применяются следующие определения.

Аварийные условия (accident conditions). Отклонения от нормальной эксплуатации более серьезные, чем ожидаемые при эксплуатации события, включая проектные аварии и тяжелые аварии.

Байпас (bypass). Устройство для преднамеренной, однако временной отмены функционирования цепи или системы, например, путем замыкания накоротко контактов реле.

Ремонтный байпас (maintenance bypass). Байпас оборудования системы безопасности во время проведения работ по техническому обслуживанию, испытаний или ремонта.

Технологический байпас (operational bypass). Байпас некоторых защитных действий, когда они не являются необходимыми в данном режиме эксплуатации станции[4].

Валидация (validation). Процесс определения пригодности продукта или услуги для удовлетворительного выполнения определенных функций. Например, в случае такой системы, как система КИПиУ, процесс подтверждения того, что система целиком (аппаратные средства и программное обеспечение) соответствует всем предъявляемым к ней функциональным и другим требованиям и не обнаруживает никакого нештатного поведения.

Верификация (verification). Процесс определения соответствия качества или характеристик продукта или услуги тому, что предписывается, предопределяется или требуется. Например, в случае процесса разработки процесс, имеющий целью обеспечить, чтобы данный этап процесса разработки удовлетворял требованиям, введенным на предыдущем этапе.

Время реакции (response time). Время, необходимое для достижения элементом определенного состояния на выходе после получения сигнала, обусловливающего переход к этому состоянию на выходе.

---

[4] Технологический байпас может использоваться в случаях, когда защитное действие мешает или может мешать надежной эксплуатации в требующемся режиме.

Вспомогательные средства системы безопасности (safety system support features). Комплект оборудования, который обеспечивает такие виды обслуживания, как охлаждение, смазка и подача энергии, необходимые для системы защиты и систем обслуживания устройств безопасности[5].

Готовность (availability). Отрезок времени, в течение которого система способна выполнять поставленную задачу.

Группа безопасности (safety group). Группа оборудования, предназначенная для выполнения всех действий, требующихся в случае конкретного постулируемого исходного события, с целью обеспечить невозможность превышения пределов, установленных в проектных основах для ожидаемых при эксплуатации событий и проектных аварий.

Действие по обеспечению безопасности (safety action). Одноразовое действие, совершенное системой обслуживания устройств безопасности (исполнительной системой безопасности) [6].

Единичный отказ (single failure). Отказ, который приводит к потере способности элемента выполнять предписанные ему функции безопасности, а также любые последующие отказы, являющиеся результатом этого.

Жизненный цикл системы (system life-cycle). Все стадии эволюции системы от разработки концепции до окончательной утилизации.

Задача обеспечения защиты (protective task). Формирование как минимум тех защитных действий, которые необходимы для выполнения задачи обеспечения безопасности, обусловленной возникновением данного постулируемого исходного события.

---

[5] После постулируемого исходного события срабатывание некоторых требующихся вспомогательных средств системы безопасности может быть инициировано системой защиты, а срабатывание других средств может инициироваться системами обслуживания устройств безопасности, которые обслуживают их; инициирование срабатывания других требующихся вспомогательных средств системы безопасности может не считаться необходимым, если они находятся в задействованном состоянии во время постулируемого исходного события.

[6] Например, введение регулирующего стержня, закрытие клапанов защитной оболочки (контейнмента) или срабатывание аварийных подпиточных насосов.

Задача обеспечения безопасности (safety task). Контроль одного или нескольких параметров, указывающих на возникновение конкретного постулируемого исходного события, обработка сигналов, инициирование и выполнение действий по обеспечению безопасности, требующихся для предотвращения превышения пределов, установленных в проектных основах, а также инициирование и выполнение определенных обслуживающих действий, осуществляемых вспомогательными средствами системы безопасности.

Защитное действие (protective action). Выполняемое системой защиты действие, требующее срабатывания конкретного исполнительного устройства безопасности.

Исполнительное оборудование (actuated equipment). Узел, состоящий из первичных двигателей и управляемого оборудования, используемого для выполнения одной или нескольких задач обеспечения безопасности.

Исполнительное устройство (actuation device). Элемент, который непосредственно управляет движущей силой исполнительного оборудования. Примерами исполнительных устройств являются выключатели и реле, которые управляют распределением и использованием электроэнергии и работой клапанов управления, регулирующих подачу рабочих жидкостей или газовых рабочих сред.

