УДК 681.3

ПРИМЕНЕНИЕ МЕТОДОЛОГИИ МУЛЬТИВЕРСИЙ В ВИДЕ БАЗОВЫХ ГЕРТ-СЕТЕВЫХ МОДЕЛЕЙ

Гринин Е. К.,
научный руководитель канд. техн. наук Царев Р. Ю.
Сибирский федеральный университет

Мультиверсионная отказоустойчивость основана на использовании двух или более версий модуля программного обеспечения, исполняемых последовательно или параллельно [1]. Версии используются как альтернативы (с отдельными средствами обнаружения ошибок), в парах или в больших группах (чтобы маскировать ошибки через голосование). Поэтому, если одна версия производит сбой на специфическом вводе, по крайней мере, одна из альтернативных версий должна обеспечить корректный вывод. Для принятия решения о правильности вывода различных блоков могут быть использованы базовые ГЕРТ – сетевые модели.

Модель блоков восстановления [2, 3] комбинирует основные идеи метода контрольных точек и рестарта для мультиверсионных компонент программного обеспечения таким образом, что различные версии используются только после того, как обнаруживается ошибка (Рис. 1).

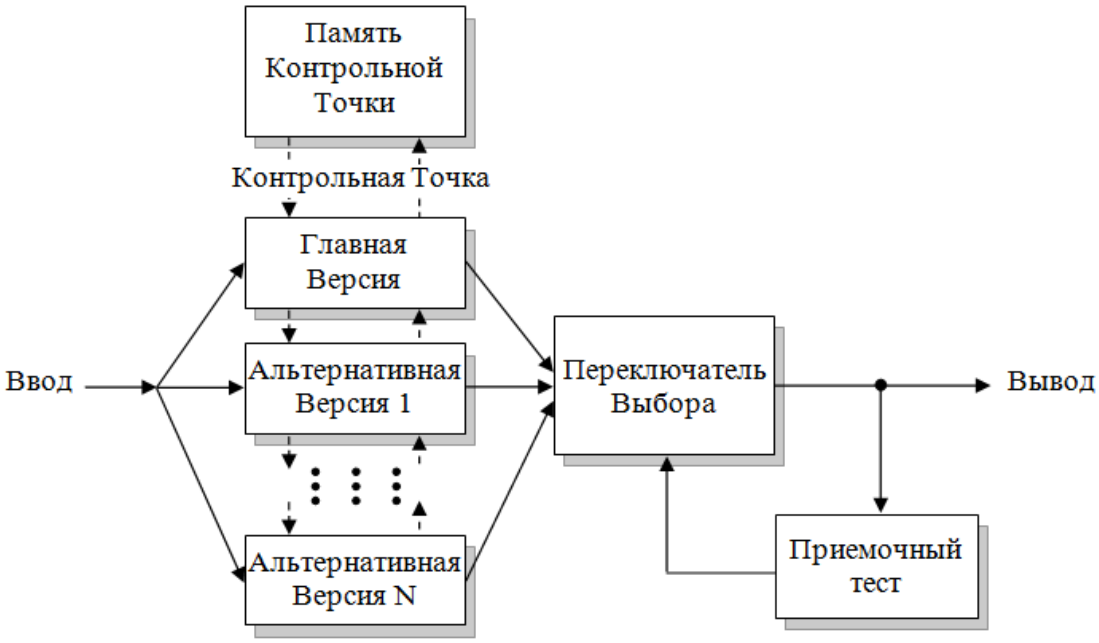

Рис. 1 - Модель блоков восстановления

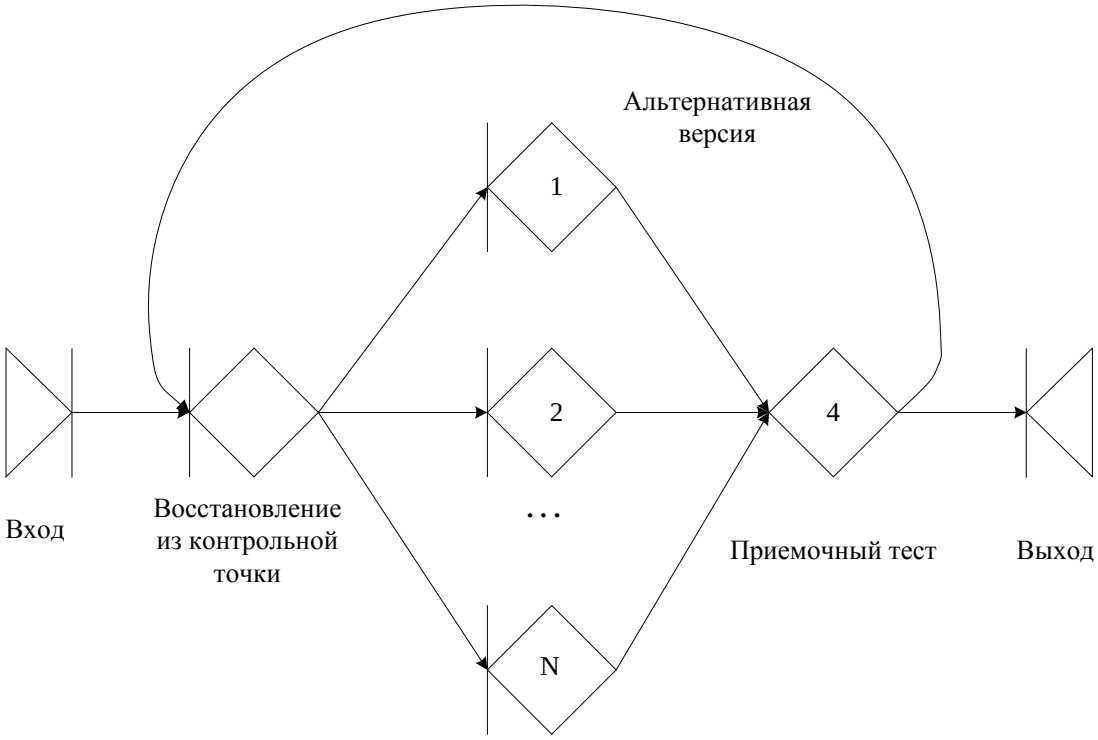

Рис. 2 - Модель блоков восстановления в виде ГЕРТ-сети

Контрольные точки определяются перед исполнением версий. Контрольные точки необходимы, чтобы восстановить состояние после того, как версия произведет сбой и не сможет обеспечить корректную начальную точку для следующего компонента. Приемочный тест не должен быть только выходным тестом и может быть осуществлен различными встроенными проверками, чтобы увеличить эффективность обнаружения ошибок. Также, из-за того, что первичная версия будет выполняться успешно в большинстве случаев, альтернативы могут быть разработаны с более низкой производительностью и качеством, в некотором смысле (например, вычисляя значения с меньшей точностью). Подобно методу разнообразия данных, вывод альтернативных версий может быть разработан таким образом, чтобы быть эквивалентным первичному (с определением эквивалентности, зависящей от