УДК 004.415: 004.412

В.В. СКЛЯР[1], В.А. ГОЛОВИР[2], А.Д. ГЕРАСИМЕНКО[2], С.А. МАЛОХАТЬКО[2],

[1]Государственный НТЦ по ядерной и радиационной безопасности, Украина
[2]Научно-производственное предприятие «Радий», Украина

МЕТОД РАЗРАБОТКИ МНОГОВЕРСИОННЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА БАЗЕ АВТОМАТОВ С ПРОГРАММИРУЕМОЙ ЛОГИКОЙ

Проведен анализ показателей надежности многоверсионных информационно-управляющих систем (ИУС) на базе автоматов с программируемой логикой. Получены теоретико-множественные модели много-версионных ИУС при использовании различных способов внесения версионной избыточности. Приведены метрики диверсности для ИУС на базе автоматов с программируемой логикой, а также результаты применения разработанного метода.

многоверсионная система, автомат с программируемой логикой, метрики диверсности

Постановка задачи и обзор публикаций

Под многоверсионностью подразумевается применение в разных системах (либо в пределах одной системы в разных каналах) различных средств и/или аналогичных средств, основанных на различных принципах действия и направленных на осуществление заданной функции Основная цель реализации многоверсионности – защита от отказов по общей причине [13].

Метод разработки многоверсионных информационно-управляющих систем (ИУС) включает процедуры:

– выбора многоверсионных технологий (МВТ) разработки ИУС;

– определения исходных данных для выбора МВТ разработки ИУС.

Выбор МВТ разработки ИУС может быть осуществлен в результате решения задачи оптимального выбора по критерию «разнообразие / стоимость» [4, 5]. Для оценки степени разнообразия между версиями ИУС применяются метрики диверсности [3].

В современных ИУС широко применяются автоматы с программируемой логикой (АПЛ), которые выступают в качестве ядра функциональных подсистем, выполняющих как управляющие, так и вспомогательные функции. На основании проведенного анализа сделан вывод о том, что АПЛ постепенно занимают нишу, которую традиционно занимали микропроцессоры с программным обеспечением. Следующий этап развития АПЛ может быть связан с реализацией сетевых функций и функций верхних уровней иерархии ИУС (отображение, сигнализация, регистрация, архивирование информации и т.п.). Таким образом, возрастает роль АПЛ в обеспечении надежности и безопасности ИУС критического применения.

Доступное на рынке разнообразие элементной базы и инструментальных средств разработки АПЛ может быть использовано в качестве основы для разработки многоверсионных ИУС. В свою очередь при разработке многоверсионных ИУС, а также высоконадежных одноверсионных ИУС критического применения должно быть выполнены требования к организации жизненного цикла ИУС на базе АПЛ, включая процессы разработки и верификации. В то же время, известные публикации не содержат анализ подходов к реализации многоверсионных ИУС на базе АПЛ, и к оценке эффекта от применения различных типов версионной избыточности [1 – 4].

Целью статьи является анализ результатов применения метода разработки многоверсионных ИУС для систем на базе АПЛ.

1. Анализ показателей надежности многоверсионных ИУС на базе автоматов с программируемой логикой

Отказы ИУС на базе АПЛ обусловлены двумя причинами: физическими дефектами и дефектами проектирования. Из-за физических дефектов происходят отказы аппаратных средств, являющиеся результатом проявления механизмов деградации. Такие отказы могут быть парированы при использовании резервирования. Дефекты проектирования могут быть устранены только изменением проекта или производственного процесса, процедур функционирования, документации и т.п. Для компенсации дефектов проектирования целесообразно применять МВТ, когда одна и та же функция ИУС выполняется разными способами. Однако, даже в случае применения версионной избыточности дефекты проектирования могут проявляться для обеих версий ИУС. Данный феномен проиллюстрирован рис. 1.