Канал (channel). Совокупность взаимосвязанных элементов в системе, которая выдает один выходной сигнал. Канал теряет свою идентичность, когда сигналы одного выхода объединяются с сигналами, поступающими от других каналов, например, от контрольно-измерительного канала или канала обслуживания устройств безопасности.

Контроль качества (quality control). Часть мер по обеспечению качества, включающая проверку того, что конструкции, системы и элементы соответствуют предъявляемым требованиям.

Логика/логическая схема (logic). Процесс формирования требуемого двоичного выходного сигнала из множества двоичных входных сигналов по заранее определенным правилам, или устройство, используемое для получения этого сигнала.

Мультиплексирование (multiplexing). Передача и прием двух или более сигналов или сообщений по одному каналу передачи данных, например,

посредством временного разделения, частотного разделения или импульсно-кодовых методов.

Надежность (reliability). Вероятность того, что система или элемент будет удовлетворять минимальным требованиям в отношении рабочих характеристик, когда это требуется.

Неодинаковость (diversity). Наличие двух или более резервных систем или элементов для выполнения одной определенной функции, при которой разные системы или элементы наделяются различными признаками таким образом, чтобы уменьшалась возможность отказа по общей причине.

Нормальная эксплуатация (normal operation). Эксплуатация в рамках регламентированных эксплуатационных пределов и условий.

Обеспечение качества (quality assurance).Планируемые и систематически проводимые мероприятия, необходимые для обеспечения достаточной уверенности в том, что изделие, процесс или услуга будут удовлетворять заданным требованиям к качеству, например требованиям, указанным в лицензии.

Общая надежность (dependability). Общий термин, применяемый для обозначения общей надежности системы; т.е. степень, в которой этой системе можно оправданно доверять. Надежность, готовность и безопасность – это атрибуты общей надежности.

Ожидаемые при эксплуатации события (anticipated operational occurrences). Отклонение эксплуатационного процесса от нормальной эксплуатации, которое предположительно может произойти как минимум один раз в течение срока службы (жизненного цикла) установки, но которое благодаря соответствующим предусмотренным в проекте мерам не нанесет значительного повреждения узлам, важным для безопасности, и не приведет к аварийным условиям.

Отказ по общей причине (common cause failure). Отказ двух или более конструкций, систем или элементов вследствие единичного конкретного события или причины.

Первичный двигатель (prime mover). Элемент, который преобразует энергию в действие при получении команды с исполнительного устройства.

Постулируемое исходное событие (postulated initiating event). Событие, определяемое на стадии проектирования как способное привести к ожидаемым при эксплуатации событиям или аварийным условиям.

Пределы безопасности (safety limits). Пределы эксплуатационных параметров, в которых, как показано, имеющая официальное разрешение установка является безопасной.

Проектная авария (design basis accident). Аварийные условия, с учетом которых проектируется атомная электростанция в соответствии с установленными проектными критериями и при которых повреждение топлива и выбросы радиоактивного материала находятся в разрешенных пределах.

Резервирование (redundancy). Использование альтернативных (одинаковых или неодинаковых) конструкций, систем или элементов таким образом, чтобы все они могли выполнять требующуюся функцию независимо от эксплуатационного состояния или выхода из строя любого из них.

Система безопасности (safety system). Система, важная для безопасности, обеспечивающая безопасный останов реактора или отвод остаточного тепла из активной зоны, либо ограничивающая последствия ожидаемых при эксплуатации событий и проектных аварий.

Система защиты (protection system). Система, которая контролирует эксплуатацию реактора и которая при обнаружении ненормального условия (состояния) автоматически включает действия, направленные на предотвращение небезопасного или потенциально небезопасного режима.

Система контрольно-измерительных приборов и управления (КИПиУ), связанная с обеспечением безопасности (safety related instrumentation and control (I&C) system). Система КИПиУ, важная для безопасности, которая не является частью системы безопасности.

Система обслуживания устройств безопасности (safety actuation system). Комплекс оборудования, необходимого для выполнения требуемых действий по обеспечению безопасности, инициируемых системой защиты.

Совпадение (coincidence). Особенность конструкции системы защиты, которая заключается в том, что для выработки логической схемой сигнала

защитного действия требуются два или более накладывающихся друг на друга или одновременно поступающих выходных сигнала из нескольких каналов.

Узел, важный для безопасности (item important to safety). Узел, который является частью группы безопасности и/или неисправность или отказ которого может привести к радиационному облучению персонала на площадке или лиц из населения.

Управляемое оборудование (driven equipment). Элемент, такой, как насос или клапан, который управляется первичным двигателем.