приложения). Фактическое выполнение множественных версий может быть последовательным или параллельным в зависимости от вычислительных мощностей и требований производительности. Если все альтернативы выдали сбой, компонент должен инициировать исключение, чтобы сообщить остальной части системы об отказе завершения его функции. Следует отметить, что такое возникновение отказа не подразумевает постоянный отказ компонента, он может быть повторно использован после изменений его состояния или ввода. Возможность совпадения отказов является источником больших дискуссий относительно всей технологии отказоустойчивого мультиверсионного программного обеспечения.

Модель блоков восстановления с согласованием [4] (Рис. 3) – это подход, комбинирующий N-версионное программирование и метод блоков восстановления, для повышения надежности по сравнению с использованием только одного из подходов. Приемочные тесты в блоках восстановления страдают из-за недостатка руководящих принципов для их разработки и общей склонности к ошибкам проектирования из-за присущей трудности создания эффективных тестов. Использование голосования как в N-версионном программировании не может быть применено во всех ситуациях,

особенно, когда возможны правильные множественные выводы. В этом случае голосование объявило бы об отказе при выборе соответствующего вывода. Блоки восстановления с согласованием используют алгоритм выбора решения, подобный N-версионному программированию, как первый уровень решения. Если этот первый уровень объявляет отказ, используется второй уровень приемочного испытания, подобный тому, который использовали в методе блоков восстановления. Хотя очевидна гораздо более высокая сложность реализации, чем любой из индивидуальных методов, сравнение модели надежности указывает, что этот комбинированный подход имеет высокий потенциал для создания более надежного программного обеспечения. Использование слова потенциал важно здесь, потому что добавленная сложность могла бы фактически работать против проекта и приводить к менее надежной системе.

