УДК 621.039.058

Е.С. БАХМАЧ[1], А.А. СИОРА[1], В.В. СКЛЯР[2], В.И. ТОКАРЕВ[1], В.С. ХАРЧЕНКО[3]

[1]*ЗАО «Радий», Украина*
[2]*Государственный научно-технический центр по ядерной и радиационной безопасности, Украина*
[3]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*

ОБЕСПЕЧЕНИЕ И ОЦЕНКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АЭС НА БАЗЕ ПЛИС

Обобщена структура программного обеспечения, разработанного ЗАО «Радий» для информационных и управляющих систем АЭС. Выполнен анализ особенностей оценки и обеспечения безопасности информационных и управляющих систем АЭС, разработанных с использованием программируемых логических интегральных схем (ПЛИС). Приведены результаты внедрения и эксплуатации ПЛИС в составе систем АЭС.

системы безопасности АЭС, ПЛИС-технологии

Постановка задачи и обзор публикаций

За период с 2003 г. ЗАО «Радий» разработало и поставило на энергоблоки АЭС Украины следующие программно-технические комплексы (ПТК), являющиеся основными компонентами информационных и управляющих систем (ИУС):

– ПТК системы аварийной и предупредительной защиты реактора (ПТК АЗ-ПЗ) [1];

– ПТК системы автоматического регулирования, разгрузки и ограничения мощности реактора и ускоренной предупредительной защиты (ПТК АРМ-РОМ-УПЗ) [2];

– ПТК системы группового и индивидуального управления приводами органов регулирования системы управления и защиты реактора (ПТК СГИУ);

– ПТК управляющей системы безопасности (ПТК УСБ).

Кроме того, для Института ядерных исследований НАНУ был разработан ПТК автоматического регулирования, контроля, управления и защиты исследовательского реактора ВВР-М (ПТК АРКУЗ).

ПО перечисленных выше ПТК обладает следующими основными особенностями:

– сложность и многокомпонентность структуры программного обеспечения (ПО) ПТК; ПО ПТК включает компоненты ПО верхнего уровня и компоненты ПО нижнего уровня, в состав которого также входит ПО, реализующее технологические алгоритмы формирования сигналов в среде ПЛИС;

– ПЛИС, наряду с микропроцессорами, промышленными компьютерами и т.п., являются программируемыми компонентами; таким образом, проекты ПЛИС могут быть рассмотрены, как специфический вид ПО;

– для реализации функций ПО нижнего уровня применяются программируемые логические интегральные схемы (ПЛИС);

– в ПТК АЗ-ПЗ, согласно требований национальных и международных стандартов [3], для выполнения функции аварийной защиты реализована программно-аппаратная диверсность на основе применения различных программируемых компонентов.

Теоретическое обоснование возможности построения информационных и управляющих систем АЭС на базе ПЛИС проводилось в работах [4-7].

Целью статьи является анализ особенностей проектов ПЛИС, как специфической разновидности ПО, а также особенностей обеспечения и оценки безопасности проектов ПЛИС, реализующих управляющие функции ИУС АЭС.

1. Анализ структуры и состава программного обеспечения разработки ЗАО «Радий»

ПТК, входящие в ИУС АЭС и разработанные ЗАО «Радий», включают верхний и нижний уровни.

ПО верхнего уровня ПТК разработано на языке программирования С++. ПО выполняется на IBM-совместимой рабочей станции под управлением операционной системы Microsoft Windows XP. Основными функциями ПО верхнего уровня является отображение и регистрация оперативной и диагностической информации.