Физическое разделение (physical separation). Разделение с использованием геометрических факторов (расстояние, ориентация и т.п.) посредством соответствующих барьеров или сочетанием указанных мер.

Функциональное разделение (functional isolation). Предотвращение влияния режима эксплуатации или отказа одной схемы или системы на другую схему или систему.

Функция безопасности (safety function). Конкретная цель, которая должна быть достигнута для обеспечения безопасности.

Эксплуатационные состояния (operational states). Состояния, соответствующие определениям нормальной эксплуатации и ожидаемых при эксплуатации событий.

Элемент (component). Отдельный компонент системы. Примерами являются провода, транзисторы, интегральные схемы, двигатели, реле, соленоиды, трубопроводы, арматура, насосы, резервуары и клапаны.

Ядерная безопасность (nuclear safety). Достижение надлежащих эксплуатационных условий, предотвращение аварий или смягчение последствий аварии, благодаря чему обеспечивается защита работников, населения и окружающей среды от чрезмерной радиационной опасности.

СОСТАВИТЕЛИ И РЕЦЕНЗЕНТЫ

Anani, N.	Совет по контролю за использованием атомной энергии, Канада
Bock, H.W.	Siemens, Германия
Duong, M.	Международное агентство по атомной энергии
Faya, A.	Совет по контролю за использованием атомной энергии, Канада
Hughes, P.J.	Инспекция по ядерным установкам, Соединенное Королевство
Johnson, G.L.	Ливерморская национальная лаборатория им. Лоуренса, Соединенные Штаты Америки
MacBeth, M.	Atomic Energy of Canada Ltd, Канада
Pachner, J.	Международное агентство по атомной энергии
Pauksens, J.	Atomic Energy of Canada Ltd, Канада
Rollinger, F.	Institut de Protection et de Sûreté Nucléaire,Франция

Настоящая публикация была заменена публикацией SSG-39.

ОРГАНЫ, УЧАСТВУЮЩИЕ В ОДОБРЕНИИ НОРМ БЕЗОПАСНОСТИ

Комитет по нормам ядерной безопасности

Аргентина: Sajaroff, P.; *Бельгия:* Govaerts, P. (председатель); *Бразилия:* Salati de Almeida, I.P.; *Канада:* Malek, I.; *Китай:* Zhao, Y.; *Франция:* Saint Raymond, P.; *Германия:* Wendling, R.D.; *Индия:* Venkat Raj, V.; *Италия:* Del Nero, G.; *Япония:* Hirano, M.; *Республика Корея:* Lee, J.-I.; *Мексика:* Delgado Guardado, J.L.; *Нидерланды:* de Munk, P.; *Пакистан:* Hashimi, J.A.; *Российская Федерация:* Баклушин, Р.П.; *Испания:* Mellado, I.; *Швеция:* Jende, E.; *Швейцария:* Aberli, W.; *Украина:* Миколайчук, О.; *Соединенное Королевство:* Hall, A.; *Соединенные Штаты Америки:* Murphy, J.; *МАГАТЭ:* Hughes, P. (координатор); *Европейская комиссия:* Gómez-Gómez, J.A.; *Международная организация по стандартизации:* d'Ardenne, W.; *Агентство по ядерной энергии ОЭСР:* Royen, J.

Комиссия по нормам безопасности

Аргентина: D'Amato, E.; *Бразилия:* Caubit da Silva, A.; *Канада:* Bishop, A., Duncan, R.M.; *Китай:* Zhao, C.; *Франция:* Lacoste, A.-C., Gauvain, J.; *Германия:* Renneberg, W., Wendling, R.D.; *Индия:* Sukhatme, S.P.; *Япония:* Suda, N.; *Республика Корея:* Kim, S.-J.; *Российская Федерация:* Вишневский, Ю.Г.; *Испания:* Martin Marquínez, A.; *Швеция:* Holm, L.-E.; *Швейцария:* Jeschki, W.; *Украина:* Смышляев, О.Ю.; *Соединенное Королевство:* Williams, L.G. (председатель), Pape, R.; *Соединенные Штаты Америки:* Travers, W.D.; *МАГАТЭ:* Karbassioun, A. (координатор); *Международная комиссия по радиологической защите:* Clarke, R.H.; *Агентство по ядерной энергии ОЭСР:* Shimomura, K.

Настоящая публикация была заменена публикацией SSG-39.

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА
ISBN 978–92–0–403108–9
ISSN 1020–5845