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]Научно-производственное предприятие «Радий», Украина
[2]Государственный НТЦ по ядерной и радиационной безопасности, Украина
[3]Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина

ПЛИС-ПЛАТФОРМА В КРИТИЧЕСКИХ ПРИЛОЖЕНИЯХ: ГАРАНТОСПОСОБНЫЕ МАСШТАБИРУЕМЫЕ РЕШЕНИЯ ДЛЯ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АЭС

Проанализированы этапы развития и результаты применения ПЛИС-технологий для построения масштабируемых платформ гарантоспособных ИУС критических объектов. Уточнена модель рисков и даны результаты анализа рисков для ПЛИС-технологий. Проанализированы возможности ПЛИС в контексте эволюции базовых принципов обеспечения гарантоспособности. Описаны особенности ПЛИС-платформы, разработанной НПП «Радий».

ИУС АЭС, ПЛИС-платформа, риски, гарантоспособность, многоверсионность, масштабируемость

Введение

Обеспечение заданной надежности и безопасности ИУС АЭС, других критических объектов зависит от уровня безотказности программно-аппаратных компонент, совершенства архитектурных решений, используемых методов и средств устойчивости к отказам, вызванным различными причинами (физическими и проектными дефектами, дефектами взаимодействия с внешней средой [1]), и других факторов [2]. Применение ПЛИС-технологий в таких системах позволяет решить ряд проблем благодаря, прежде всего, гибкому инструментарию разработки и реализации проектов и существенному упрощению процедур верификации.

В известных работах [3 – 5] описываются различные аспекты применения ПЛИС для создания отказоустойчивых и отказобезопасных устройств и систем, а также методы оценки и обеспечения их надежности. Однако, десятилетний опыт использования ПЛИС современного уровня сложности в критических приложениях, в том числе и при разработке ИУС АЭС, накопленный в Украине [5], требует детального осмысления и анализа. Такое исследование должно проводиться в контексте сравнения возможных рисков, которые имеют место при использовании микропроцессорных и ПЛИС-технологий, а также эволюции базовых принципов обеспечения гарантоспособности (надежности, функциональной и информационной безопасности) [6]. К их числу относятся принципы резервирования, независимости, а также принцип диверсности, реализация которого является одним из требований при разработке систем аварийной защиты реакторов АЭС [2].

Цель данной работы – анализ этапов развития и результатов применения ПЛИС-технологий для построения масштабируемых платформ гарантоспособных ИУС критических объектов. Для ее достижения решаются следующие задачи:

– уточняется модель рисков и даются результаты их анализа при использовании микропроцессоров и ПЛИС при создании ИУС АЭС (раздел 2);

– анализируются возможности и достоинства ПЛИС-технологий в контексте эволюции базовых принципов обеспечения гарантоспособности, в частности, принципа диверсности (раздел 3);

– описываются особенности масштабируемых решений для ИУС критических объектов на базе ПЛИС-платформы, разработанной НПП «Радий» (раздел 4).

2. Анализ рисков применения ПЛИС

Функциональная безопасность и модель рисков ИУС. Базовая модель рисков, возникающих в случае применения информационных технологий, разработана в стандарте [7]. Однако, данная модель направлена на обеспечение информационной безопасности (ИБ) (security), т.е. способности системы защищать информацию и данные от неавторизованного доступа и модификаций.

Для ИУС критических объектов наиболее важным является свойство функциональной безопасности (ФБ) (safety), под которой понимается часть общей безопасности объекта контроля и управления, относящаяся к ИУС и зависящая от ее правильного функционирования.

Соотношение между свойствами ИБ и ФБ зависит от типа системы. Для информационных систем хранения и обработки данных ФБ может являться составляющей ИБ или подчиненным ей свойством. Для информационно-управляющих систем критических объектов – обратная ситуация, когда ФБ является превалирующим свойством, входящим в гарантоспособность (dependability) [1,6] (рис. 1).

