УДК.621.039.562–564

А. С. Алпеев

Федеральное государственное учреждение «Научно-технический центр по ядерной и радиационной безопасности» (НТЦ ЯРБ), Российская Федерация

Верификация и валидация программируемых управляющих систем атомных станций

Рассматриваются вопросы, связанные с подтверждением технологии разработки программируемых управляющих систем (верификация ПУС) и их соответствия требованиям технического задания на систему при передаче в промышленную эксплуатацию (валидация ПУС) на АС. Отмечены преимущества и недостатки ПУС, роль нормативных документов в разработке управляющих систем, важных для безопасности, и ограничения применения ПУС для реализации функций, важных для безопасности АС.

Ключевые слова: атомная станция, безопасность, управляющие системы, функции, верификация, валидация.

А. С. Алпєєв

Верифікація та валідація програмованих керуючих систем АЕС

Розглядаються питання, пов'язані з підтвердженням технології розробки програмованих керуючих систем (верифікація ПКС) та їх відповідності вимогам технічного завдання на систему в процесі передавання в промислову експлуатацію (валідація ПКС) на АС. Зазначено переваги й недоліки ПКС, роль нормативних документів у розроблянні керуючих систем, важливих для безпеки, та обмеження застосування ПКС для реалізації функцій, важливих для безпеки АС

.

Ключові слова: атомна станція, безпека, керуючі системи, функції, верифікація, валідація.

Важность программируемых управляющих систем (ПУС), создаваемых на основе компьютерной техники, для безопасности атомных станций (АС) в настоящее время возрастает, поскольку быстро увеличивается их применение на вновь создаваемых и действующих энергоблоках атомных станций. Они уже используются в системах, связанных с безопасностью, выполняя функции управления и информационные функции, важные для безопасности, а также функции, критические для безопасности, в том числе функции аварийной защиты.

Возрастающее применение ПУС определяется рядом преимуществ, которыми они обладают. В частности, это связано с тем, что в этих системах обеспечиваются:

улучшенный контроль параметров АС, в том числе параметров, важных для безопасности;

улучшенный интерфейс оператор — объект;

оперативные испытания;

самоконтроль средств автоматизации и функциональных групп;

улучшенная диагностика;

повышенная точность измерения;

повышенная устойчивость;

уменьшение потребности в кабельных соединениях благодаря применению мультиплексных структур (общих информационных шин);

облегчение модификации управляющих систем под развивающиеся задачи эксплуатации.

Указанные преимущества ПУС не исключают наличия недостатков таких систем. Недостатки обусловлены сложностью процесса разработки и создания программного обеспечения, в результате чего существует большая вероятность формирования ошибок, выявление которых представляет собой достаточно сложную задачу. К недостаткам относится и трудность демонстрации характеристики безотказности; кроме того, реализация программного обеспечения, как правило, представляет собой дискретные логические модели реального мира, что имеет два типа последствий: 1) программное обеспечение более чувствительно (т. е. менее терпимо) к «маленьким» ошибкам; 2) методы интерполяции и экстраполяции полностью непригодны, поскольку приводят к недостоверным результатам.

Одним из факторов, влияющим на применение ПУС, важных для безопасности АС, является наличие нормативно-технических документов, регламентирующих условия и ограничения применимости ПУС. Следует отметить, что специфике применения ПУС на атомных станциях в отечественных нормативных документах не уделяется должного внимания, хотя практика применения таких систем уже существует несколько лет. Эта практика базируется на требованиях международных нормативных документов. К основным из них, содержащим требования к цифровым управляющим системам, относятся:

МАГАТЭ NS-G-1.1. Программное обеспечение управляющих систем, важных для безопасности, выполненных на основе компьютерной техники;

МЭК 61513. Атомные электрические станции. Управляющие системы, важные для безопасности. Общие требования;

МЭК 60880. Программное обеспечение компьютеров в системах безопасности атомных станций;

МЭК 60880–1. Программное обеспечение компьютеров в системах безопасности атомных станций. Ч. 1: Общие характеристики;

МЭК 60880–2. Программное обеспечение компьютеров в системах безопасности атомных станций. Ч. 2: Программные аспекты защиты от отказов по общей причине, использование новых программных средств и ранее разработанного программного обеспечения;

МЭК 60987. АЭС. Управляющие системы. Программируемые цифровые компьютеры, используемые в управляющих системах, важных для безопасности атомных станций.

