УДК 621.039: 681.5

**А.А. СИОРА**

***Научно-производственное предприятие «Радий», Кировоград, Украина***

# АНАЛИЗ МОДЕЛЕЙ И КРИТЕРИЕВ ВЫБОРА МНОГОВЕРСИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

*Проанализированы модели многоверсионных систем (МВС): теоретико-множественные модели МВС, модели их жизненного цикла, графы многоверсионных технологий (МВТ). Приведен пример фрагмента графа МВТ для систем с версионно-информационной избыточностью. Уточняются задачи и критерии выбора МВТ. Определяются направления практического внедрения МВС и МВТ.*

***Ключевые слова:*** *модель, многоверсионная система, многоверсионная технология, граф многоверсионных технологий.*

## Введение

Для обеспечения надежности и функциональной безопасности компьютерных систем управления (КСУ) критическими объектами в атомной энергетике (системы аварийной и предупредительной защиты АЭС), аэрокосмической технике (бортовые управляющие и вычислительные системы, включая системы аварийного прекращения пуска для ракетоносителей), железнодорожной автоматике (системы централизации и блокировок) и др. используется принцип диверсности (многоверсионности), когда применяется несколько резервных каналов с различной программно-аппаратной реализацией [1]. Это позволяет целенаправленно снижать риски наиболее опасного события – отказа по общей причине (ООП), характеризуемого однопричинной и одновременной потерей работоспособности двумя и более резервными каналов.

Наиболее вероятные источники ООП для КСУ – это дефекты проектирования, внесенные при разработке, не выявленные при тестировании и верификации и проявляющиеся при определенных входных данных, а также дефекты взаимодействия физической или информационной природы, приводящие к идентичным последствиям (кратковременным или устойчивым нарушениям работоспособности каналов).

Несмотря на исследования, проводившиеся в Украине и за ее пределами (A. Avizienis, B. Littlewood, P. Popov, L. Strizini, R. Wood и др.) (см. обзор, приведенный в [2]), а также многолетнее практическое использование принципа диверсности, остается нерешенным ряд традиционных задач (количественного и качественного анализа уровня диверсности в проектах, выбора видов и объема версионной избыточности, оценки эффективности ее использования, разработки архитектур систем, устойчивых к причинам, порождающим ООП) и новых проблем, связанных с применением технологий ПЛИС, формальным доказательством достаточности объема версионной избыточности для снижения рисков ООП до приемлемого уровня, разработкой методов автоматизированного синтеза многоверсионных систем (МВС) и др.

**Цель работы** – обзор теоретических и практических аспектов анализа и синтеза МВС в контексте использования ПЛИС-технологий.

## 1. Основные понятия

Основные понятия, используемые в теории МВС, следующие [2]:

- *версия* – вариант адекватной по решаемой задаче (исходной спецификации) реализации продукта (архитектуры, аппаратных или программных средств и др.) или процесса с сопоставимыми результатами;

– *версионная избыточность* (ВИ) – вид избыточности с использованием разных версий; может иметь несколько подвидов (типов); существуют несколько классификационных схем ВИ, которые могут объединяться в сетевой схеме – *кубе многоверсионности*;

– *многоверсионность* или *диверсность* (МВ) – принцип, предусматривающий генерацию (синтез) и использование нескольких версий для выполнения одной и той же задачи (получения продукта или реализации процесса) двумя и более способами, а также формирование конечных или промежуточных данных путем обработки результатов разных версий;

– *многоверсионная система* (МВС) – система, в которой используется несколько версий; *мульти-*

*диверсная система* (МДВС) содержит две версии с несколькими вида ВИ; (n, m)-*система* – m-версионная система с n видами ВИ;

– *стратегия многоверсионности* – совокупность общих критериев и правил, определяющих принципы формирования и выбора видов ВИ;

– *многоверсионная технология* (МВТ) – совокупность взаимосвязанных правил и проектных действий, приводящих в соответствии со стратегией МВ к получению двух и более промежуточных или конечных продуктов, используемых для верификации или реализации в МВС;

– *многоверсионный проект* (МВП) – проект, в котором с использованием МВТ (ВИ процессов) создается одно- или многоверсионная система;

– *многоверсионный жизненный цикл* (МВЖЦ) – жизненный цикл МВП;

– *метрика многоверсионности (диверсности)* – показатель степени независимости версий МВС (МВП), определяемый вероятностями проявления дефектов, приводящих к отказу двух и более версий, или отношениями мощностей соответствующих множеств дефектов версий.

Обобщающим является понятие *многоверсионных вычислений* (многоверсионного компьютинга), объединяющего методы, средства и технологии обработки информации с использованием принципа МВ.

