УДК 681.51

ПРИМЕНЕНИЕ ПЛАТФОРМЫ RadiCS ДЛЯ РАЗРАБОТКИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ АЭС

А.В. ДИТЯШЕВ

ПАО «НПП «Радий»
Героев Сталинграда, 29, Кировоград, 25009,Украина

Поступила в редакцию 6 февраля 2015

История ПАО «НПП «Радий»

ПАО «НПП «Радий» основано 1 января 1954 г. Основным направлением деятельности в период с 1954 по 1995 гг. было производство абонентских громкоговорителей, электробытовых изделий, оснащения телевизионных комплексов, передвижных телевизионных станций, телевизионных и радиовещательных передатчиков, аппаратуры кабельного телевидения и динамических громкоговорителей. В период с 1982 по 1989 гг. предприятие участвовало в разработке и поставке оборудования стартовых комплексов «Энергия» и «Буран».

Эволюция технических средств для разработки АСУ ТП АЭС

С 1995 г. НПП «Радий» приступило к серийному изготовлению и поставке аппаратуры унифицированного комплекса технических средств (УКТС) для автоматизированных систем управления технологическими процессами (АСУ ТП) атомных электростанций (АЭС).

Вслед за этим на предприятии было разработано новое поколение блоков УКТС ДПИ с цифровой обработкой сигналов помехоустойчивого исполнения со встроенной функцией диагностики. Для реализации типовых функций блоков впервые были применены программируемые вентильные матрицы, построенные на FPGA-архитектуре. Всего на АЭС было поставлено 15 комплексов управляющей системы безопасности первого поколения, которые содержат более 50 000 чипов FPGA. С 2000 г. НПП «Радий» на основании опыта поставок и эксплуатации комплексов I-поколения было разработано II-е поколение цифровых измерительных и управляющих систем (измерительно-управляющая платформа «Radiy») с применением FPGA от ведущих мировых производителей.

Платформа RadiCS

Третьим поколением систем, построенных на базе FPGA, является платформа RadiCS. Цифровая информационно-управляющая платформа RadiCS разработана в 2010–2011 гг. на основе более чем 10-летнего опыта разработки, производства, эксплуатации и обслуживания цифровой платформы Radiy. Платформа RadiCS представляет собой совокупность модулей, а также дополнительных средств для их программирования. Работа модулей платформы основана на применении чипов FPGA в качестве вычислительных, обрабатывающих информацию и управляющих системных устройств.

Характеристики платформы RadiCS:

– смоделирована на основе FPGA;

– соответствует требованиям стандарта МЭК 61508:2010 по уровню SIL 3 сертификации (при построении в одноканальном варианте);

– специально разработана для информационно-управляющей системы (ИУС)

безопасности, связанной с нормальной эксплуатацией;

– обеспечивает высокую надежность, функциональную и информационную безопасность;

– имеет полностью проверенный и испытанный диапазон входных и выходных сигналов;

– гибкое управление избыточностью/резервированием;

– всеобъемлющая «онлайн» диагностика;

– малое время реакции (менее 5 мс);

– возможность горячей замены модулей;

– высокая устойчивость к внешним воздействиям (в т. ч. к сейсмическим).

Описание технологии FPGA

Технология FPGA является альтернативой микропроцессорным и другим технологиям, основанным на различных типах программируемых логических устройств. Физически FPGA является комплексным полупроводниковым программируемым устройством, которое может быть сконфигурировано для выполнения функций, необходимых заказчику. Данное устройство включает в себя микросхему FPGA, представляющую собой аппаратные средства, которые можно оценить на предмет соответствия требованиям аппаратных квалификационных испытаний, а также электронный проект FPGA, представленный в виде набора инструкций на языке описания аппаратных средств, который может быть верифицирован на предмет соответствия функциональным требованиям.