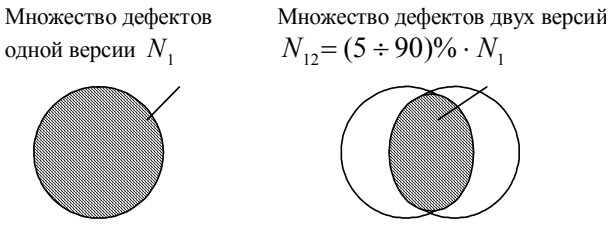

Рис. 1. Влияние применения многоверсионности на количество дефектов проектирования ИУС

По разным оценкам, количество дефектов двухверсионной системы может составлять от 5% до 90% от количества дефектов одноверсионной системы [1]. Если принять обоснованное в [2] допущение о пропорциональности количества отказов ИУС количеству вызвавших их дефектов проектирования, то тогда интенсивность отказов ИУС из-за дефектов проектирования будет пропорциональна количеству дефектов проектирования: $\lambda_1 = K \cdot N_1$; $\lambda_{12} = K \cdot N_{12}$. Кроме того, существует зависимость между интенсивностями отказов двухверсионной и одноверсионной ИУС: $\lambda_{12} = K_D \cdot \lambda_1$, где K_D – коэффициент снижения количества отказов двухверсионной ИУС по сравнению с одноверсионной.

Построим структурные схемы надежности (ССН) ИУС с учетом отказов из-за физических дефектов и дефектов проектирования. Для нерезервированной системы (рис. 2, а) вероятность безотказной работы (ВБР) составляет $P = P_{деф\text{-}в\ проект.} \cdot P_{физ.\ деф\text{-}в}$, где $P_{\text{деф-в проект.}}$ – ВБР с учетом отказов, вызванных дефектами проектирования; $P_{\text{физ. деф-в}}$ – ВБР с учетом отказов, вызванных физическими дефектами.

Для дублированной системы (рис. 2, б) вероятность безотказной работы (ВБР) составляет:

$$P = P_{деф\text{-}в\ проект.} \cdot \left[1-(1-P_{1\ физ.\ деф\text{-}в} \cdot P_{2\ физ.\ деф\text{-}в}) \right].$$

Для дублированной двухверсионной системы (рис. 2, в) вероятность безотказной работы (ВБР) составляет:

$$P = P_{12\ деф\text{-}в\ проект.} \cdot \left[1-(1-P_{1\ физ.\ деф\text{-}в} \times \right.$$

$$\left. \times P_{1\ деф\text{-}в\ проект.} \cdot P_{2\ физ.\ деф\text{-}в} \cdot P_{2\ деф\text{-}в\ проект.}) \right].$$

Вероятности безотказной работы могут быть определены по экспоненциальному закону. Интенсивности отказов из-за физических дефектов могут быть определены по справочным данным. Интенсивности отказов одноверсионной ИУС из-за дефектов проектирования могут быть определены по статистическим данным. Однако, для многоверсионной ИУС таких данных в достаточном количестве не имеется. Таким образом, для расчета надежности ИУС на базе АПЛ необходимо определить коэффициент снижения количества отказов двухверсионной ИУС по сравнению с одноверсионной.

Кроме того, при разработке многоверсионной ИУС следует решить оптимизационную задачу выбора способа реализации версионной избыточности ИУС, который обеспечивает:

$$\begin{cases} D \geq D_{\text{ЗАДАННОЕ}} \\ C \rightarrow \min, \end{cases}$$

где D – значение метрики диверсности;

C – стоимость ИУС.