## 2. Модели

Модельная база МВС включает следующие основные модели.

1. *Теоретико-множественные модели МВС.* Как известно [3], МВС W описывается пятеркой:

$$W_n = \{X, F, U, V, Z\}, \qquad (1)$$

где X, U – входные и выходные алфавиты; $F = \{f_d, d = 1,\ldots, k\}$ – множество выполняемых функций; $V = \{v_i, i = 1,\ldots, n\}$ – множество версий с выходными алфавитами $U_1,\ldots, U_n$; Z – функция отображения $U_{id}$ в $U_d$ при выполнении функции $f_d$, т.е. $U_d = Z(U_{1d},\ldots,U_{nd})$.

Если $R=\{r_q, q=1,\ldots, m\}$ – множество видов ВИ, θ – их отображение на элементы множества $v_j(\Delta R_j)\in V$, $\Delta R_j \subset R$, то (n,m)-версионная система описывается следующим выражением, обобщающим (1):

$$W_{n,m} = \{X, F, U, V, R, \theta, Z\}. \qquad (2)$$

В итоговых версиях продуктов МВС аккумулируются различные виды версионной избыточности $r \in R$, что описывается булевой матрицей

$$\Theta = \| \theta_{dj} \|, \; d = \overline{1,m}, \; j = \overline{1,n},$$

где $\Theta_d = 1(0)$, если соответствующий вид ВИ d используется (не используется) в версии j.

Для МВС важно также задать соответствие между множествами версий V и резервных каналов системы $C=\{c_q, q=1,...,l\}$, задаваемое отображением

$$Q : V \to C,$$

описываемое булевой матрицей

$$Q = \| \omega_{jg} \|, \; d = \overline{1,m}, \; g = \overline{1,l},$$

где $\omega_{gj} = 1(0)$, если версия i реализуется (не реализуется) каналом j.

Тогда имеем модель МВС в следующем виде:

$$W_{n,m,l} = \{ X, F, U, V, R, \theta, Z, C, Q\}. \qquad (3)$$

Модели динамических МВС могут дополняться множествами алгоритмов одно- и многопараметрической адаптации при различных отказах A, которые влияют на вид функции Z. Для МВС, реализуемых на ПЛИС, конструктивными могут оказаться автоматные модели (модели многоверсионных конечных автоматов), в которых функция Z формируется с учетом вида функций переходов и выходов [2].

2. *Модели МВЖЦ.* МВЖЦ описывается моделями жизненного цикла как и для одноверсионных проектов. Для многоверсионного программного обеспечения возможны водопадная, спиралеобразная и V-модели. Последняя из них получила наибольшее распространение. Разработка моделей МВЖЦ осуществляется с использованием специальных операций над версиями:

– генерации $H = \{h_a, a = 1,\ldots, f\}$ ,

– селекции $S= \{s_b, b = 1,\ldots, p\}$,

– объединения $J = \{j_c, c = 1,\ldots,t\}$.

Каждое из множеств этих операций разделяется на подмножества микроопераций, позволяющих конструировать формальную модель жизненного цикла. Примеры таких моделей, учитывающих специфику проектирования КСУ на ПЛИС, приведены в [3].

3. *Графы МВТ.* Для решения задач описания, разработки и выбора многоверсионных технологий удобно использовать графовое представление МВТ. Множество проектных решений (видов ВИ и вариантов их выбора) может быть описано биполярным E-уровневым графом с начальной $L_и$, $L_p$ промежуточными ($L_p = \Xi_1 \times \Xi_2 \times ... \Xi_e \times ... \Xi_E$, e = 1,…, E, $\Xi_e$ – число вариантов выбора версионной избыточности на этапе e, E – число этапов жизненного цикла иди этапов, на которых возможно внесение ВИ) и конечной $L_к$ вершинами Дуги графа определяются отношениями совместимости ВИ смежных этапов. Каждой из вершин графа ставится в соответствие метрики диверсности $d_{eq}$ и стоимости $c_{eq}$ ($q = 1,\ldots, \Xi_e$).

Различные типы графов и постановок оптимизационных задач выбора МВТ и архитектур МВС по критерию «многоверсионность (надежность, безо-

пасность) – стоимость» описаны в [2,3]. Графы МВТ дополняются матрицами проектных решений, получаемых для разных технологий разработки КСУ с использованием микропроцессоров и ПЛИС.