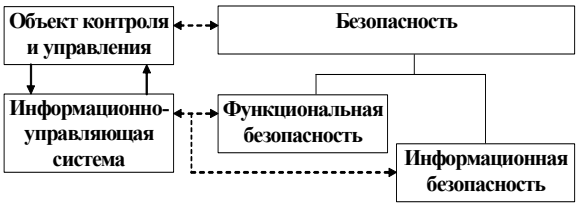

Рис. 1. Соотношения между свойствами ФБ и ИБ для ИУС критических объектов

В [2,8] дано понятие функциональной безопасности для ИУС и программного обеспечения (ПО). Общая концепция анализа рисков и модель рисков ИУС, предложенные в [3,9], основаны на формировании требований к ИУС в качестве критериев оценке и на последующем рассмотрении рисков, заключающихся в нарушении требований к ИУС. В [9] разработан метод сравнительного анализа рисков при внедрении в ИУС новых информационных технологий, а в [10] предложена модель ФБ, которая модифицирована для ИУС (рис. 2).

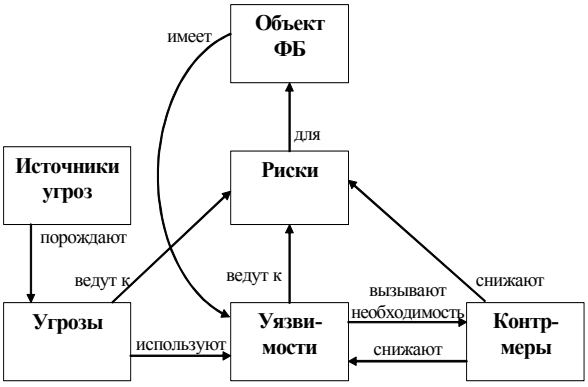

Рис. 2. Модель ФБ и рисков ИУС

Одним из показателей ФБ являются значения рисков [9]. Риск $R(t)$ за время t, связанный с некоторым событием определяется как произведение вероятности этого события $P(t)$ на неблагоприятные последствия D, вызванные этим событием, т.е.:

$$R(t) = P(t) \cdot D \,. \qquad (1)$$

Кроме численных значений рисков могут рассматриваться лингвистические значения (диапазоны значений, например, «низкий», «средний», «высокий»). Результаты анализа рисков представляются в виде матриц рисков, либо в виде ее трехмерной геометрической интерпретации (рис. 3), где разные уровни критичности, получаемые в зависимости от вероятности и ущерба, определяют значение третьей координаты (на вертикальной оси).

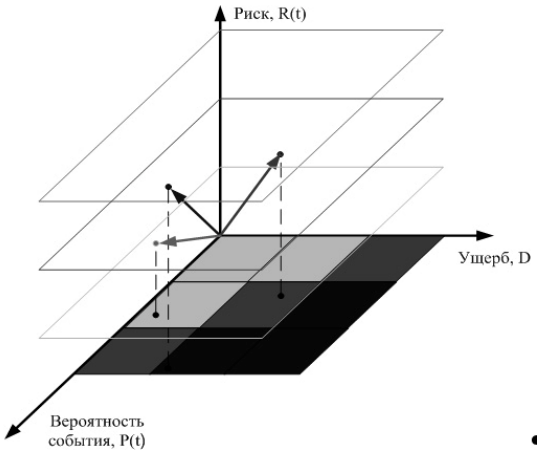

Рис. 3. Геометрическая интерпретация результатов анализа рисков

Анализ рисков применения ПЛИС и микропроцессоров в ИУС критических объектов. Подход, основанный на оценках возможного нарушения нормативных требований [3], использован для сравнительного анализа рисков применения в ИУС АЭС микропроцессоров (МП) и ПЛИС. В соответствии с проведенной идентификацией и классификацией рисков, они включают три группы (табл. 1):

1) риски, связанные со свойствами продуктов (ПЛИС и микропроцессоров);

2) риски, связанные с реализацией процессов жизненного цикла;

3) специфические риски, связанные с реализацией схемотехнических решений на базе ПЛИС.

Результаты анализа рисков [3] показали, что применение ПЛИС позволяет снизить (по сравнению с микропроцессорами) десять из шестнадцати видов общих рисков первой и второй группы. В то же время, исследование специфических рисков, возникающих в случае применения ПЛИС, показало, что они незначительны и могут быть снижены с использованием стандартных или специальных апробированных решений и, следовательно, их наличие не приводит к существенному уменьшению преимуществ применения ПЛИС в ИУС. Этот вывод усиливается еще и потому, что часть рисков, отнесенных к числу специфических для ПЛИС, характерна в той или иной форме и для МП, однако, их анализ (в соответствии с принятым консервативным подходом) не проводился.