Особенности технологии FPGA:

– реализация функций безопасности без использования какого-либо программного обеспечения и операционной системы;

– оптимизация времени, необходимого для проверки программного обеспечения на стадии проектирования;

– гибкость платформы ИУС, которая может быть сконфигурирована для любого типа функций и конструкций реакторов;

– простота модификации управляющей логики без необходимости модификации аппаратного обеспечения;

– возможность выполнения всех требований безопасности в интегрированных системах безопасности ИУС;

– устойчивость к внутренним ошибкам и внешним воздействиям;

– устойчивость к устареванию оборудования из-за переносимости кода языка описания аппаратного обеспечения (HDL) на FPGA-чипы различных поколений и производителей;

– повышенная защищенность от киберугроз по сравнению с устройствами основывающимися на технологии программируемого логического контроллера (PLC);

– использование кодов HDL (обычно в VHDL или Verilog) без необходимости использования операционной системы для программирования FPGA. В настоящее время нет никаких известных вирусов и вредоносных программ для HDL;

– дизайн и работа продуктов на базе FPGA не полагается на операционную систему и, следовательно, не имеют скрытых, неиспользуемых возможностей, которые могут подвергаться атакам;

– HDL код находится во флэш-памяти (отдельном чипе), к физической модификации которого доступа нет;

– программирование и перепрограммирование FPGA может быть осуществлено только при помощи специального интерфейса. Невозможно подключить централизованную среду для хранения информации или коммуникационные устройства, которые могут заразить код логики управления, как это было в случае с вредоносной программой w32.Stuxnet;

– возможности для наглядного и простого представления как процессов инжиниринга и проверки, так и реализованной логики работы устройства;

– возможность глубокой валидации и верификации как платформенного, так и пользовательского программного обеспечения.

Сравнение технологии FPGA с микропроцессорной техникой

В отличие от систем, построенных на микропроцессорах, технология FPGA позволяет реализовать параллельную обработку всех алгоритмов управления в течение одного цикла и проверенных детерминистических характеристик синхронизации в результате параллельной работы алгоритмов управления. Также важным свойством платформы RadiCS является отсутствие угрозы возникновения отказа по общей причине, что достигается благодаря отсутствию какого-либо программного обеспечения и операционной системы. Таким образом, элементы платформы RadiCS характеризуются повышенной надежностью в сравнении с платформами, основанными на микропроцессорных элементах.

Минимальная канальная конфигурация информационно-управляющих систем безопасности, основанная на платформе RadiCS, состоит из одного логического канала (шасси), который содержит два резервированных логических модуля (выполняющих функции логической обработки, управления и диагностики), что улучшает безопасность и надежность платформы, и до 14 других модулей (входных/выходных и оптических связей) в любой их комбинации. Основной комплект типов входных/выходных модулей содержит модуль аналоговых входов, модуль дискретных входов, модуль дискретных выходов и модуль аналоговых выходов (модуль управления силовыми приводами). Также для систем контроля нейтронного потока предусмотрен входной модуль специального назначения для приема сигналов с ультранизким уровнем токов – модуль измерения нейтронного потока. Модуль оптической связи может быть использован для расширения систем до конфигурации, включающей в себя множество шасси (см. рис. 1). Кроме того, возможно обеспечение межканальных связей между 2, 3 или 4 каналами информационно-управляющих систем с помощью оптоволоконных связей напрямую между их логическими модулями или образованных с помощью модулей оптической связи.

Рис. 1. Описание шасси

Логический модуль обрабатывает данные от входных модулей и данные каналов связи в соответствии со сконфигурированной пользователем логикой, обсчитывает текущее состояние системы согласно сконфигурированной логике, обновляет величины управляющих сигналов для выходных модулей, собирает диагностические данные и данные об общем состоянии работоспособности системы от всех модулей входов/выходов и от второго логического модуля, установленных в том же шасси. Модули входов/выходов обеспечивают интерфейсы с другими устройствами (например, детекторами, датчиками, сенсорами, приводами, устройствами сигнализации и прочими источниками входной информации). Функциональность каждого модуля определяется логикой, запрограммированной в соответствующей FPGA.

