2. РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Канд. физ.-мат. наук А.О. Мирошник

ВОПРОСЫ ВЕРИФИКАЦИИ И ВАЛИДАЦИИ ПРОГРАММНО-ТЕХНИЧЕСКИХ КОМПЛЕКСОВ В СОСТАВЕ ЭЛЕКТРООБОРУДОВАНИЯ СИСТЕМ УПРАВЛЕНИЯ И ЗАЩИТЫ РЕАКТОРОВ ВВЭР

Повышение требований к безопасности эксплуатации АЭС, создание современных автоматизированных систем управления технологическими процессами (АСУТП) энергоблоков привели к необходимости расширения информационно-диагностических возможностей комплекса электрооборудования СУЗ в целом и реализации в его рамках ряда дополнительных функций, повышающих качество процесса управления.

Вследствие этого, для вновь строящихся и модернизируемых энергоблоков АЭС (АЭС «Тяньвань» в Китайской Народной Республике, Калининской АЭС, Ново-Воронежской АЭС и др.) в составе комплекса электрооборудования СУЗ, традиционно реализуемого с использованием аппаратных средств жесткой логики, используется оборудование, созданное на средствах вычислительной техники (СВТ).

Как известно, системы, построенные с использованием СВТ, обладают характеристиками, коренным образом отличающими их от аппаратных средств на базе жесткой логики. Компьютеризированные системы являются программируемыми и, соответственно, используют в своем составе программные изделия (ПИ). Благодаря свойству программируемости эти системы, помимо способности выполнения своих основных технологических функций, позволяют осуществлять более качественный контроль состояния оборудования АЭС, а также более качественное тестирование, калибровку, самопроверку и диагностику отказов. Гибкость и простота модифицирования компьютеризированных средств оказываются чрезвычайно полезными при проведении модификаций и усовершенствований систем на их основе. Но, с другой стороны, наличие ПИ в составе оборудования усложняет процесс его разработки и тестирования. В аппаратных системах отказы могут возникать вследствие возможных ошибок при конструировании и изготовлении. Ча-

ще, однако, отказы возникают из-за износа или деградации, обусловленных воздействием внешних факторов, и носят случайный статистический характер, поддающийся математической оценке. Программные изделия не подвержены износу. Отказы программных изделий всегда являются результатом случайных или систематических ошибок при определении технических требований, на этапах проектирования и разработки. Это приводит к тому, что системы на базе СВТ не только труднее разрабатывать и тестировать, но и гораздо труднее точно оценить их надежность по сравнению с обычными непрограммируемыми электронными системами.

Общепризнано, что в настоящее время компьютеризированные системы не поддаются количественной оценке надежности – главным образом из-за наличия в них программного элемента. Поэтому оценка систем на базе СВТ должна основываться на доказательстве правильности их функционирования (по отношению к техническим требованиям) и того, что они в полной мере реализует требования, сформулированные в задании на проектирование. Иными словами, необходимо показать, что программные изделия в таких системах обладают высоким уровнем целостности. **Целостность** определяется как свойство законченности, зависимости и отсутствия дефектов. Следует подчеркнуть, что в соответствии с современной международной практикой демонстрация целостности является необходимым качественным атрибутом систем и считается законной основой для приемки компьютеризированных систем в эксплуатацию. Целостность должна обеспечиваться путем разработки с применением системного, тщательно контролируемого и отслеживаемого инженерного процесса, в котором предусмотрены мероприятия по верификации и валидации на всех этапах жизненного цикла вычислительной системы. Под **верификацией** здесь и далее понимается процесс проверки соответствия результатов разработки системы на каждом этапе требованиям, установленным на предыдущем этапе (IEC 60880 (МЭК 880, п.2.21)). Под **валидацией** - тестирование и оценка интегрированной вычислительной системы, которые обеспечивают подтверждение функциональных и эксплуатационных свойств системы, а также правильность функционирования внешних интерфейсов (МЭК 880, п.2.20).

Настоящая статья посвящена рассмотрению одного из возможных подходов к достижению целостности компонентов электрооборудования СУЗ, относящихся к классу безопасности 3Н в соответствии с ПНАЭ Г-01-011-97 (ОПБ-88/97) и построенных с применением СВТ, ее демонстрации в процессе проведения процедур верификации и валидации.