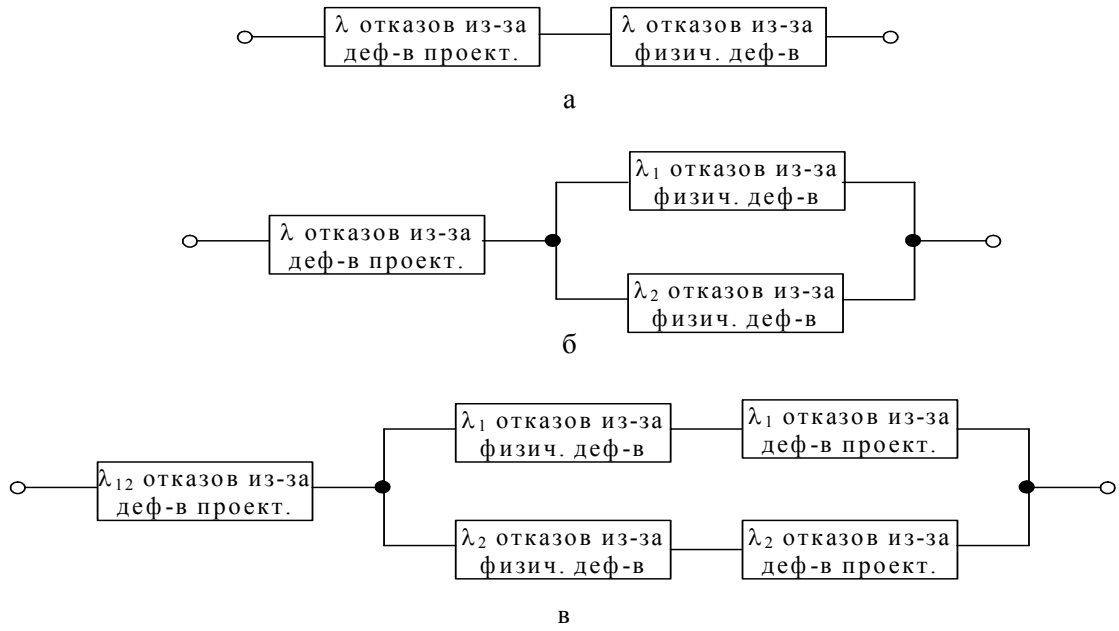

Рис. 2. Структурные схемы надежности ИУС с учетом отказов из-за физических дефектов и дефектов проектирования: а – одноканальная одноверсионная система; б – двухканальная одноверсионная система; в – двухканальная двухверсионная система

2. Теоретико-множественные модели многоверсионных ИУС

Для множеств отказов ИУС справедливо соотношение: $MN_{ИУС} = MN_1 \cup MN_2 \cup MN_{12}$. Соответственно количество отказов ИУС описывается как $N = N_1 + N_2 + N_{12}$.

Примем допущение, что количество отказов в версиях ИУС является равным, т.е. $N_1 = N_2$, что является достаточно реалистичным при современных технологиях разработки [3,4]. Тогда $N^{1B} = N_1 + N_{12} = N_2 + N_{12}$, и такое количество отказов соответствует количеству отказов одной из версий ИУС (одноверсионной ИУС).

Введем коэффициент снижения отказов двухверсионной ИУС по сравнению с одноверсионной:

$$K_D = N_{12} / N^{1B}. \quad (1)$$

Рассмотрим, каким образом влияют различные способы внесения версионной избыточности на количество совпадающих отказов ИУС из-за дефектов проектирования. Проведенный анализ позволил сформулировать следующие принципы внесение многоверсионной избыточности:

1) применение любого из способов внесения версионной избыточности позволяет снизить количество совпадающих отказов двухверсионной ИУС по сравнению с одноверсионной (рис. 1);

2) при наличии нескольких вариантов реализации способа внесения версионной избыточности (см. таблицу. 1) способ, позволяющий достичь наибольшего различия между версиями, позволяет максимально снизить количество совпадающих отказов (рис. 3, а);

3) при одновременной реализации нескольких способов внесения версионной избыточности количество совпадающих отказов двухверсионной ИУС одновременно снижается в соответствие суперпозицией снижения количества отказов каждого из способов (рис. 3, б);

4) при одновременной реализации версионной избыточности на нескольких этапах ЖЦ количество совпадающих отказов двухверсионной ИУС одновременно снижается в соответствие суперпозицией снижения количества отказов каждого из этапов (рис. 3, в).

