УДК 004.052.42

ВЕРИФИКАЦИЯ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ УСБ АЭС ПОСРЕДСТВОМ САПР GET-R1

СЕЛИВЕРСТОВ Е.С., ГАЛИЦЫН Ю.С., ИВАНОВА А.А.

Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова»

(Москва, Российская Федерация)

Аннотация. Темой доклада является освещение процедуры верификации прикладного программного обеспечения УСБ Белорусской АЭС посредством САПР GET-R1. Описаны инструменты САПР, позволяющие проводить верификацию, и приведена методология испытаний прикладного программного обеспечения.

Ключевые слова: АЭС, ТПТС-СБ, автоматизация, автоматизированные системы управления, система безопасности, верификация, прикладное программное обеспечение, сценарий проверки

VERIFICATION OF NPP SAFETY CONTROL SYSTEM APPLICATION SOFTWARE USING GET-R1 CAD

EVGENIY.S. SELIVERSTOV, YURY.S. GALITSYN, ANNA.A. IVANOVA

The Federal State Unitary Enterprise "All-Russia Research Institute of Automatics named after N.L. Dukhov" (Moscow, Russian Federation)

Abstract. The topic of the report is to highlight the procedure for verifying the application software of the safety control system of the Belarusian NPP using the CAD GET-R1. The CAD tools that allow for verification are described, and the methodology for testing the application software is given.

Keywords: NPP, TPTS-SB, automation, automated control systems, safety system, verification, application software, test script.

Введение

В настоящее время программируемые технические средства автоматизации нашли широкое применение в управляющих системах безопасности (УСБ) и в системах, важных для безопасности АЭС. В связи с этим остро встает вопрос надежности прикладного программного обеспечения (ППО), использующегося в программируемых программных средствах. Существующие международные стандарты предписывают использовать верифицированные программные средства, а значит и верифицированное ППО. Для решения этой задачи в составе САПР GET-R1, созданном во ВНИИА им. Духова, был разработан ряд автоматизированных решений, позволяющих проводить испытания ППО.

Основная часть

Верификация ППО является одним из методов, применяемых для защиты управляющей системы от отказа по общей причине. Объектом проведения верификации являлось ППО следующих ПТК, входящих в состав УСБ энергоблоков №1 и №2 Белорусской АЭС:

- ПТК инициирующей части АЗ-УСБТ на базе платформы ТПТС-СБ, относящиеся к классу безопасности 2;
- ПТК инициирующей части ПЗ на базе платформы ТПТС-НТ, относящиеся к классу безопасности 3.

Общая концепция испытаний ППО ПТК для инициирующих частей АЗ-УСБТ и ПЗ состоит из нескольких этапов:

- верификация прикладной конфигурации ПТК (базы данных Задания заводу-изготовителю (ЗЗИ) и ППО (GET-проекта) - этап 1;
- статическое тестирование прикладной программной конфигурации оборудования ТПТС (GET-проект) - этап 2;
- динамическое тестирование прикладной программной конфигурации оборудования ТПТС (GET-проект) - этап 3;
- функциональные испытания ПТК в части технологических разделов - этап 4;
- функциональные испытания оборудования ПТК - этап 5.

Реальная аппаратура ПТК представляет собой программно-аппаратные средства, для которых ППО, реализующее функциональную технологическую логику, представляет собой

самостоятельную часть, разрабатываемую с помощью STEP-кодов, генерируемых САПР GET-R1. Именно эта часть ППО проверяется на этапе статического тестирования, которому и уделено основное внимание в докладе.

Под статическим тестированием понимаются испытания ППО ПТК, проводимые с целью подтверждения соответствия ППО технологическим алгоритмам Задания на автоматизацию (1) без учета реакции объекта управления. Статическое тестирование ППО УСБ энергоблоков №1 и №2 Белорусской АЭС проводилось специалистами ОКБ «ГИДРОПРЕСС» при участии специалистов группы разработки ППО ФГУП «ВНИИА».

Статическое тестирование основано на использовании идеологии «черного ящика». Принимается, что разработанные базы данных и сгенерированные коды представляют собой неизвестный объект, способ проверки которого осуществляется заданием на его входы возмущающих воздействий в определенном объеме параметров и получением сигналов, поступающих с выходов объекта для проведения последующего анализа и обработки полученной информации. Такой подход позволяет абстрагироваться от внутренней организации прикладного ПО ПТК и уделить основное внимание его функционированию.