На нижнем уровне ПТК разработки ЗАО «Радий» применяется ПО следующих трех типов:

– технологические алгоритмы защит, блокировок, управления и регулирования, разрабатываемые в графическом виде и на языке проектирования аппаратуры VHDL в среде ПЛИС; для основного комплекта ПТК АЗ-ПЗ и ПТК АРМ-РОМ-УПЗ применяются ПЛИС семейства Cyclone фирмы Altera; для диверсного комплекта ПТК АЗ-ПЗ, ПТК СГИУ и ПТК УСБ применяются ПЛИС семейства Cyclone II фирмы Altera;

– ПО на языке Assembler, в качестве программируемых компонентов применяются микропроцессоры MSP430F149 фирмы Texas Instruments; ПО такого типа применяется в основном комплекте ПТК АЗ-ПЗ и в ПТК АРМ-РОМ-УПЗ;

– ПО на языке С, в качестве программируемых компонентов применяются ПЛИС Altera Cyclone; ПО функционирует в среде эмуляторов процессоров Altera Nios, которые имплементируются в логическую структуру ПЛИС; ПО такого типа применяется в диверсном комплекте ПТК АЗ-ПЗ, в ПТК СГИУ и в ПТК УСБ; следует отметить, что в блоках БФЗ применяется одна микросхема ПЛИС Altera Cyclone II, в логическую структуру имплементируется и ПО на языке С, и ПО, реализующее технологические алгоритмы.

В табл. 1 приведены результаты анализа структуры ПО нижнего уровня. В поле «Наименование ПО и блоков» указаны блоки ПТК, в составе которых применяются программируемые компоненты. В полях, соответствующих ПТК, для каждого из блоков указан тип применяемого ПО и тип программируемого компонента. Отметим, что помимо типовых блоков ввода аналоговых и дискретных сигналов, диагностики и формирования управляющих сигналов, в составе ПТК УСБ и ПТК СГИУ присутствуют блоки, наличие которых вызвано спецификой этих комплексов.

2. Особенности оценки и обеспечения безопасности ИУС АЭС, разработанных с использованием ПЛИС

В настоящее время существует два основных способа построения ИУС – на базе микропроцессорных технологий (с использованием традиционного ПО) и на базе ПЛИС-технологий. Возникает вопрос: какая из технологий является более приемлемой для разработки ИУС АЭС? Очевидно, что для критических объектов выбор должен быть сделан в пользу решений, обеспечивающих более высокий уровень безопасности. В свою очередь, подобное сравнение двух альтернатив (микропроцессоров и ПЛИС) возможно при проведении для них сравнительного анализа рисков [4]. Следует отметить, что хотя ЗАО «Радий» применяет для разработки систем, в том числе, и микропроцессоры, однако, технологические алгоритмы защит, блокировок, управления и регулирования реализуются только в среде ПЛИС.

Проведенный анализ показал, что риски, связанные с применением ПЛИС и микропроцессоров в ИУС АЭС, могут быть разделены на две группы:

– общие риски, связанные с нарушением требований стандартов к ИУС АЭС;

– специфические риски, связанные с реализацией схемотехнических решений.

Таблица 1

Результаты анализа структуры ПО нижнего уровня ПТК разработки ЗАО «Радий»

Наименование ПО и блоков	ПТК разработки ЗАО «Радий»				
	ПТК АЗ-ПЗ, основной комплект	ПТК АЗ-ПЗ, диверсный комплект	ПТК АРМ-РОМ-УПЗ	ПТК СГИУ	ПТК УСБ
ПО блоков ввода аналоговых сигналов, БВА	ЯП Assembler, процессоры Texas Instruments MSP430F149	ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone	ЯП Assembler, процессоры Texas Instruments MSP430F149	–	ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone
ПО блоков ввода аналоговых сигналов от термопар, БВТ	то же	то же	то же	–	то же
ПО блоков ввода дискретных сигналов, БВД	то же	то же	то же	–	то же
ПО блоков диагностики, БДН	то же	то же	то же	ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone	то же
ПО блоков сигнализации БС	то же	ЯП Assembler, процессоры Texas Instruments MSP430F149	то же	–	–
ПО блоков, специфических для ПТК	–	–	–	ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone	ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone
ПО блоков формирования управляющих сигналов, БФЗ	алгоритмы – цифровые схемы и ЯП VHDL, ПЛИС Altera Cyclone; вспомогательное ПО – ЯП Assembler, процессоры Texas Instruments MSP430F149	алгоритмы – цифровые схемы и ЯП VHDL, ПЛИС Altera Cyclone II; вспомогательное ПО – ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone II	алгоритмы – цифровые схемы и ЯП VHDL, ПЛИС Altera Cyclone; вспомогательное ПО – ЯП Assembler, процессоры Texas Instruments MSP430F149	алгоритмы – цифровые схемы и ЯП VHDL, ПЛИС Altera Cyclone II; вспомогательное ПО – ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone II	алгоритмы – цифровые схемы и ЯП VHDL, ПЛИС Altera Cyclone II; вспомогательное ПО – ЯП С, эмуляторы процессоров Altera Nios в среде ПЛИС Altera Cyclone II