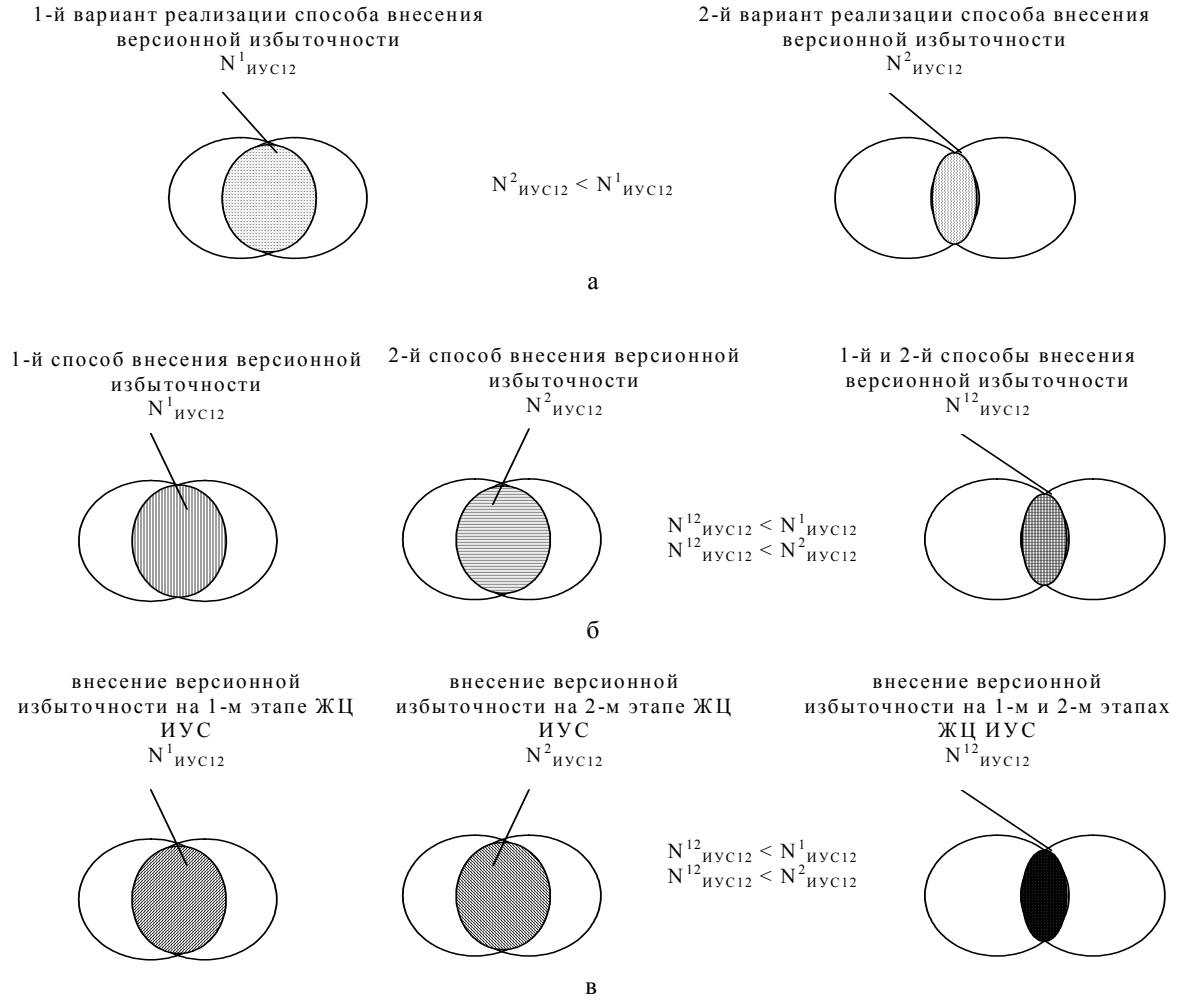

Рис. 3. Анализ влияния различных подходов к внесению версионной избыточности на количество совпадающих отказов двухверсионной ИУС: а – применение различных вариантов реализации одного способа внесения версионной избыточности; б – одновременное применение различных способов внесения версионной избыточности; в – одновременное применение версионной избыточности на различных этапах жизненного цикла ИУС

