УДК 004.051

ОСОБЕННОСТИ ВЕРИФИКАЦИИ И ВАЛИДАЦИИ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ КОМПЛЕКСОВ НА АППАРАТУРЕ ТПТС ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ АЭС

Е.Ю. МАЛИКОВА, С.И. КУПЦОВ

Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова
Сущевская, 22, Москва, 127055, Россия

Поступила в редакцию 2 февраля 2015

Технология разработки и испытаний программно-технических комплексов (ПТК) для систем контроля и управления опирается на модель жизненного цикла ПТК и входящих в их состав программных средств. Жизненный цикл разбивается на ряд этапов, каждый из которых характеризуется определенными целями и результатами, и которые должны завершаться проверками, подтверждающими качественное завершение каждого этапа.

Далее кратко рассмотрен типовой процесс разработки прикладного программного обеспечения (ПО) в рамках создания ПТК, который успешно применяется во ФГУП «ВНИИА», в том числе и для разработки ПТК, применяемых в системах безопасности (3 и 4 энергоблоки Калининской АЭС). Прикладное программное обеспечение ПТК для систем безопасности разрабатывается в соответствии с рекомендациями МЭК 60880 [1].

До начала разработки ПТК осуществляется кропотливая работа по созданию типовых элементов, которые лежат в основе его программно-аппаратной конфигурации. В этих работах наряду с ФГУП «ВНИИА» принимают участие проектные и наладочные организации, имеющие большой опыт по созданию и наладке подобных комплексов для АЭС. Эти работы завершаются выпуском следующих взаимосогласованных документов:

1. Руководящий документ, определяющий порядок создания ПТК, в котором описаны все этапы работ, включающие анализ задания, конфигурирование, изготовление, испытания и приемку.
2. Типовые схемы подключения периферийного оборудования.
3. Библиотека типовых алгоритмических решений по реализации функций контроля и управления.
4. Библиотека стандартных программных блоков, реализующих определенные алгоритмы и функции.
5. Стандартные методики тестирования ПТК.

Последующее проектирование осуществляется в строгом соответствии с этими документами, что позволяет существенно уменьшить возможные ошибки, как в аппаратной, так и в программной конфигурации ПТК.

Правильно организованный процесс разработки ПТК должен обязательно подкрепляться исчерпывающими проверками на каждом этапе его жизненного цикла (данные таблицы). В этой статье рассматриваются только этапы жизненного цикла ПТК в ФГУП «ВНИИА». Работы с ПТК на площадке АЭС проводятся по документам, выпускаемым организациями, ответственными за ввод ПТК в эксплуатацию.

С целью упорядочения проверочных работ выпускается план верификации и валидации, соответствующий определенным требованиям [2–4]. Для каждого этапа жизненного цикла ПТК план верификации и валидации определяет: задачи; методы верификационных процедур; критерии оценки; исходные данные и порядок оценки результатов верификации; сроки выполнения работ; ресурсы в части персонала, проводящего проверки; распределение

обязанностей и ответственность должностных лиц; требования к оформлению и содержанию документов, выпускаемых по результатам проверок и испытаний.

Наиболее ответственные проверки по этому плану выполняются независимыми экспертами других организаций. Как правило, это организации, которые впоследствии будут осуществлять наладку поставляемых ПТК на АЭС, представители поставщика и самой АЭС, жизненно заинтересованные в хорошем качестве ПТК.

Процесс разработки ПТК

Этап жизненного цикла ПТК	**Работа**	**Метод**	**Кто проводит**	**Документ**
Задание на разработку ПТК	Верификация задания	Экспертиза	Эксперты ФГУП «ВНИИА»	Заключение по анализу задания. Акт приемки задания
Разработка проекта ПО	Верификация проекта ПО	Автоматизированная проверка соответствия заданию	Эксперты независимых организаций	Отчет по верификации проекта ПО
Генерация кода	Верификация кода	Автоматическая проверка инструментальными средствами	Персонал ФГУП «ВНИИА»	Протокол
Интеграция	Верификации правильности загрузки ПО в ПТК	Автоматическая проверка правильности загрузки	Персонал ФГУП «ВНИИА»	Протокол
Программа и методика тестирования ПТК	Верификация программы и методики	Экспертиза в форме согласования заказчиком и внешними организациями, участвующими в проекте	Эксперты независимых организаций	Согласованная программа и методики
Тестирование ПТК	Валидация	Испытания по программе и методике	Эксперты ФГУП «ВНИИА» и независимых организаций	Отчет
Приемка ПТК	Валидация	Экспертиза	Эксперты ФГУП «ВНИИА» и независимых организаций в составе комиссии по приемке ПТК	Акт комиссии

На этапе выдачи задания на разработку ПТК основной задачей процедуры верификации является проверка соответствия требований и данных, содержащихся в задании, положениям руководящего документа и документации на программно-аппаратные средства. Методом анализа Задания является экспертиза, которая проводится назначенными экспертами ФГУП «ВНИИА». Критерии – соответствие требованиям руководящего документа по составу, полноте, согласованности и правильности оформления, а также соответствие данных, определяющих конфигурацию ПТК, возможностям и техническим характеристикам аппаратуры ТПТС. По результатам анализа выпускается заключение. При наличии замечаний задание направляется на доработку. После устранения замечаний задание принимается по акту.