Рассмотрение специфических рисков, возникающих в случае применения ПЛИС [5], позволило сделать вывод, что риски данной группы незначительны, могут быть снижены с использованием стандартных или специальных апробированных решений и, следовательно, их наличие не приводит к существенному уменьшению преимуществ от применения ПЛИС в ИУС АЭС.

Что касается первой группы рисков, то применение ПЛИС позволяет достичь значительных преимуществ в снижении рисков нарушения требований к временным характеристикам ИУС, а также рисков невыявления скрытых дефектов в процессе верификации. Это утверждение может быть проиллюстрировано при помощи фрагмента проекта ПЛИС (рис. 1).

Защита № 12, 13
Алгоритм формирования сигналов АЗ
Отключение 3-х из 4-х, 2-х из 3-х, 1-го из 2-х работающих ГЦН при мощности реактора более 5% Nном с выдержкой времени 1,4 сек.
Отключение 2-х из 4-х работающих ГЦН одновременно или последовательно в течении времени менее 70 сек,
при N реактора более 75% Nном с выдержкой времени 6 сек.

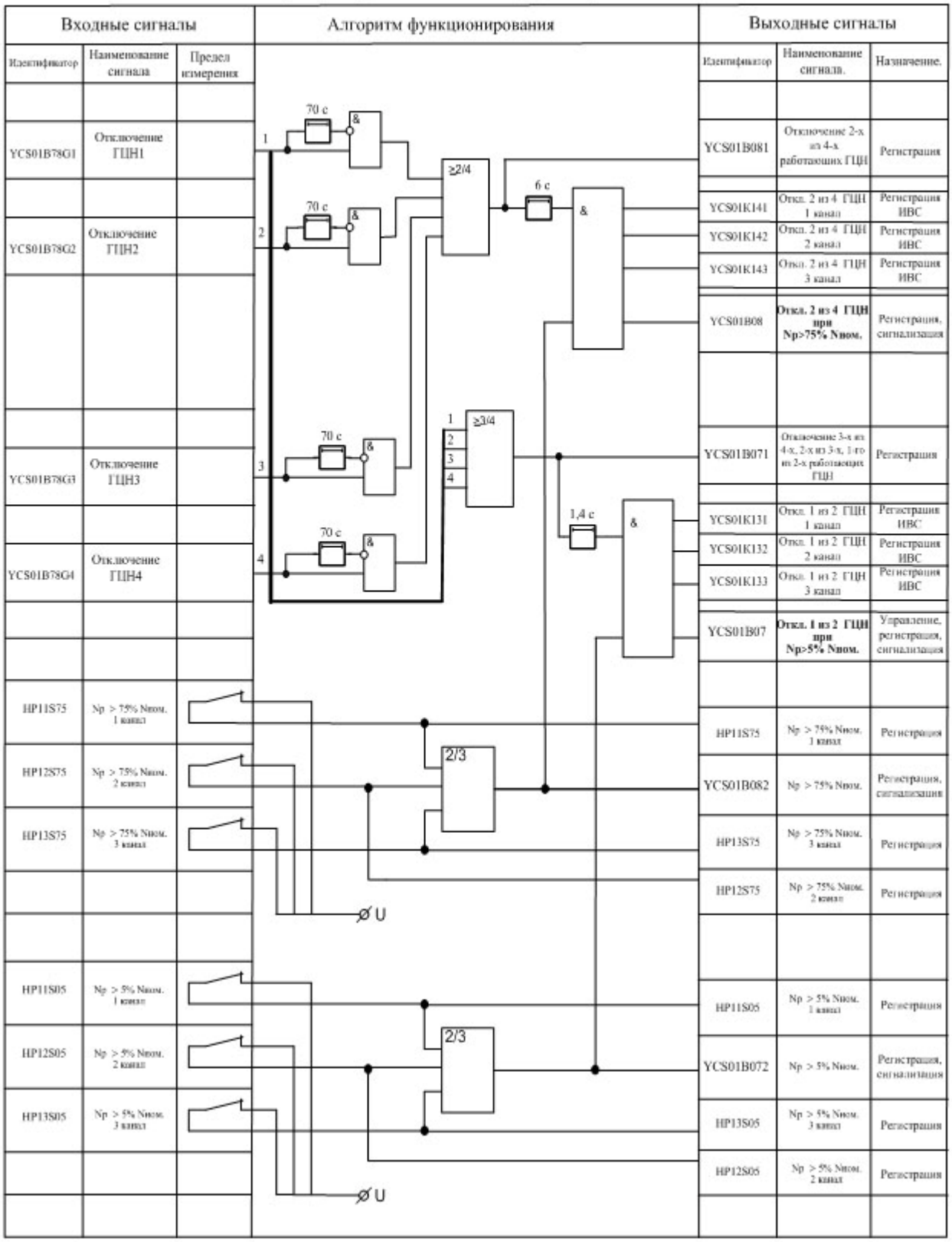

Рис. 1. Пример алгоритма формирования сигналов аварийной защиты ядерного реактора ВВЭР-1000, реализуемого проектом ПЛИС

Риск нарушения требований к временным характеристикам для ПЛИС ниже, чем для микропроцессоров. Схемотехнический подход к реализации алгоритмов обработки данных позволяет выполнить реальное распараллеливание процессов обработки и получить прозрачную структуру с детерминированными временными характеристиками. Кроме того, ПЛИС-реализация функций ИУС в конечном итоге является аппаратной