По результатам проведенного анализа влияния различных подходов к внесению версионной избыточности на количество совпадающих отказов двухверсионной ИУС введем следующее соотношение для коэффициента снижения отказов двухверсионной ИУС по сравнению с одноверсионной:

$$K_D = 1/(1+K_\Sigma), \qquad (2)$$

где K_Σ – интегральная метрика диверсности, учитывающая все способы внесения версионной избыточности на всех этапах ЖЦ ИУС; в случае, когда версионная избыточность не применяется, $K_\Sigma = 0$, $K_D = 1$ и, в соответствие с (2.1) $N_{12} = N^{1B}$.

Из формул (1) и (2) следует, что

$$N_{12} = N^{1B}/(1+K_\Sigma). \qquad (3)$$

Данное соотношение целесообразно применять для оценки эффективности многоверсионных решений, поскольку оно показывает, на сколько может быть снижено количество отказов двухверсионной системы по сравнению с одноверсионной.

Для определения интенсивности отказов совпадающих отказов двухверсионной ИУС необходимо задать временной интервал (интервалы), и принять гипотезу, что интенсивность отказов является постоянной. При необходимости может быть задано несколько временных интервалов. Таким образом, интенсивность совпадающих отказов двухверсионной ИУС отказов может

быть определена как $\lambda_{12} = N_{12} / \tau$, где τ – длина временного интервала, для которого определено количество отказов N_{12}. С учетом (3) имеем:

$$\lambda_{12\ \text{систематических отказов}} = \frac{N^{1B}}{(1 + K_\Sigma)\tau} . \qquad (4)$$

Таким образом, увеличение различия (диверсности) между версиями ИУС, которая измеряется при помощи метрик диверсности, приводит к снижению интенсивности отказов двухверсионной ИУС.

3. Анализ метрик диверсности многоверсионных ИУС на базе автоматов с программируемой логикой

Способы внесения версионной избыточности для ИУС на базе АПЛ и значения соответствующих метрик диверсности приведены в таблице 1.

Таблица 1

Численные значения метрики диверсности K для различных вариантов реализации способов внесения версионной избыточности

Способ внесения версионной избыточности	Вариант реализации способа внесения версионной избыточности	K
Разнообразие элементной базы (**A**)	Разнообразие разработчиков (фирм-производителей) элементной базы (**A1**)	4
	Разнообразие технологий реализации элементной базы (**A2**)	3
	Разнообразие семейств элементной базы (**A3**)	2
	Разнообразие видов элементной базы, относящихся к одному семейству (**A4**)	1
Разнообразие инструментальных средств (САПР) (**B**)	Разнообразие разработчиков инструментальных средств (**B1**)	3
	Разнообразие видов (наименований) инструментальных средств (**B2**)	2
	Разнообразие конфигурации (состава и версии) инструментальных средств (**B3**)	1
Разнообразие языков проектирования АПЛ (**C**)	Разнообразие на базе одновременного использования графического языка представления схем и языка программирования (языка описания аппаратуры) (**C1**)	2
	Разнообразие на базе использования разных языков программирования (языков описания аппаратуры) (**C2**)	1
Разнообразие языков проектирования спецификаций АПЛ (**D**)	Разнообразие на базе одновременного использования разных языков проектирования спецификаций АПЛ (**D1**)	1

Для получения метрик диверсности, учитывающих интегральные различия для всего жизненного цикла (ЖЦ) ИУС на базе АПЛ необходимо все метрики диверсности для каждого из этапов ЖЦ:

$$K_\Sigma = \sum_{i=1}^{N} \sum_{j=1}^{M_i} \alpha_{ij} K_{ij} , \qquad (2.5)$$

где N – количество этапов ЖЦ ИУС на базе АПЛ;

M_i – количество способов внесения версионной избыточности, используемых на i-м этапе ЖЦ;

α_{ii} – весовые коэффициенты соответствующих метрик.