Остановимся на пп. 1.6 и 2.9, документа [1], которые дают основания для очень важных выводов. В [1, п. 1.6] сказано:

«Так как в настоящее время безотказность компьютерной системы не может быть предсказана на единой основе или обоснована в процессе проектирования, то трудно определить и согласиться с систематически появляющимися послаблениями в руководствах по применению программного обеспечения систем, связанных с безопасностью».

В п. 2.9 этого же документа говорится:

«Количественная оценка безотказности цифровых программируемых систем из-за ряда недостатков более трудна, чем для непрограммируемых систем. Это может вызывать определенные трудности в демонстрации ожидаемой безопасности системы, выполненной на основе компьютерной техники. В настоящее время требования высокой программной безотказности не доказуемы. Следовательно, проекты, базирующиеся на единственной системе, выполненной на основе компьютерной техники и достигающей вероятности отказа на требование более низкой, чем 10^{-4} для программного обеспечения, должны реализовываться с предосторожностью».

Два этих положения содержат следующие базовые аргументы:

безотказность компьютерной системы не может быть предсказана или обоснована в процессе проектирования;

в настоящее время требования высокой программной безотказности не доказуемы.

Таким образом, применение только ПУС для выполнения функций, важных для безопасности АС, представляется невозможным из-за отсутствия доказательств требуемой безотказности их выполнения.

Хотя возможностям применения ПУС на АС посвящены все положения указанных нормативных документов, эти базовые аргументы остаются в силе и решение об использовании ПУС в УСВБ остается в компетенции разработчика, пользователя и регулирующего органа.

Наиболее перспективно применение ПУС и непрограммируемых управляющих систем (НПУС) в качестве дублирующих подсистем при реализации функций безопасности, что хорошо вписывается в концепцию обязательности реализации структуры системы с защитой от отказов по общей причине. При этом для управления энергоблоком в режимах нормальной эксплуатации можно пользоваться услугами ПУС, а в случае отказа ПУС и в аварийных ситуациях возможно управление от НПУС.

Этот вопрос тесно связан с проблемой выбора технологии разработки УСВБ.

Современные условия создания и модернизации управляющих систем АС характеризуются:

различными технологиями разработки управляющих систем;

развитыми структурами национальных и международных нормативных документов;

широким рынком средств автоматизации;

большим опытом разработки, испытаний, эксплуатации и модернизации.

В отечественной практике хорошо известны две технологии разработки управляющих систем АС, которые закреплены нормативными документами: «Единой системой стандартов автоматизированных управляющих систем» (совокупность ГОСТов 24.---, годы выпуска 1980—1985), а также «Комплексом стандартов и руководящих документов на автоматизированные системы» (ГОСТы 34.--- под наименованием «Информационная технология», годы выпуска 1989–1990).

Технология разработки управляющих систем, как правило, содержит перечень этапов разработки и требования к каждому этапу разработки. Таким образом, результат каждого этапа разработки должен соответствовать требованиям, предъявляемым к этому этапу.

Внедрение в последние годы для управляющих систем процедур верификации и валидации наиболее остро ставит проблему, связанную с необходимостью применения достаточно обоснованной технологии их создания. Разработчик управляющих систем, частей АСУТП и АСУТП в целом должен уже при формировании тендерных предложений декларировать применяемую технологию разработки или модернизации.

Верификация управляющей системы, важной для безопасности (УСВБ), представляет собой решение задачи определения соответствия процесса разработки УСВБ предварительно заявленной разработчиком технологии разработки, представляющей собой совокупность требований к этапам создания УСВБ от формирования тендерных предложений до разработки проекта и внедрения созданной на его основе УСВБ в эксплуатацию.