Статическое тестирование проводится с использованием штатных модулей САПР GET-R1 – подсистемы моделирования SimuNT и подсистемы выполнения сценариев. Эти модули обладают следующими функциями:

- формирование модели работы алгоритмов ПТК;
- задание значений входных сигналов и отслеживание значений выходных сигналов;
- сверка реакции модели (выходные сигналы) с ожидаемым поведением;
- отображение текущего значения сигналов и результатов операций над сигналами на GET-планах в процессе работы модели;
- формирование сценария проверки с помощью скриптового языка.

Основной принцип тестирования заключается в оказании воздействия на модель ПТК путём задания значений входных переменных и последующего сравнения реакции модели с заранее заданным критерием успешности выполнения теста. Причём, процесс тестирования предполагает его автоматизацию, но с возможностью вмешательства пользователя: возможен запрос каких-либо действий, выполняемых пользователем вручную, предложение выбора пользователем дальнейшего действия (остановить выполнение сценария или продолжить) и, при необходимости, экстренное прерывание выполнения сценариев проверки. Задание входных значений на модель ПТК, с их последующей проверкой, происходит с помощью запуска скриптов, написанных на языке сценариев.

Модель демонстрирует работу алгоритмов, позволяет проверить корректность их работы. На рис. 1 представлена схема тестирования ППО с помощью подсистемы моделирования SimuNT САПР GET-R1.

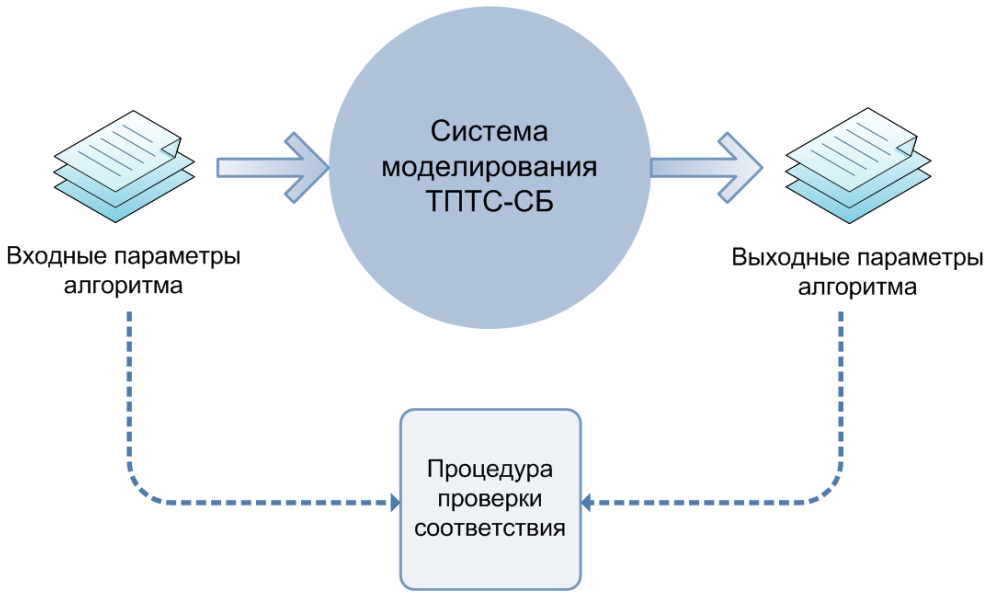

Рис. 1. Схема тестирования ППО

Порядок проведения статического тестирования предусматривает выполнение следующих основных действий:

- составление исходных данных на основании рассмотрения [1] (как основного документа, определяющего функциональные требования);
- определение массивов данных входных параметров для задания условий, соответствующих определенным условиям срабатывания или в соответствии со значениями параметров, используемых в [1];
- написание сценариев проверки в подсистеме редактирования и выполнения сценариев САПР GET-R1, задающих начальные состояния входных параметров, которые соответствуют определенному режиму реакторной установки, затем последовательно реализующих логику изменения входных параметров в соответствии с определенными условиями срабатывания или функцией автоматизации, а так же определяющими перечень параметров для вывода в файл или для записи в файл регистрации фактических моментов изменений значений переменных, необходимый для проведения заключительного анализа;
- подготовка программно-аппаратного комплекса с САПР GET-R1;
- запуск сценариев в подсистеме редактирования и выполнения сценариев САПР GET-R1 для проверки функционирования ППО ПТК;
- проведение анализа результатов испытаний и составление отчета, в котором фиксируются все этапы проверок, приводятся результаты и выводы о проведенных проверках ППО ПТК.

Условия срабатывания определяются на основании анализа Задания [1]. При проведении анализа необходимо учитывать разветвленную и взаимосвязанную структуру алгоритмов функций безопасности, а именно, учитывать то, что одно условие срабатывания может приводить к активации разных функций безопасности, и, как следствие, к активации целой группы выходных сигналов.