В табл. 2 представлены результаты применения метода разработки многоверсионных ИУС для системы аварийной и предупредительной защиты реактора (АЗ-ПЗ) [4]. В системе АЗ-ПЗ для реализации основных управляющих функций применяются АПЛ в среде программируемой логической интегральной схемы (ПЛИС). Диверсность реализована путем применения различных кристаллов ПЛИС в диверсных комплектах АЗ-ПЗ. При этом в два раза возрастают затраты по стоимости на разработку АПЛ, выполняющего функции формирования сигналов аварийных и предупредительных защит.

Таблица 2

Результаты применения метода разработки многоверсионных ИУС для системы АЗ-ПЗ на базе АПЛ

Этап ЖЦ ИУС на базе АПЛ	Описание	K_{i1}	K_{i2}	K_i
1. Разработка схем алгоритмов формирования сигналов	Разнообразие конфигурации инструментальных средств (В3) 1-й комплект АЗ-ПЗ: базовая конфигурация САПР Quartus 2-й комплект АЗ-ПЗ: конфигурация САПР Quartus с добавлением специализированных модулей для ПЛИС семейства Cyclone	1	0	1
2. Разработка программных моделей алгоритмов формирования сигналов в среде проектирования	Разнообразие конфигурации инструментальных средств (В3, см. выше) и разнообразие на базе одновременного использования графического языка представления схем и языка программирования (С1) 1-й комплект АЗ-ПЗ: графический язык представления схем САПР Quartus 1-й комплект АЗ-ПЗ: язык описания аппаратуры VHDL	1	2	3
3. Разработка программной модели АПЛ в среде проектирования	Разнообразие конфигурации инструментальных средств (В3, см. выше) и разнообразие на базе одновременного использования графического языка представления схем и языка программирования (С1, см. выше)	1	2	3
4. Имплементация программной модели АПЛ в программируемый компонент	Разнообразие семейств элементной базы (А3) и разнообразие конфигурации инструментальных средств (В3 см. выше) 1-й комплект АЗ-ПЗ: ПЛИС Apex 2-й комплект АЗ-ПЗ: ПЛИС Cyclone	2	1	3
K_Σ		**10**		

Выводы

Полученный метод разработки многовер-сионных ИУС базируется, во-первых, на решении задачи оптимального выбора МВТ разработки ИУС, и, во-вторых, на анализе модели ЖЦ ИУС, включая определение значений метрик диверсности для каждого из способов внесения версионнной избыточности на каждом из этапов ЖЦ ИУС. Применение метода разработки многоверсионных ИУС при проектировании системы аварийной и предупредительной защиты реактора позволило обосновать выбор применяемой МВТ и оценить степень различия диверсных комплектов АЗ-ПЗ. Значение интегральной метрики диверсности составило для применяемых АПЛ составило $K_\Sigma = 10$, что позволяет (без учета весовых коэффициентов метрик) на порядок по сравнению с одноверсионной системой снизить интенсивность отказов, вызванных проявлением дефектов проектирования.

В дальнейшем целесообразно распространить полученные результаты на различные типы многоверсионных систем и уточнить методику определения весовых коэффициентов, а также коэффициентов взаимного влияния метрик.

Литература

1. Avizienis A., Lapri J.-C. Dependable Computing: From Concepts to Design Diversity // Proceedings IEEE, 1986. – Vol. 74, n. 5. – P. 8-21.

2. Харченко В.С., Жихарев В.Я., Илюшко В.М., Нечипорук Н.В. Многоверсионные системы, технологии. – Х.: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2003. – 486 с.

3. Скляр В. В. Анализ метрик диверсности программного обеспечения // Электронное моделирование. – 2004. – № 26. – С.95-104.

4. Скляр В.В., Головир В.А. Задача оптимального выбора многоверсионных технологий // Радіоелектронні і комп'ютерні системи. – 2007. – №. 7 7 (26). – С. 62-67.

5. Конюховский П.В. Математические методы исследования операций в экономике. – СПб.: Питер, 2000. – 208 с.

Поступила в редакцию 29.01.2008

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