К изделиям данного класса в составе электрооборудования СУЗ

можно отнести шкафы контроля положения и управления органами регулирования реактора (ШКУ), шкафы автоматического регулирования мощности (АРМ) и разгрузки реактора (РОМ), шкафы групповой индикации (ШГИ). Все вышеперечисленные устройства представляют собой системы, построенные на базе одноплатных микроконтроллеров серии ОМК2х и программируемых контроллеров серии В-10Р.

Одноплатные микроконтроллеры серии ОМК2х являются законченными функциональными модулями со встроенными программными изделиями (размещаемыми на микросхемах ППЗУ или непосредственно в кристалле микропроцессора), ориентированными на реализацию алгоритмов непосредственного обслуживания, диагностики и управления специализированным технологическим оборудованием. Эти модули оснащены простыми интерфейсами связи (RS-232, RS-485), аналогового и цифрового ввода-вывода и имеют ограниченную гибкость в части выбора параметров функционирования.

В связи с ограниченными вычислительными мощностями микроконтроллеров серии ОМК2х, требованием максимального быстродействия и компактности, разрабатываемые для них программные изделия функционируют, как правило, по жесткой циклической программе без использования средств операционных систем. Благодаря ограниченной функциональности, микроконтроллеры серии ОМК2х в большинстве случаев поддаются исчерпывающему тестированию в рамках функциональных испытаний.

Универсальные программируемые контроллеры серии В-10Р предназначены для обработки информации, поступающей с уровня технологических контроллеров и непосредственно от датчиков технологического оборудования. В их функции входит реализация алгоритмов управления, контуров регулирования, сбора и обработки информации, информационного обмена с сетевым уровнем электрооборудования СУЗ, реализация минимальных функций операторского интерфейса (задачи сигнализации оперативному персоналу).

Программируемые контроллеры представляют собой готовые программируемые технологические информационно-управляющие системы общего назначения. Аппаратное и программное обеспечение таких систем разрабатывается конфигурируемым под различные варианты применения. Используемые в составе программных изделий процессорных плат контроллеров В-10Р специализированные модули работы с платами цифрового и аналогового ввода-вывода проходят полный цикл отладки и тестирования в процессе разработки соответствующих плат. Это позволяет при проведении процедур верификации и валидации программных изделий контроллера рассматривать их в качестве **предварительно разработанных программных средств** (ПРПС)**.** Под ПРПС понимаются

программные средства (подпрограммные модули или изделия), целостность которых была продемонстрирована ранее, доступные для использования в компьютеризированных системах.

Таким образом, шкафы нового поколения в составе электрооборудования СУЗ, использующие в своем составе СВТ, могут быть отнесены к программно-техническим комплексам (ПТК), т. е. к законченным устройствам, представляющим собой единый программно-аппаратный комплекс, никакая часть которого не может быть без ущерба для функциональности выделена и использована автономно вне своего прямого назначения. В полной мере это относится и к программным изделиям, входящим в состав ПТК. Никакое ПИ или его часть не могут быть выделены, установлены и запущены на каком-либо техническом средстве вне состава шкафа, для которого они были разработаны, или использованы в автономном режиме. Такой подход позволяет говорить не о верификации и валидации отдельных программ в составе ПТК, а о верификации и валидации ПТК как единого целого.

При планировании и проведении процедур верификации и валидации программно-технических комплексов на базе СВТ необходимо принимать во внимание класс безопасности функций, выполняемых этими ПТК в составе электрооборудования АЭС. Правильная классификация ПТК с этой точки зрения позволяет, с одной стороны, надлежащим образом ранжировать степень внимания проектировщиков и надзорных органов при определении технических условий, проектировании, обеспечении качества, изготовлении и испытаниях, с другой стороны, – избежать неоправданных затрат материальных и трудовых ресурсов, используемых при разработке, что непосредственным образом влияет на конечную себестоимость и конкурентоспособность ПТК.

По своему функциональному назначению, требованиям к надежности и бесперебойности функционирования разрабатываемое НПП ВНИИЭМ оборудование на базе СВТ в составе электрооборудования СУЗ относится к системам нормальной эксплуатации, важным для безопасности (класс 3Н в соответствии с ПНАЭ Г-01-011-97 (ОПБ-88/97)). Отказы этого оборудования приводят к потере функций, не ухудшающих показатели работы реакторной установки, либо, в худшем случае, приводящих к снижению показателей работы реактора на ограниченный срок. Следовательно, требования МЭК 880, выступающие как признанный эталон проведения процедур верификации и валидации высоконадежного программного обеспечения, предназначенного для использования в системах безопасности атомных электростанций, для ПТК класса безопасности 3Н в составе электрооборудования СУЗ непосредственно не относятся.