реализацией, обеспечивающей более высокое быстродействие. В то же время, для микропроцессоров данная группа рисков не может быть равна нулю, если на протяжении одного вычислительного цикла решается большая группа задач (десятки и сотни алгоритмов, подобных рис. 1).

Идентичность проекта ПЛИС схемам технологических алгоритмов формирования сигналов управления исполнительными механизмами позволяет получить прозрачную структуру схемотехнического решения. Это позволяет облегчить процесс верификации за счет того, что верификатор работает не с программным кодом, а со схемой, сопоставимой с исходными данными для разработки. Указанные свойства ПЛИС позволяют снизить риски данной группы по сравнению с ПО микропроцессоров.

При разработке проекта ПЛИС реализуется реальное распараллеливание обработки данных в схеме ПЛИС. Реализация нециклических управляющих структур позволяет создать ИУС с гарантированными временными характеристиками. Для микропроцессоров, которые должны реализовать обработку всех данных за один цикл, практически невозможно реализовать задачу большой размерности с гарантированными временными характеристиками.

Кроме того, особенностью применения ПЛИС-технологий является реализация принципа разнообразия (диверсности) в ПТК АЗ-ПЗ. Под разнообразием подразумевается применение в разных системах (либо в пределах одной системы в разных каналах) различных средств и/или аналогичных средств, основанных на различных принципах действия, для осуществления заданной функции. Основная цель реализации принципа разнообразия – защита от отказов по общей причине.