Таблица 1

Модель рисков, связанных с применением ПЛИС и микропроцессоров в ИУС

Вид риска
1. Риски, связанные со свойствами продуктов
1.1. Риски нарушения требований к возникновению отказов по общей причине (ООП)
1.2. Риски нарушения требований к временным характеристикам
1.3. Риски нарушения требований по надежности
1.4. Риски нарушения требований к защите от искажения входной информации
1.5. Риски нарушения требований к защите от несанкционированного доступа (НСД)
1.6. Риски нарушения требований по стойкости к внешним воздействующим факторам (ВВФ)
1.7. Риски нарушения требований по стойкости к изменению параметров электропитания (ИПЭП)
1.8. Риски нарушения требований к по стойкости к электромагнитным ВВФ (ЭВВФ)
1.9. Риски нарушения требований к техническому диагностированию
2. Риски, связанные с реализацией процессов жизненного цикла
2.1. Риски нарушения требований к процессу разработки
2.2. Риски нарушения требований к процессу верификации
2.3. Риски нарушения требований к процессу эксплуатации
2.4. Риски, связанные с применением ранее разработанных проектов
2.5. Риски, связанные с применением системного программного обеспечения
2.6. Риски, связанные с применением прерываний
2.7. Риски, связанные с применением инструментальных средств (ИС) разработки и верификации (см. также риски 3.1)
3. Риски, связанные с реализацией схемотехнических решений на базе ПЛИС
3.1. Риски, связанные с применением САПР для разработки ПЛИС
3.2. Риски, связанные с отказами в ячейках памяти
3.3. Риски, связанные с отказами логических ячеек
3.4. Риски, связанные с отказами входов/выходов, настраиваемых пользователем
3.5. Риски, связанные с отказами электрических интерфейсов при обвязке одной микросхемы
3.6. Риски, связанные с отказами электрических интерфейсов при реализации проекта на нескольких микросхемах
3.7. Риски, связанные с отказами оконечной нагрузки тактирующих выводов (внешняя синхронизация)
3.8. Риски, связанные с ошибками внутренней синхронизации
3.9. Риски, связанные с ошибочным сбросом

3. Принцип диверсности и обеспечение гарантоспособности ИУС на ПЛИС

Эволюция реализации принципа диверсности. Позитивные выводы относительно применения ПЛИС, базирующиеся на риск-ориентированных оценках, следует дополнить анализом возможностей этой технологии с точки зрения реализации нормативных принципов обеспечения надежности и безопасности при создании ИУС. К числу таких, пожалуй, наиболее сложных и фундаментальных принципов относится принцип диверсности (разнообразия, многоверсионности) [2].

Анализ показывает, что за последние 30 лет в развитии подходов к реализации этого принципа в ИУС АЭС можно выделить три этапа:

1) *80-е годы* – переход от аппаратно-реализованных комплектов систем к схеме, когда один комплект (primary system) реализовывался аппаратно, т.е. на жесткой логике и использовалась предыдущая версия системы, а второй (secondary system) – с использованием программно-управляемого решения на микропроцессорах;

2) *90-е годы* – разработка первого и второго комплектов на идентичных или разных типах МП с использованием разных языков программирования. Пример такой системы – разработка системы аварийной защиты на основе МП Intel и Motorola с использованием языков C++ и Ada [2];

3) *2000-е годы* – использование ПЛИС для разработки обоих комплектов. При этом могут применяться кристаллы от разных производителей, различные технологии изготовления, автоматные модели, языки описания аппаратуры и т.д. [5].

Таким образом, эволюция реализации принципа диверсности является примером реализации диалектического закона *«отрицания отрицания»*, поскольку пройден цикл из двух переходов:

1) двухфазного «отрицания» двухкомплектных (недиверсных) систем на жесткой логике (HW и HW) диверсными системами с использованием программной реализации на МП (SW1 и SW2);

2) последующего «отрицания» двухкомплектных диверсных систем (SW1 и SW2) системами с диверсными комплектами на ПЛИС (ПЛИС1 и ПЛИС2), т.е. фактически комплектами на жесткой логике, «зашиваемой» в кристалл, хотя и с использованием специальных программных средств САПР.

Возможен еще один вариант реализации диверсных систем, когда их первый и второй комплекты реализуются с использованием МП и ПЛИС соответственно, однако, он сложен в реализации (из-за проблем с верификацией комплекта на МП) и неудобен в эксплуатации.