Квалифицированный по результатам испытаний информационно-управляющий канал на основе платформы RadiCS обеспечивает защищенные внешние интерфейсы для работы входов/выходов; резервированное питание за счет двух независимых источников электропитания; защищенные от потери информации линии связи; надежную работу локальных входов/выходов (от встроенных в шасси/шкафы детекторов/сенсоров/ключей или к индикаторам). Внутренние интерфейсы шасси обеспечивают связь установленных в шасси модулей посредством выделенных изолированных высокоскоростных коммуникационных линий связи (LVDS).

Сертификация по SIL3

Компания exida L.L.C. 26 сентября 2014 г. присвоила ПАО «НПП «Радий» сертификат, подтверждающий, что платформа RadICS на базе FPGA производства ПАО «НПП «Радий» успешно прошла оценку согласно требованиям стандарта МЭК 61508:2010, части 1–7. Платформа RadICS была признана соответствующей требованиям, обеспечивая уровень полноты безопасности SIL3 при однократном исполнении. Контроллер может быть применен для разработки приложений уровня SIL3. Таким образом, платформа RadICS производства ПАО «НПП «Радий» является единственной в мире платформой, разрешенной для применения в разработке АСУ ТП АЭС и удовлетворяющая требованиям SIL3 в одном канале.

Жизненный цикл проекта разработки АСУ ТП АЭС

Структура жизненного цикла проекта разработки АСУ ТП АЭС на ПАО «НПП «Радий» является результатом применения обширного профильного опыта и соответствует всем отраслевым стандартам (например, МЭК 61508, МЭК 61513, МЭК 60880, МЭК 60987). Следующее изображение кратко характеризует основные этапы жизненного цикла и дает один из вариантов V-образной модели, применение которой для построения процессов и разработки продуктов приводит к требуемому уровню SIL.

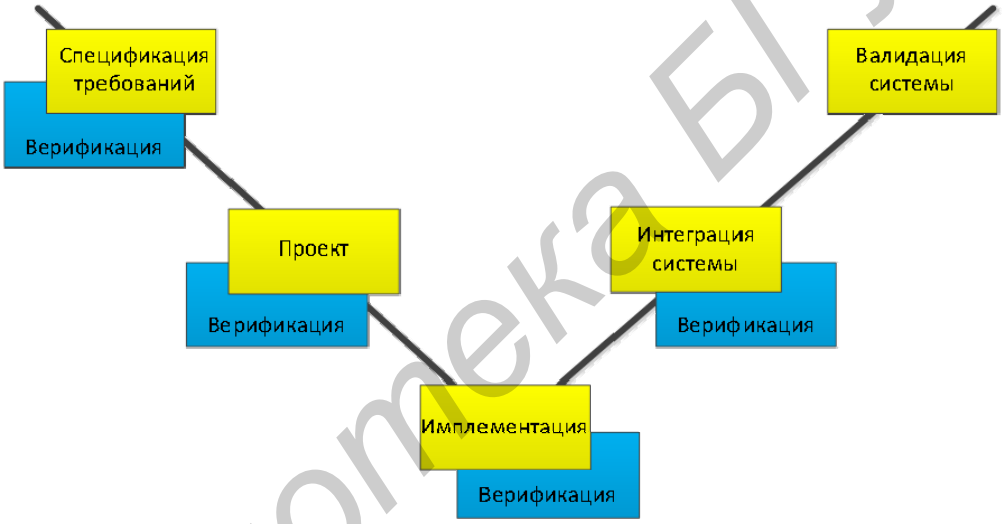

Рис. 2. V-образная модель, характеризующая основные этапы жизненного цикла проекта разработки АСУ ТП АЭС

Рассмотрим более подробно этапы жизненного цикла проекта разработки АСУ ТП АЭС.

1. *Спецификация требований*. Точкой отчета жизненного цикла является анализ технического задания от заказчика. Специалисты ПАО «НПП «Радий» – инженеры СКУ, технологи, специалисты по программному и аппаратному дизайну, верификаторы и валидаторы – оценивают и анализируют техническое задание и сопутствующую документацию. Результатом их работы является составление базовой конфигурации оборудования, подлежащей согласованию с заказчиком.