Для ПТК АЗ-ПЗ разработаны основной и диверсный комплекты. Разнообразие реализуется путем применения в разных комплектах ПТК АЗ-ПЗ различных программно-аппаратных средств, а также различных подходов к разработке и различных команд разработчиков. Таким образом, для реализации разнообразия в ПТК АЗ-ПЗ одновременно применены следующие четыре способа [8]:

1) аппаратная диверсность – разнообразие достигается за счет использования различных технических средств (различных производителей или построенного по различным технологиям, например, с использованием различной элементной базы).

2) программная диверсность – разнообразие достигается за счет использования различных версий ПО;

3) проектная диверсность– разнообразие достигается за счет применения различных методов (подходов) проектирования аппаратных или программных средств;

4) субъектная диверсность – разнообразие достигается за счет использования различных исполнителей работ (команд исполнителей).

В табл. 2 представлены результаты анализа различий между ПО основного и диверсного комплектов ПТК АЗ-ПЗ. Различия были реализованы с использованием четырех указанных способов. Следует отметить, что указанные в табл. 2 аппаратная и программная диверсность должны рассматриваться в комплексе, поскольку по существу являются составляющими единой программно-аппаратной платформы для реализации разнообразия. Кроме того, в табл. 2 отдельно проанализирован способ реализации диверсности для каждой из двух составляющих ПО ПТК АЗ-ПЗ: для программного кода и для графической части проекта ПЛИС.

Таблица 2

Результаты анализа реализации принципа разнообразия (диверсности) для ПТК АЗ-ПЗ

Способ реализации разнообразия	Основной комплект ПТК АЗ-ПЗ	Диверсный комплект ПТК АЗ-ПЗ
Аппаратная диверсность	1) программный код: в качестве программируемых компонентов используется несколько процессоров Texas Instruments MSP430F149	1) программный код: в качестве программируемых компонентов используется ПЛИС Altera Cyclone в среде которой реализуется несколько эмуляторов процессоров Nios
	2) графическая часть: в качестве программируемых компонентов используется ПЛИС Altera Cyclone	2) графическая часть: в качестве программируемых компонентов используется ПЛИС Altera Cyclone II
Программная диверсность	1) программный код: разрабатывается на языке Assembler	1) программный код: разрабатывается на языке С
	2) графическая часть: разрабатывается на графическом языке представления схем	2) графическая часть: разрабатывается языке описания аппаратуры VHDL
Проектная диверсность	1) программный код: разрабатывается в среде Assembler фирмы IAR Systems с применением методов программирования на языке Assembler	1) программный код: разрабатывается в среде САПР Quartus и эмулятора процессора Nios фирмы Altera с применением методов программирования на языке высокого уровня
	2) графическая часть: разрабатывается в среде САПР Quartus с применением методов синтеза цифровых схем	2) графическая часть: разрабатывается в среде САПР Quartus с применением методов программирования на языке описания аппаратуры VHDL
Субъектная диверсность	ПО основного и диверсного комплектов ПТК АЗ-ПЗ разрабатывается различными группами программистов	

Для всех планов и отчетов по верификации ПО ПТК, разработанных ЗАО «Радий», проводилась экспертиза ядерной и радиационной безопасности [3]. В ходе экспертизы проводилась оценка соответствия ПО требованиям по безопасности, содержимся в национальных и международных нормативно-технических документов.

Национальные регулирующие требования к программному обеспечению включают следующие группы требований:

– к функциям, структуре и элементам ПО;

– к диагностированию и самоконтролю;

– к обеспечению защиты от отказов, искажений, ошибочных и несанкционированных действий;

– к разработке ПО;

– к верификации ПО.