Для разработки прикладного ПО используются инструментальные средства (GET-R, GET-R1). Это специализированные средства, предназначенные для конфигурирования только аппаратуры ТПТС. Их применение позволяет объединить несколько соседних этапов классической модели жизненного цикла программного обеспечения (от проекта до реализации) и автоматизировать работу на этих этапах.

На этапе разработки проекта прикладного ПО основными верификационными задачами являются: проверка документации на рабочие места с инструментальными средствами конфигурирования, и, главное – проверка разработанного проекта ПО в виде функциональных схем на графическом языке инструментальных средств и параметров, определяющих прикладную конфигурацию ПТК, на соответствие требованиям Задания.

Методом верификации рабочих мест с инструментальными средствами конфигурирования является аттестация, проводимая службой качества ФГУП «ВНИИА». Критерий – соответствие требованиям по составу оборудования и программных средств, наличие необходимой документации, соблюдение руководства по эксплуатации на инструментальные средства. Методом верификации проекта ПО на соответствие требованиям Задания является экспертиза, проводимая независимыми экспертами сторонней организации. Критерий – соответствие проекта ПО требованиям Задания. Проводится автоматизированная проверка соответствия проекта ПО аппаратной конфигурации ПТК (базе данных), а также соответствие принятым библиотечным типовым алгоритмическим решениям по реализации функций контроля и управления.

На этапе генерации кода задачей по верификации является проверка правильности сгенерированного загружаемого кода. Методом верификации является автоматическая проверка, выполняемая инструментальными средствами. Критерий – отсутствие сообщений об ошибках во время выполнения процедуры генерации кода.

На этапе интеграции прикладного ПО с аппаратными средствами задачей по верификации является проверка правильности загрузки ПО в ПТК. Метод проверки – автоматизированное обратное считывание ПО из модулей ПТК и сравнение с исходным разработанным ПО. Критерий – соответствие загруженного и исходного ПО.

На этапе разработки программы и методики тестирования ПТК основной задачей работ по верификации является проверка адекватности программы и методики тестирования. Методом верификации программы и методики функциональных испытаний ПТК является процедура согласования программы и методики с проектными и наладочными организациями, участвующими в создании ПТК, а также с организациями заказчика и регулятора. Критерий – достаточность объема и методов испытаний для подтверждения правильности реализации ПТК (соответствие Заданию).

На этапе тестирования ПТК задачей работ по валидации является подтверждение правильности функционирования ПТК (работы прикладного ПО, реализующего заданные алгоритмы) в реальном аппаратном окружении с применением средств имитации периферийного оборудования (датчики, исполнительные механизмы и т.п.) и системы верхнего блочного уровня. Метод проверки – программа и методика тестирования. Критерий – соответствие ПТК требованиям Задания в части выполняемых функций.

На этапе приемки ПТК основной задачей работ по валидации является рассмотрение имеющейся документации по разработке, изготовлению и тестированию ПТК, а также эксплуатационной документации с целью определения соответствия ПТК требованиям Задания и возможности отправки ПТК на АЭС. Метод проверки – проведение экспертной комиссии по приемке ПТК с участием представителей заказчика, регулирующего органа, других организаций, принимавших участие в работах по созданию ПТК. Критерий – соответствие ПТК требованиям Задания.

Рассмотренные выше работы включены в отдельную процедуру, входящую в состав руководства по обеспечению качества, которая детально описывает процесс выполнения этих работ.

К особенностям работ по проведению верификации и валидации прикладного программного обеспечения ПТК, разрабатываемых ФГУП «ВНИИА» для систем безопасности АЭС, можно отнести следующее:

– Работы по созданию прикладного программного обеспечения выполняются с помощью специализированных инструментальных средств, имеющих сертификат IStec, допускающий их применение для конфигурирования программно-технических комплексов, применяемых в системах безопасности и системах, важных для безопасности. Эти инструментальные средства имеют в своем составе широкий спектр средств проверки правильности проекта ПО и генерации кода.

– Особое внимание уделяется подготовительным работам – разработке типовых, хорошо проверенных решений, лежащих в основе программной конфигурации ПТК. Наиболее ответственные работы по верификации и валидации проводятся независимыми экспертами, работающими в организациях, заинтересованных в надлежащем качестве ПТК.

– Большая часть верификационных и валидационных процедур, относящихся к прикладному ПО, проводится на поставляемом ПТК с применением имитаторов периферийного оборудования и системы верхнего блочного уровня, что позволяет выявлять возможные ошибки ПО в реальном окружении.

Список литературы

1. ГОСТ Р МЭК 60880 – 2011 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А».
2. ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств».
3. Верификация и валидация программных средств управляющих систем, важных для безопасности атомных станций. Общие требования. Руководящий документ. 58413824.23512.001-390.РД-01-2002.М.
4. IEEE Std 1012. IEEE Standard for Software Verification and Validation Plans.