После запуска модели ПТК перед запуском сценариев проверки задается исходное состояние всей системы. Начальные значения входных сигналов задаются таким образом, чтобы состояние параметров реакторной установки соответствовало определенному режиму работы, например, уровень мощности 100 % при четырех работающих ГЦНА. При этом инициирование защитных действий не происходит. Исходное состояние системы сохраняется в память и загружается после каждого выполненного сценария перед выполнением следующего, тем самым обеспечивая одинаковое состояние модели ПТК перед каждой проверкой и исключая влияние одного сценария проверки на другие.

ППО ПТК представляет собой программный код, созданный и откомпилированный в САПР GET-R1 на основании материалов, изложенных в [1]. Функциональные схемы редактора САПР GET-R1 являются графическим представлением алгоритмов, приведенных в [1] с максимальной степенью детализации. Каждая функция автоматизации, описанная в [1], отражает логику срабатывания соответствующего алгоритма и действия соответствующих исполнительных механизмов, которые должны быть активизированы. Для проверки правильности работы созданного ППО ПТК необходимо задать входным параметрам такие значения, чтобы активизировать алгоритм и получить выходные сигналы, соответствующие командам на активацию исполнительных механизмов, указанным в [1].

Критерий полноты проверок – в процессе тестирования проверяются все, определенные в [1] условия срабатывания функций безопасности АЗ-УСБТ, ПЗ. Если проверка каких-либо условий срабатывания невозможна или не обязательна, то это должно быть обосновано.

Критерий соответствия (правильности) – активация исполнительных механизмов в соответствии с определенными в [1] и на его основании условиями срабатывания.

При изменении значений входных сигналов производится контроль выходных сигналов и сравнение их с ожидаемыми значениями. Если ожидаемые выходные сигналы отсутствуют, то обнаруженные в процессе анализа несоответствия фиксируются и заносятся в отчет по тестированию. Если при тестировании происходит генерация выходных сигналов, появление которых не было запланировано, то производится анализ функций в соответствии с [1] и функциональных диаграмм, реализованных в САПР GET-R1. Затем делается вывод о правильности генерации выходных сигналов. Если выходные сигналы не были определены в программе тестирования, и их появление является следствием расхождения реализации

функциональных схем с логикой, описанной в соответствующей функции автоматизации, то выявленные в процессе анализа несоответствия фиксируются и заносятся в отчет по тестированию. Полученные результаты передаются группе разработки ППО ФГУП «ВНИИА». Все результаты проверок, обнаруженные несоответствия и действия по их исправлению заносятся в отчет о тестировании.

В процессе работы над верификацией ППО УСБ энергоблоков №1 и №2 Белорусской АЭС специалистами ОКБ «ГИДРОПРЕСС» было разработано более трехсот сценариев проверки для каждого энергоблока. Были выпущены отчеты о результатах тестирования, содержащие перечни условий срабатывания функций безопасности, перечни входных сигналов и способы их изменения, перечни инициированных выходных сигналов, массивы сценариев проверки, графики изменения входных и выходных сигналов, подробные описания возникающих ошибок в ППО, предложения по улучшению и развитию инструментария для тестирования в САПР GET-R1. На основании полученных материалов группой разработки ППО ФГУП «ВНИИА» производилась корректировка ППО УСБ и давались рекомендации для модернизации САПР GET-R1. Разработанные ОКБ «ГИДРОПРЕСС» сценарии проверки легли в основу сценариев периодических проверок ПТК, выпускаемых ФГУП «ВНИИА» в составе заводской рабочей документации к ПТК АЗ-УСБТ и ИЧ ПЗ энергоблоков №1 и №2 Белорусской АЭС.

Заключение

В результате выполненной работы по проведению верификации прикладного программного УСБ энергоблоков №1 и №2 Белорусской АЭС посредством САПР GET-R1 можно отметить, что надежность систем контроля и управления, построенных на программируемых технических средствах автоматизации, обеспечивается, в том числе, за счет реализации системной многоступенчатой процедуры тестирования программного обеспечения, начиная от тестирования отдельных программных модулей и заканчивая функциональным тестированием на полигоне в динамических режимах с использованием модели объекта управления. Системная многоступенчатая процедура тестирования ППО УСБ на средствах ТПТС может быть эффективно реализована при наличии соответствующей среды разработки, минимизирующей ошибки при создании ППО – САПР GET-R1.

Список литературы

1. Белорусская АЭС. Энергоблок №1 Техническое задание. Инициирующая часть УСБТ. Задание заводу-изготовителю BLR1.B.110.1.&&&&&&.01&&&.021.MB.0001. Книга 1 алгоритмы функций безопасности, 2015.