Международные регулирующие требования к программному обеспечению, установленные в стандартах МАГАТЭ (Международного агентства по атомной энергии) и МЭК (Международной электротехнической комиссии), включают следующие группы требований:

– к простоте проектирования;

– к культуре безопасности;

– к классификации по безопасности;

– к защите в глубину и к разнообразию;

– к поддержке избыточности каналов и логики голосования;

– к контролю, диагностированию и устойчивости к отказам;

– к защищенности от несанкционированного доступа;

– к сопровождаемости;

– к тестируемости, трассируемости и обозримости;

– к интерфейсам ИУС и ПО;

– к реализации процесса разработки ПО;

– к использованию автоматизированных инструментальных средств;

– к использованию стандартов;

– к используемым методам;

– к обеспечению качества;

– к оценке третьей стороной;

– к временным и точностным характеристикам;

– к изложению функциональных требований;

– к изложению нефункциональных требований;

– к управлению конфигурацией;

– к этапу разработки требований к ИУС;

– к этапу проектирования ИУС;

– к этапу разработки требований к ПО;

– к этапу проектирования ПО;

– к этапу реализации ПО;

– к верификации ПО;

– к этапу интеграции ИУС;

– к валидации ИУС;

– к инсталляции и вводу в эксплуатацию;

– к эксплуатации;

– к модификации ПО после поставки;

– к применению и оценке ранее разработанного ПО;

– к документации.

Результаты оценки подтвердили соответствие ПО, разработанного ЗАО «Радий», указанным выше группам требований по безопасности.

3. Результаты применения ИУС на базе ПЛИС на энергоблоках АЭС

Начиная с 2003 г., ЗАО «Радий» разработало и внедрило на энергоблоках АЭС Украины с реактором ВВЭР-1000 двадцать ПТК, входящих в состав систем управления и защиты реактора (СУЗ) и управляющих систем безопасности (УСБ) (табл. 3). Кроме того, в настоящее время готовится внедрение ПТК СГИУ на энергоблоках Запорожской АЭС.

Таблица 3

Данные об эксплуатации ПЛИС в составе ПТК разработки ЗАО «Радий»

Дата ввода в эксплуатацию	Энергоблок АЭС	Наименование ПТК	Кол-во ПЛИС в составе ПТК
Май 2003	Блок №1 Запорожской АЭС	АЗ-ПЗ (основной комплект)	3
Май 2004	Блок №1 Запорожской АЭС	АЗ-ПЗ (диверсный комплект)	3
Сентябрь 2004	Блок №2 Хмельницкой АЭС	АЗ-ПЗ (основной комплект)	3
Сентябрь 2004	Блок №2 Хмельницкой АЭС	АРМ-РОМ-УПЗ (1-й комплект)	6
Сентябрь 2004	Блок №4 Ровенской АЭС	АЗ-ПЗ (основной комплект)	3
Сентябрь 2004	Блок №4 Ровенской АЭС	АЗ-ПЗ (диверсный комплект)	3
Октябрь 2004	Блок №4 Ровенской АЭС	АРМ-РОМ-УПЗ (1-й комплект)	6
Ноябрь 2004	Блок №3 Запорожской АЭС	АЗ-ПЗ (диверсный комплект)	34
Ноябрь 2004	Блок №3 Запорожской АЭС	АРМ-РОМ-УПЗ (один канал)	2
Май 2005	Блок №1 Запорожской АЭС	АРМ-РОМ-УПЗ	6
Октябрь 2005	Блок №1 Южно-Украинской АЭС	АЗ-ПЗ (основной комплект)	3
Октябрь 2005	Блок №1 Южно-Украинской АЭС	АЗ-ПЗ (диверсный комплект)	34
Октябрь 2005	Блок №1 Южно-Украинской АЭС	АРМ-РОМ-УПЗ	6
Октябрь 2005	Блок №1 Южно-Украинской АЭС	УСБ-3	339
Ноябрь 2005	Блок №2 Хмельницкой АЭС	АЗ-ПЗ (диверсный комплект)	3
Ноябрь 2005	Блок №2 Хмельницкой АЭС	АРМ-РОМ-УПЗ (2-й комплект)	6
Декабрь 2005	Блок №3 Ровенской АЭС	АЗ-ПЗ (основной комплект)	3
Апрель 2006	Блок №4 Ровенской АЭС	АРМ-РОМ-УПЗ (2-й комплект)	6
Май 2006	Блок №2 Южно-Украинской АЭС	АЗ-ПЗ (основной комплект)	34
Сентябрь 2006	Блок №1 Южно-Украинской АЭС	УСБ-2	376