Пример фрагмента графа МВТ для разработки систем с использованием версионно-информационной избыточности (избыточности систем счисления) приведен на рис. 1, где:

– $r_1$ определяет виды модулярной системы счисления (СС), например, на основе R – кодов ($r_{11}$), L – кодов ($r_{12}$) или RL – кодов ($r_{13}$);

– $r_2$ – виды оптимизации СС, нумеруемые с учетом индексов предыдущего яруса ($r_{211}$, $r_{212}$, $r_{213}$, $r_{214}$; $r_{221}$, $r_{222}$, $r_{223}$, $r_{224}$; $r_{231}$, $r_{232}$, $r_{233}$, $r_{234}$);

– $r_3$ – варианты реализации ($r_{311}$, $r_{312}$, $r_{313}$, $r_{314}$, $r_{315}$; $r_{321}$, $r_{322}$, $r_{323}$, $r_{324}$, $r_{325}$; $r_{331}$, $r_{332}$, $r_{333}$, $r_{334}$, $r_{335}$).

Виды версионной избыточности. соответствующие уровням графа описаны в [2].

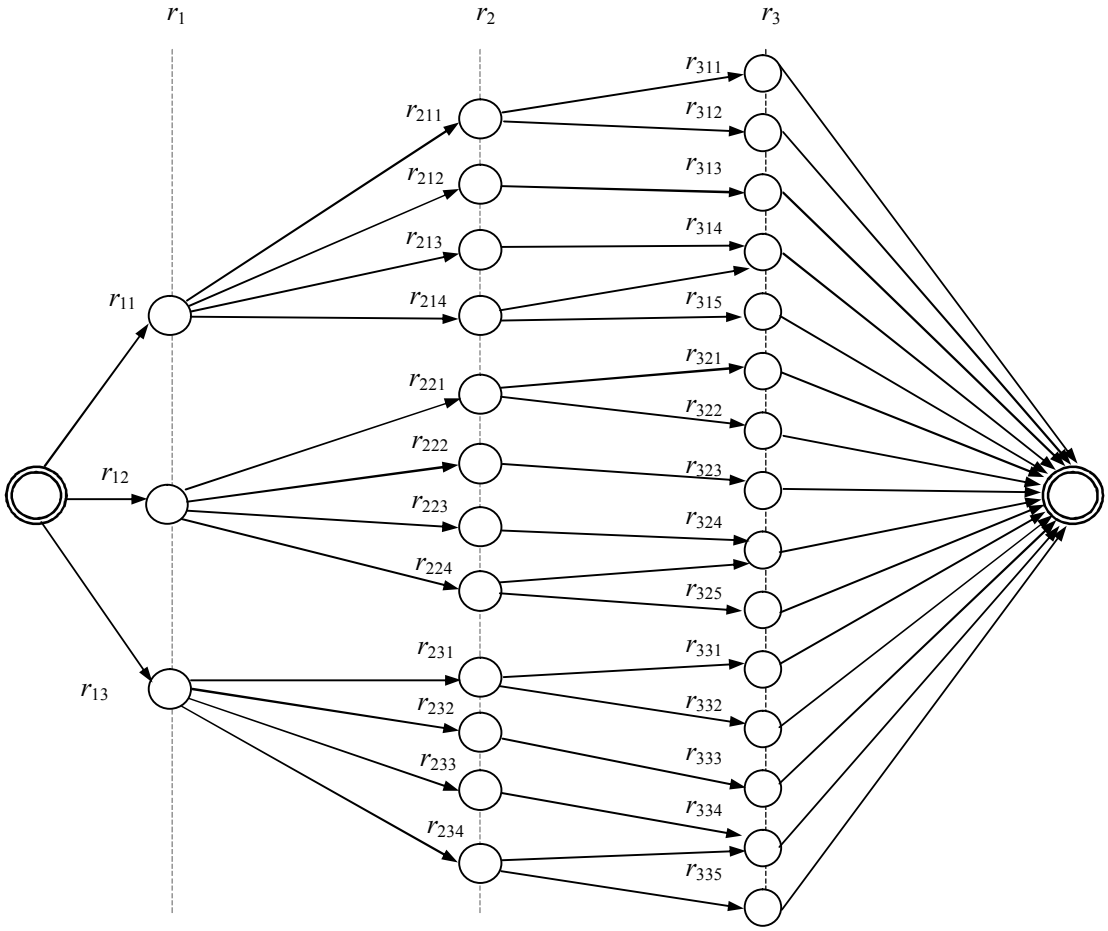


Рис. 1. Фрагмент графа МВТ

## 3. Критерии

Выбор типа МВС и МВТ осуществляется в соответствии со следующими критериями.

1. *Критерий надежности (безотказности)*. По этому критерию выбор осуществляется по показателю вероятности безотказной работы (или вероятности отказа) P или иному показателю.