Однако отсутствие российских и международных документов, четко регламентирующих этапы и способы проведения процедур верификации и валидации для систем третьего класса безопасности, заставляет разработчиков принимать за основу положения МЭК 880, ставя перед ними непростую задачу нахождения компромисса между целостностью разрабатываемой системы и трудоемкостью и стоимостью разработки.

Предлагаемая процедура верификации и валидации выполняется в процессе разработки шкафов в составе электрооборудования СУЗ, относящихся к классу безопасности 3Н, имеющих в своем составе СВТ и ПИ, которые по своему составу могут быть классифицированы как программно-технический комплекс. Формальную основу процедуры составляют:

- единый план проведения работ по верификации и валидации соответствующего ПТК;
- программы обеспечения качества на этапах разработки и изготовления электрооборудования СУЗ;
- процедуры управления качеством разработки программных изделий, входящих в состав ПТК.

Согласно модели жизненного цикла программных средств ГОСТ РИСО (МЭК 12207-99), процедуры верификации и валидации ПТК в составе электрооборудования СУЗ разбиваются на следующие этапы:

- этап 1 – определение оснований для проведения работ по верификации и валидации, включая составление и утверждение планов проведения работ по верификации и валидации, программ качества на этапах разработки и изготовления;

- этап 2 – разработка частных технических заданий на программные изделия устройств, входящих в состав ПТК;

- этап 3 – разработка программных изделий устройств, входящих в состав ПТК;

- этап 4 – интегрирование и предварительное тестирование устройств, входящих в состав ПТК;

- этап 5 – автономные испытания ПТК;

- этап 6 – комплексные испытания ПТК в составе электрооборудования СУЗ;

- этап 7 – ввод в эксплуатацию и сопровождение.

Последний из перечисленных этапов выходит за рамки данной статьи и далее рассматриваться не будет.

На этапе 1 работ по верификации и валидации, исходя из специфических требований Заказчика, по согласованию с надзорными органами определяется состав руководящих и нормативных документов для обеспечения надежности, качества и

проведения процедур верификации и валидации. Принимаются организационные решения на уровне администрации НПП ВНИИЭМ по созданию отдельных экспертных групп и определению персональной ответственности исполнителей. Требование независимости экспертных групп, предусмотренное МЭК880, трактуется как вывод данных групп из прямого административного подчинения руководителям подразделений, из состава которых они сформированы. НПП ВНИИЭМ выпускаются и согласовываются с Заказчиком программы обеспечения качества разработки и изготовления электрооборудования СУЗ и отдельные процедуры по обеспечению качества разработки ПИ в их составе. Основные этапы и методы проведения процедур верификации и валидации формулируются в виде единого плана проведения работ по верификации и валидации ПТК в составе электрооборудования СУЗ, охватывающего собой весь круг предстоящих работ. План проведения работ по верификации согласовывается с представителями уполномоченных надзорных органов.

На этапе 2 работ, исходя из выбранного распределения функций между аппаратными и программными компонентами конкретного ПТК, производится разработка частных технических заданий ГОСТ 34602-89 на программные изделия устройств, входящих в состав ПТК, в соответствии с требованиями общего технического задания на комплекс электрооборудования СУЗ. В задачи верификации на данном этапе входит проверка частных технических заданий на программные изделия устройств, входящих в состав ПТК, на предмет их соответствия требованиям общего технического задания.

На этапе 3 работ проходит непосредственная разработка программного обеспечения. На основе частных технических заданий выполняется процесс программирования и первичной отладки с использованием инструментальных средств общего назначения ПИ устройств, входящих в состав ПТК. При программировании для обеспечения референтности широко используется имеющийся в НПП ВНИИЭМ задел, прошедший опытную эксплуатацию программного обеспечения и алгоритмов. Так, при программировании одноплатных контроллеров ОМК21 и ОМК22, входящих в состав шкафа контроля и управления ПКУ1М, был использован задел программного обеспечения и алгоритмов контроллеров серии ОМК2х, входивших в состав комплекса СООИ подсистемы СГИУ энергоблока №3 Балаковской АЭС. На разработанные программные изделия выпускается комплект документации (ГОСТы группы 19, Единая система программной документации (ЕСПД)), включая исходные тексты программ. По выпущенной программной документации проводится процесс

верификации разработанных программных изделий на предмет их соответствия требованиям частных технических заданий. Учитывая относительную простоту и ограниченную функциональность программных изделий, входящих в состав ПТК, класс безопасности разрабатываемого устройства, использование в составе ПИ предварительно разработанных программных средств, представляется возможным опустить на данном этапе требование МЭК 880 о независимом аудите исходных текстов программных изделий, заменив его отладкой с использованием инструментальных средств общего назначения и расширенными испытаниями алгоритмов функционирования интегрированного ПТК на пятом этапе.