Результатом верификации УСВБ является выпуск отчета, содержащего результаты, подтверждающие соответствие УСВБ каждому требованию по каждому этапу ее разработки. Иными словами, верификация УСВБ представляет собой совокупность результатов валидации каждого этапа разработки УСВБ.

Валидация УСВБ представляет собой решение задачи, связанной с подтверждением соответствия характеристик УСВБ требованиям технического задания, реализуемого проведением испытаний, расчетами или опытом применения аналогичных систем.

Результатом валидации управляющей системы является отчет, содержащий перечень требования к управляющей системе и перечень протоколов испытаний или результатов расчетов, которые подтверждают соответствие предъявленным требованиям.

В отечественной практике для валидации принято проведение испытаний управляющей системы: 1) на заводе-изготовителе (заводские испытания); 2) при поставке на объект (приемочные испытания); 3) испытания управляющей системы, интегрированной с технологическим оборудованием АС и смежными системами (испытания на объекте).

Отчеты по валидации управляющих систем, как правило, формируются согласно результатам указанных испытаний. При этом валидация управляющей системы считается выполненной, если выполнена валидация всех функциональных групп [2] этой системы.

Для обеспечения и демонстрации соответствия управляющих систем (например, управляющих систем безопасности) принципу отказа по общей причине требуется некоторое разнообразие либо средств автоматизации, либо

применяемых методов реализации функций, либо и то и другое вместе [3].

Применение программируемых средств автоматизации возможно только при условии введения некоторых ограничений. При этом возможно использование различных методов, снижающих, как показывает практика, вероятность их отказа.

Метод «жесткого программирования» приводит, практически, к соответствию программируемых средств автоматизации непрограммируемым средствам автоматизации, для которых справедливы методы статистической оценки отказов, сводя на нет многие преимущества программируемых средств автоматизации.

Метод «мягкого программирования» накладывает ряд условий для его применения:

отсутствие прерываний;

использование в дублирующих каналах разных операционных систем;

использование «вырожденных» операционных систем, т. е. операционных систем, необходимых только для решения одной задачи;

применение в дублирующих каналах непрограммируемых средств автоматизации.

Эти методы рекомендуются для применения при разработке ПУС.

Что касается соответствия УСВБ критерию разнообразия, нужно отметить, что в проекте управляющей системы следует рассматривать такие общие причины возникновения отказа функциональных групп УСВБ, как:

наличие единственного изготовителя средств автоматизации;

идентичность дублирующих каналов, выполняющих одну функцию;

применение одинаковых операционных систем в дублирующих каналах (в случае применения программируемых средств автоматизации);

ошибка оператора;

электромагнитное воздействие;

сейсмическое воздействие;

пожар;

наводнение и т. д.

Для каждой из общих причин отказа в проекте УСВБ следует выполнять анализ последствий, которые могут быть вызваны возникновением такой причины, и предусматривать меры по их предотвращению или уменьшению ущерба от них.

Выводы

По представленным в статье соображениям можно предложить следующие выводы:

управляющие системы безопасности атомных станций следует выполнять, как минимум, из двух независимых подсистем на основе программируемых и непрограммируемых средств автоматизации, что позволит совместить достоинства программируемых систем для реализации функций безопасности атомной станции и позволит успешно демонстрировать показатели безотказности этих систем регулирующим органам;

необходима гармонизация нормативных документов, регламентирующих аспекты верификации и валидации управляющих систем, которые в настоящее время допускают довольно разные трактовки.

Список литературы

1. МАГАТЭ NS-G-1.1. Программное обеспечение управляющих систем, важных для безопасности, выполненных на основе компьютерной техники. — 2000.

2. НП-026–04. Требования к управляющим системам, важным для безопасности атомных станций. — М.:НТЦ ЯРБ, 2004.

3. НП-082–07. Правила ядерной безопасности реакторных установок атомных станций. — М.: НТЦ ЯРБ, 1997.

Надійшла до редакції 08.06.2010.