2. *Критерий диверсности (безопасности)* В соответствии с данным критерием выбор осуществляется по вероятности перехода системы в опасное состояние $Q_Б$, которая зависит от интегральной метрики диверсности (ИМД), определяющей вероятность ООП. Предпочтение будет иметь пара (тройка) решений с максимальной ИМД, которая является функцией от метрик диверсности по каждому из ярусов графа МВТ $d_e$. Она может определяться как аддитивная свертка метрик $d_e$ с весовыми коэффициентами, изменяющимися в пределах от 0 до 1 (их сумма равна 1).

3. *Критерий достоверности контроля* дополняет критерии надежности и безопасности и учитывает совершенство средств проверки. Достоверность контроля D определяется произведением полноты контроля, обнаруживающей способности метода и вероятностью безотказной работы средств контроля.

При сравнении результатов, формируемых каналами (версиями), достоверность контроля определяется значением метрик диверсности.

4. *Критерий производительности.* МВС является системой с асинхронно работающими каналами, в которой такт работы должен определяться исходя из наиболее медленного канала (версии). Следовательно, по этому критерию П должны выбираться быстродействующие версии и учитываться задержка на выполнение функции Z.

5. *Критерий стоимости.* По данному критерию предпочтение имеют одноверсионные технологии разработки. Для МВТ суммарная стоимость проекта С является функцией метрик стоимости диверсных решений $c_e$, вычисляемых для каждого из Е ярусов.

Постановка задачи для компьютерных систем управления объектами критического применения, в которых определяющими являются аспекты надежности и безопасности: выбрать такую технологию (МВТ), которая обеспечит минимальную стоимость проекта $C_{min}$ при заданных показателях надежности $P \geq P_{треб}$ и безопасности (диверсности) – допустимом значении $Q_Б(\mu) \leq Q_{Бдоп}$ и требуемой производительности $П \geq П_{треб}$.

## Заключение

Ключевой проблемой остается оценка уровня безопасности уникальных (n,m)- и (n,m,l)-систем в условиях недостаточной информации для вычисления метрик диверсности. К числу наиболее важных практических задач следует отнести также разработку инструментальных средств поддержки принятия решений при создании МВС (проектировании, верификации и экспертизе).

Такие средства для МВС, разрабатываемых с использованием ПЛИС, должны интегрироваться со стандартными САПР. Ряд сложных задач, опыт решения которых описан для КСУ АЭС в [3], связан с их архитектурированием, лицензированием, модернизацией и эксплуатацией с учетом выполнения всего комплекса требований к таким системам.

## Литература

*1. Avizienis A. Dependable Computing: From Concepts to Design Diversity / A.Avizienis, J.-C. Lapri // Proceedings IEEE.– 1986. – Vol. 74, №. 5. – P. 8-21.*

*2. Сиора А.А. Отказоустойчивые системы с версионно-информационной избыточностью / А.А. Сиора, В.А. Краснобаев, В.С. Харченко; под ред. В.С. Харченко. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2009. – 321 с.*

*3. Kharchenko V.S. FPGA-based NPP Instrumentation and Control Systems: Development and Safety Assessmen / V.S. Kharchenko, V.V. Sklyar (edits). – Kharkiv, Kirovograd: RPC "Radiy", KhAI, STC on Nuclear and Radiation Safety, 2008. – 188 p.*

*Поступила в редакцию 20.01.2010*

**Рецензент:** д-р техн. наук, проф., завідувач кафедри автоматизації проектування обчислювальної техніки Г.Ф. Кривуля, Харківський національний університет радіоелектроніки, Харків.

### МОДЕЛІ ТА КРИТЕРІЇ ВИБОРУ БАГАТОВЕРСІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

***О.А. Сіора***

Проаналізовано моделі багатоверсійних систем (БВС): теоретико-множинні моделі БВС, моделі багатоверсійного життєвого циклу, графи багатоверсійних технологій (БВТ). Надано приклад графа МВТ для систем з версійно-інформаційною надмірністю. Уточнено задачі та критерії вибору БВТ. Визначено напрями практичного впровадження БВС і БВТ.

**Ключові слова:** модель, багатоверсійна система, багатоверсійна технологія, граф багатоверсійних технологій.

### MODELS AND CRITERIA FOR CHOICE OF MULTI-VERSION SYSTEMS AND TECHNOLOGIES

***A.A. Siora***

Models of multi-version systems (MVS) including theoretic-set models, models of life cycle, graphs of multi-version technologies (MVT) are analyzed. An example of the MVT graph for system with version-information redundancy is described. Tasks and criteria of BVT choice are specified. Directions of MVSs and MVTs implementation are proposed.

**Key words**: model, multi-version system, multi-version technology, graph of multi-version technologies.

**Сиора Александр Андреевич** – канд. техн. наук, председатель правления Научно-производственного предприятия «Радий» Кировоград, Украина, e-mail: marketing@radiy.kr.ua.