Более эффективным для некоторых типов систем может быть шаг, когда используются диверсные ПЛИС-проекты, базирующиеся на разных вариантах реализации так называемой технологии «soft» процессоров, при которой функции системы «зашиваются» в кристалл в виде многоверсионных процессорных IP-ядер [11]. Такой шаг фактически следует рассматривать как первую фазу следующего цикла «отрицания».

Широкий спектр вариантов реализации принципа диверсности привел к появлению и формализации понятия многоверсионной системы (МВС) и многоверсионной технологии (МВТ) [12].

Использование ПЛИС при разработке интеллектуального ядра ИУС – программно-технического комплекса создало уникальные возможности не только для теоретического расширения множества МВТ, а для их реального практического наполнения и обеспечения гарантоспособности систем в целом.

Свойства ПЛИС и обеспечение гарантоспособности. К свойствам ПЛИС, способствующим реализации механизмов гарантоспособности и снижению рисков, относятся следующие [5, 11, 13]:

1) *в части упрощения («прозрачности») процессов разработки и верификации:*

– возможность аппаратного распараллеливания выполнения алгоритмов и реализация каждой функции отдельными элементами ПЛИС;

– отсутствие циклических структур в проектах;

– идентичность представления проекта ПЛИС исходным схемотехническим решениям;

– наличие развитых средств тестирования в составе САПР;

– наличие верифицированных библиотечных компонентов и IP-ядер;

2) *в части обеспечения безотказности, достоверности и обслуживаемости:*

– возможность реализации резервирования на внутрикристальном и межкристальном уровнях;

– возможность реконфигурация и восстановления при отказах компонентов;

– возможность реализации расширенных процедур диагностирования;

3) *в части обеспечения информационной безопасности* – возможность реализации защиты от НСД благодаря тому, что перепрограммирование ее внутренней структуры, которое приведет к изменению выполняемых алгоритмов, осуществимо только с использованием специального оборудования;

4) *в части обеспечения стойкости и живучести*:

– устойчивость микросхемы ПЛИС к электромагнитным воздействиям и другим внешним воздействующим факторам;

– возможность реализации механизмов управляемой многоступенчатой деградации с использованием структурно-пространственной и других методов многопараметрической адаптации [12].

Подытоживая сказанное, следует обратить внимание на две возможности, предоставляемые ПЛИС-технологиями:

– во-первых, возможность *мультиреконфигурации*, включающей реконфигурацию реализуемых алгоритмов, функциональных [14] и надежностных [15] архитектур;

– во-вторых, возможность реализации так называемой *мультидиверсности* [16], когда в диверсных комплектах применяется несколько видов версионной избыточности – кристаллы от разных производителей, разные языки описания проектов и разные инструментальные средства. Другими словами, в мультидиверсной МВС может иметь место «кумулятивный» эффект от применения различных видов версионной избыточности, реализующих концепцию защиты в глубину [2], что, в свою очередь, может снизить вероятность отказа по общей причине.

4. Реализация гарантоспособных масштабируемых решений на базе ПЛИС-платформы «Радий»

Принципы построения и реализации платформы. Преимущества и возможности ПЛИС-технологий реализованы в *программно-аппаратной платформе*, разработанной на НПП «Радий». На базе этой платформы предприятием создан и поставлен на АЭС Украины ряд ИУС, которые успешно эксплуатируются в течение нескольких лет. Кроме того, платформа «Радий» используется и для создания других АСУ ТП.

Платформа «Радий» включает верхний и нижний уровни. *Верхний уровень* реализуется на покупных промышленных IBM-совместимых рабочих станциях, выполняющих следующие функции с использованием ПО собственной разработки:

– прием технологической и диагностической информации и реализация человеко-машинного интерфейса в составе БЩУ;

– отображение технологической информации по всем алгоритмам управления о ходе их выполнения составными частями ИУС, а также диагностической информации об отказах элементов;

– регистрация, архивирование и визуализация технологической и диагностической информации.

Нижний уровень включает типовые шкафы, состоящих из типовых функциональных блоков.

Особенностью платформы «Радий» является использование в качестве программируемых компонентов ПЛИС большой степени интеграции (1 млн.

и более логических вентилей). При создании ПЛИС-проектов применяются технологии разработки:

– графической схемы с использованием стандартных и дополнительных (собственных) библиотечных примитивов, реализованных в среде САПР;

– программной модели с использованием специальных языков описания цифровых устройств (VHDL, AHDL, Verilog и др.);

– программного кода, реализуемого в среде эмулятора микропроцессора, который имплементируется в кристалл ПЛИС в виде отдельного функционального ядра.