Из табл. 3 следует, что за период с 2003 г. по настоящее время в аппаратуре СУЗ и УСБ, установленной на семи энергоблоках АЭС Украины с реакторами ВВЭР, было использовано около 900 микро-

схем фирмы Altera. За этот период не было зарегистрировано ни одного отказа ПЛИС. Максимальный срок эксплуатации имеет ПТК АЗ-ПЗ (основной комплект) энергоблока № 1 Запорожской АЭС – более трех с половиной лет. Суммарная наработка ПЛИС всех ПТК АЭС на январь 2007 г. составила более 6 млн. реакторо-часов.

Выводы

Особенностью программно-технических комплексов для АЭС, разрабатываемых ЗАО «Радий», является широкое применение ПЛИС для реализации управляющих функций.

Схемы проектов ПЛИС эквивалентны технологическим алгоритмам формирования сигналов управления исполнительными механизмами АЭС. Таким образом, в отличие от процесса разработки программного обеспечения, для проектов ПЛИС при переходе от одного этапа разработки к другому исходная информация для разработки изменяется незначительно, что снижает риск ее искажения и риск внесения дефектов. Физическое распараллеливание алгоритмов внутри кристалла ПЛИС позволяет создавать системы с детерминированными временными характеристиками.

Согласно результатам эксплуатации ПТК на энергоблоках АЭС Украины, можно сделать вывод о том, что реализация функций защит, блокировок, управления и регулирования на базе ПЛИС является наиболее эффективным средством для разработки ИУС, соответствующих требованиям украинских и международных нормативно-технических документов по безопасности [3].

Литература

1. Программно-технические комплексы аварийной и предупредительной защиты ядерных реакторов: обеспечение и оценка безопасности / Е.С. Бахмач, С.В. Виноградская, Ю.В.Розен и др. // Ядерная и радиационная безопасность. - 2005. – Т. 8, № 1. – С. 21-50.

2. Программно-технические комплексы автоматического регулирования, разгрузки и ограничения мощности реактора и ускоренной предупредительной защиты: обеспечение и оценка безопасности / Е.С. Бахмач, С.В. Виноградская, Ю.В. Розен и др. // Ядерная и радиационная безопасность. - 2005. – Т. 8, № 1. – С. 67-90.

3. Безопасность атомных станций: Информационные и управляющие системы / М.А. Ястребенецкий, В.Н. Васильченко, С.В. Виноградская и др. – К.: Техніка, 2004. – 472 с.

4. Скляр В.В., Харченко В.С., Ушаков А.А. Анализ безопасности и выбор технологий реализации информационно-управляющих систем АЭС: риск-ориентированный подход // Экология и ресурсы: Зб. научных трудов Института проблем национальной безопасности. – К.: ИПНБ. – 2006. – № 13. – С. 39-64.

5. Анализ рисков проектирования и эксплуатации цифровых систем на ПЛИС / А.А. Ушаков, А.В. Желтухин, В.В. Скляр и др. // Радіоелектронні і комп'ютерні системи. – 2006. – №. 7 (19). – С. 88-98.

6. Скляр В.В., Головир В.А. Метрики оценки сложности проектов ПЛИС, реализующих алгоритмы управления технологическим оборудованием АЭС // Радіоелектронні і комп'ютерні системи. – 2006. – №. 7 (19). – С. 82-87.

7. Скляр В.В., Харченко В.С., Ястребенецкий М.А. Особенности и оценка безопасности программного обеспечения информационных и управляющих систем АЭС Украины // Ядерные измерительно-информационные технологии. – 2006. – № 1 (17). – С. 3-18.

8. Preckshot G. Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems. NUREG/CR-6303. – Livermore, USA: Lawrence Livermore National Laboratory, 1994. – 35 p.

Поступила в редакцию 12.01.2007

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.