На этапе 4 работ в соответствии с программной документацией производится изготовление программных изделий (программирование носителей), интегрирование ПИ и оборудования в единый программно-технический комплекс (установка ПИ в состав оборудования ПТК) и предварительное тестирование интегрированного ПТК. По результатам интегрирования ПТК проводятся необходимые отладочные мероприятия с использованием программно-аппаратных средств общего назначения (отладчики, эмуляторное оборудование), разрабатывается и корректируется программная и пользовательская документация. К четвертому этапу работ относится разработка и изготовление специализированного тестового оборудования и программного обеспечения для проведения автономных и комплексных испытаний разрабатываемого ПТК в составе электрооборудования СУЗ.

На этапе 5 работ проходят автономные валидационные испытания ПТК как единого целого. Испытания проводятся по трем основным направлениям:

- расширенные автономные испытания алгоритмов функционирования ПИ, входящих в состав ПТК, проводимые на опытных образцах ПТК с использованием специализированного тестового оборудования и программного обеспечения, разработанного на предыдущем этапе. Данные испытания предусматривают максимально полную проверку алгоритмов функционирования ПИ в составе ПТК, глубина которой ограничивается только возможностями используемого испытательного оборудования. Испытания проходят в объеме существенно превышающем стандартные функциональные испытания и заменяют собой для ПТК класса безопасности 3Н автономные испытания программных модулей, предусмотренные МЭК 880;

- функциональные испытания опытных образцов ПТК совместно с реальным технологическим оборудованием для

проверки правильности программно-аппаратных решений, заложенных при разработке. В качестве примера подобных испытаний можно привести испытания опытного образца шкафа контроля и управления ПКУ1М, в составе управляющего и информационно-регистрирующего комплекса на стенде горячей обкатки приводов В-1000 в ОКБ “Гидропресс” г. Подольск Московской области, в условиях реального функционирования с датчиками ДПШ приводов органов регулирования реактора ШЭМ-3.

- сокращенные функциональные испытания поставочных образцов ПТК в рамках приемо-сдаточных и приемочных испытаний с использованием тестового оборудования и программного обеспечения.

По результатам проведенных испытаний вносятся необходимые изменения в конструкторскую, программную и эксплуатационную документацию.

На этапе 6 работ проходят комплексные валидационные испытания ПТК в составе стендовых и полигонных фрагментов электрооборудования СУЗ. Испытания проводятся как на имеющихся в НПП ВНИИЭМ стендах с использованием тестового оборудования и имитаторов для отработки совместного функционирования законченных фрагментов электрооборудования СУЗ (два и более шкафов из состава электрооборудования СУЗ, объединенных сетевыми и проводными связями по штатной схеме), так и на специализированных полигонах сторонних организаций для проверки интерфейсов взаимодействия различных уровней АСУ ТП энергоблока.

Данный этап завершает цикл работ по верификации и валидации ПТК на этапах разработки и изготовления.

По результатам каждого из рассмотренных выше этапов подготавливается отдельный отчет о выполненных работах. К отчетам прикладываются копии всех необходимых документов, позволяющие, в соответствии с требованиями МЭК 880, обеспечить возможность их проверки лицами, не занятыми непосредственно в разработке системы и в программе верификации.

Окончание работ по верификации и валидации ПТК фиксируется актом, согласованным с представителями уполномоченных надзорных органов. Выпускается итоговый информационный отчет о результатах верификации и валидации, включаемый в состав документации соответствующего ПТК.

Рассмотренная в статье процедура была в той или иной форме успешно применена при проведении верификации и валидации шкафов ПКУ1М, АРМ6М, шкафов АРМ5СРВ и РОМ5СРВ для Ново-Воронежской станции, при квалификации электрооборудования для АЭС «Тяньвань».