2. *Проект*. На этапе инжиниринга составляются подробные планы программных и аппаратных средств, а также планы верификации и валидации.

3. *Имплементация*. Следующий этап – реализация детализованной конфигурации оборудования в физические аппаратные средства и программный код, а также проведение проверки системы методами верификации на соответствие исходного задания.

4. *Интеграция системы* предполагает сведение укомплектованных шкафов с загруженным программным кодом в единый комплекс и всестороннее тестирование по заранее сформулированному плану. Подобные испытания производятся на полигонной площадке на территории ПАО «НПП «Радий», а затем повторяются и углубляются в период пуско-наладки на площадке конечного использования.

5. *Валидация системы* происходит после построение полного ПТК и гарантирует соответствие комплекса исходным требованиям.

Как видно из представленной схемы, каждый этап жизненного цикла сопровождается верификацией системы на соответствие поставленным требованиям. В результате, итоговый продукт полностью соответствует тем требованиям, которые предъявил заказчик и гарантированно готов к выполнению своих функций на протяжении заявленного периода эксплуатации. Существующие в пределах жизненного цикла процессы и процедуры гарантируют создание продукта, соответствующего высоким стандартам качества и надежности, и являются обязательными для всех проектов, реализуемых ПАО «НПП «Радий». При этом в случае необходимости и запроса со стороны заказчика, процессы жизненного цикла могут быть дополнены опциональными тестами, документами или процедурами.

Референтность

Платформа RadICS на основе FPGA используется для большинства критических, требующих высокой надежности и функциональной безопасности систем АСУ ТП АЭС. Примером таких систем являются следующие комплексы:

– ПТК аварийной и предупредительной защиты реактора (АЗ-ПЗ);

– ПТК автоматического регулирования и ограничения мощности реактора, ускоренной предварительной защиты (АРМ-РОМ-УПЗ);

– управляющая система безопасности (УСБ);

– система группового и индивидуального управления и защиты (СГИУ);

– система нормальной эксплуатации реакторного и турбинного отделений (СНЭ РО и СНЭ ТО);

– ПТК автоматического регулирования, контроля, управления защиты (АРКУЗ) для исследовательских реакторов.

За последние годы на основе платформы RadICS и Radiy были реализованы и находятся в стадии разработки следующие проекты для строящихся (РАЭС-3,4 и ХАЭС-1,2) и модернизируемых блоков АЭС:

– совместный проект НПП «Радий» с EdF: I&C Test Platform for EdF;

– АЭС Эмбалсе (Аргентина): система сигнализации БЩУ и РЩУ и система контроля скорости вращения ГНЦ;

– исследовательский реактор IEA-R1, институт IPEN-CNEN (Сан-Пауло, Бразилия): ПТК АКНП и панель ЧМИ для БЩУ;

– опыт применения в Украине:

Запорожская АЭС:	ПТК АЗ-ПЗ (основной и диверсный) все 6 блоков
	ПТК АРМ-РОМ-УПЗ 3 блока
	Симулятор ПТК АЗ-ПЗ
Южноукраинская АЭС:	ПТК АЗ-ПЗ (основной и диверсный) 3 блока
	ПТК АРМ-РОМ-УПЗ 2 блока
	ПТК УСБ 2 блока
	ПТК КЭ СУЗ 2 блока
Хмельницкая АЭС:	ПТК АЗ-ПЗ (основной и диверсный) 2 блока
	ПТК АРМ-РОМ-УПЗ 2 блока
Ровенская АЭС:	ПТК АЗ-ПЗ (основной и диверсный) все 4 блока
	ПТК АРМ-РОМ-УПЗ 2 блока
	ПТК УСБ 2 блока
	ПТК СНЭ 2 блока

– опыт применения в Болгарии:

АЭС Козлодуй:	ПТК КЭ СУЗ, ПТК УСБ блоки 5 и 6.