Платформа «Радий» реализует следующие решения, обеспечивающие гарантоспособность:

– платформа представляет собой универсальный комплекс программно-технических средств, пригодный для ИУС ректоров различных типов; кроме того, она может быть использована в системах контроля и управления любыми исполнительными механизмами в отраслях с повышенными требованиями к быстродействию, надежности и безопасности (нефтегазовый комплекс, металлургия, химическая промышленность и т.д.).

– платформа выполняет управляющие и другие критические для безопасности функции по принципу «жесткой» логики (в структуре ПЛИС для каждого алгоритма определены свои технические средства), без применения ПО; ПО реализует функции диагностирования, передачи данных между частями ПТК, обеспечения человеко-машинного интерфейса, отказы которых не влияют на выполнение основных функций комплекса; отсутствие операционной системы исключает возникновение отказов системы из-за программных сбоев;

– организована параллельная обработка всех технологических алгоритмов управления за один цикл; отказ в выполнении одного из алгоритмов не ведет к отказу всех других; нет необходимости назначения приоритетов выполнения алгоритмов – все алгоритмы обрабатываются одновременно;

– высокое быстродействие систем на базе платформы (например, время реакции системы аварийной и предупредительной защиты реактора – не более 20 мс) и доказанные детерминированные временные характеристики за счет параллельной работы управляющих алгоритмов;

– в ПТК используется высоконадежная элементная база Industry от ведущих мировых производителей и реализуется многоярусное сетевое мажоритарное резервирование; это позволяет также повысить достоверность обработки информации и практически исключить вероятность ложных срабатываний/несрабатываний оборудования;

– применение резервирования позволило реализовать принцип единичного отказа – система выполняет функции, важные для безопасности, при любом отказе одного из элементов; за счет применения высокоинтегрированных решений и оптоволоконных линий связи более чем в 10 раз снижено число контактных и клеммных соединений, являющихся причиной отказов оборудования в реальных условиях эксплуатации; реализован режим "горячей" замены сменных модулей;

– применен принцип разнообразия (диверсности) и мультидиверсных решений – совместного использования аппаратной диверсности (разнообразия программируемых компонентов для реализации алгоритмов защиты реактора и для реализации функций ввода/вывода сигналов, диагностики, информационного обмена), программной диверсности (разнообразие языков программирования и инструментальных средств) и субъектной диверсности (разнообразие разработчиков проектов ПЛИС);

– глубокое диагностирование оборудования, позволяющее быстро и однозначно определить место, время, характер неисправности и степень ее опасно-

сти; наличие встроенных автоматизированных средств калибровки измерительных каналов;

– реализация средств информационной поддержки операторов, обеспечивающих сбор, представление и хранение информации о состоянии системы, что снижает вероятность ошибки персонала;

– сертификация технических средств на стойкость к внешним воздействиям для применения в оборудовании, важном для безопасности АЭС и др.

На базе платформы «Радий» внедрены:

– ПТК системы аварийной и предупредительной защиты (ПТК АЗ-ПЗ), включая основной и диверсный комплекты – на 10 энергоблоках АЭС;

– ПТК автоматического регулирования разгрузки и ограничения мощности реактора и ускоренной предупредительной защиты (ПТК АРМ-РОМ-УПЗ) – на 7 энергоблоках АЭС;

– ПТК управляющей системы безопасности (ПТК УСБ) – на 7 энергоблоках АЭС;

– ПТК системы группового и индивидуального управления приводами органов регулирования системы управления и защиты реактора (ПТК СГИУ) – опытная эксплуатация на Запорожской АЭС;

– ПТК автоматического регулирования, контроля, управления и защиты (ПТК АРКУЗ) исследовательского реактора ВВР-М Института ядерных исследований НАН Украины.

Масштабируемость решений. Таким образом, платформа «Радий» предоставляет спектр масштабируемых решений для ИУС критических объектов. Масштабируемость реализуется в части:

– *объема, характера и особенностей выполнения функций* путем изменения количества и типов исполнительных механизмов, приемников информации и входных сигналов, а также технологических алгоритмов;

– *обеспечиваемого уровня гарантоспособности* за счет варьирования числа резервируемых каналов и ярусов и набора процедур контроля, диагностирования и реконфигурации при отказах, вызванных разными причинами (физическими дефектами, дефектами разработки и взаимодействия);

– *типов и глубины диверсности* с использованием унифицированного множества вариантов процессно-продуктной версионной избыточности и алгоритмов выбора МВТ в зависимости от типа системы и предъявляемых требований.

Выводы

Одним из путей повышения функциональной безопасности и гарантоспособности ИУС критических объектов является использование ПЛИС-технологий и реализуемых на их основе масштабируемых платформ и параметризируемых решений. Дуальная природа ПЛИС, гибкость этой технологии позволили сделать следующий шаг в развитии методов реализации принципа диверсности и других фундаментальных принципов создания надежных и безопасных ИУС.

Опыт разработки и эксплуатации ПТК ИУС на базе ПЛИС-ориентированной платформы «Радий» подтвердил целесообразность применения этой технологии для построения систем управления и защит АЭС.

Повышенный интерес исследователей, конструкторов и экспертов в области критических систем к использованию ПЛИС является свидетельством важности и перспективности этих технологий.

Литература

1. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Trans. On Dependable and Secure Computing. – 2004. – Vol. 1. – № 1. – P. 11-33.

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

3. Скляр В.В., Харченко В.С., Ушаков А.А. Анализ безопасности и выбор технологий реализации информационно-управляющих систем АЭС: риск-ориентированный подход // Екологія і ресурси: Зб. наук праць Інституту проблем національної безпеки. – К.: ІПНБ, 2006. – № 13. – С. 39-64.

4. Бахмач Е.С., Сиора А.А., Скляр В.В., Токарев В.И., Харченко В.С. Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС // Радіоелектронні і комп'ютерні системи. – 2007. – № 7 (26). – С. 75-82.

5. Бахмач Е.С., Герасименко А.Д., Головир В.А. и др. Отказобезопасные информационно-управляющие системы на программируемой логике / Под ред Харченко В.С., Скляра В.В. – Нац. аэрокосм. ун-т «ХАИ», НПП «Радий». – 2008. – 380 с.

6. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С. 7-19.

7. ИСО/МЭК 15408-1:1999 «Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель».

8. Липаев В.В. Функциональная безопасность программного обеспечения. – М.: СИНТЕГ, 2005. – 224 с.

9. Sklyar V.V. A Risk-Oriented Approach to Assessment and Assurance of Safety of Critical Instrumentation and Control Systems // Radio-electronic and Computer Systems. – 2006. – № 5 (17). – P. 85-90.

10. Харченко В.С., Скляр В.В., Конорев Б.М. и др. Оценка и обеспечение качества программных средств космических систем / Под ред. В.С. Харченко, Б.М. Конорева – Нац. косм. агентство Украины, Госцентркачества, Нац. аэрокосм. ун-т «ХАИ», 2007. – 243 с.

11. Kharchenko V., Prokhorova J., Ostroumov S., Kulanov V. Fault-Tolerant SOPC-based Approaches with Multi-Version IIP // Radioelectronic and computer systems. – 2007. – № 8 (27). – P. 71-77.

12. Харченко В.С., Жихарев В.Я., Илюшко В.М. и др. Многоверсионные системы, технологии, проекты. / Под ред. В.С. Харченко. – Х.: Нац. аэрокосм. ун-т «ХАИ», 2003. – 486 с.

13. Скляр В.В., Харченко В.С., Ястребенецкий М.А. Особенности оценки и обеспечения безопасности информационных и управляющих систем АЭС, разработанных с использованием программируемых логических интегральных схем // Ядерные измерительно-информационные технологии. – 2007. – № 3 (23). – С. 4-23.

14. Палагин А.В., Опанасенко В.Н. Реконфигурируемые вычислительные системы. – К.: Просвіта, 2006. – 295 с.

15. Харченко В.С., Тарасенко В.В., Ушаков А.А. Встроенные отказоустойчивые цифровые системы с программируемой логикой. - Х: Мин. образования и науки Украины, 2004. – 188 с.

16. Харченко В.С., Скляр В.В., Сиора А.А., Белый Ю.А. Модели безотказности и готовности встроенных мультидиверсных систем // Авиационно-космическая техника и технология. – 2008. – № 1 (48). – С. 64-69.

Поступила в редакцию 15.02.2008

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