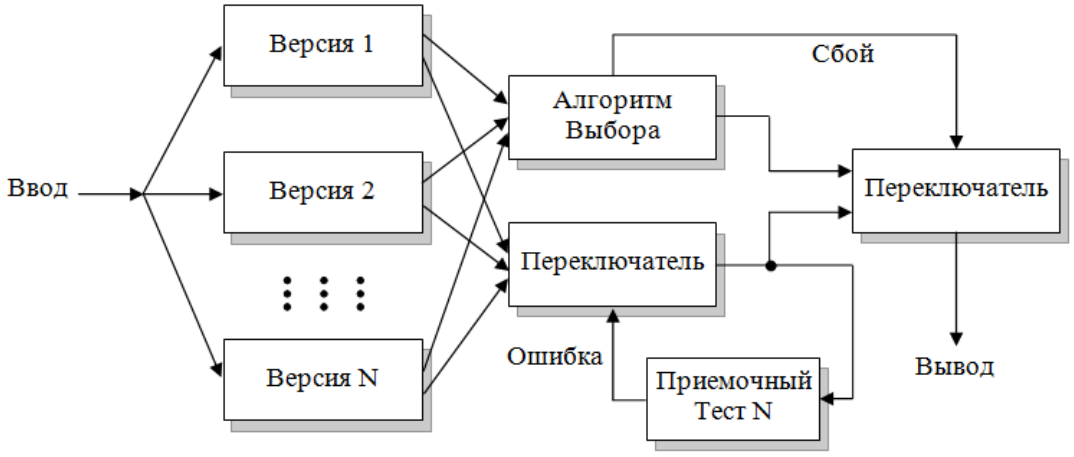

Рис. 3 - Модель блоков восстановления с согласованием

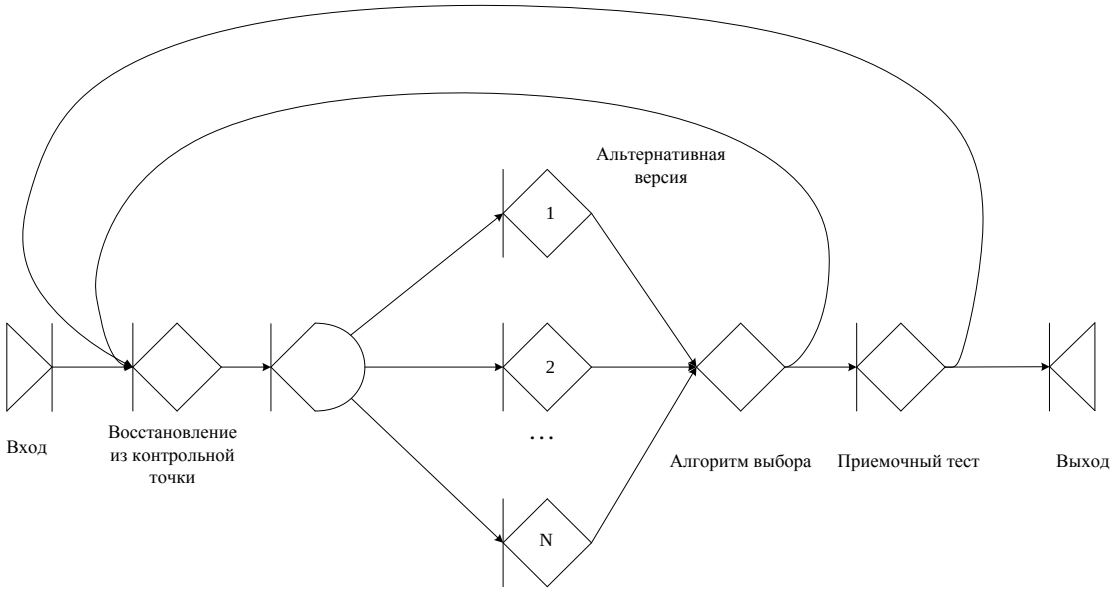

Рис. 4 - Модель блоков восстановления с согласованием в виде ГЕРТ-сети

Предложенные способы реализации методологии мультиверсий в виде базовых ГЕРТ-сетевых моделей, позволяют создавать ГЕРТ-сети описывающие соответствующий вид мультиверсионных архитектур программного обеспечения, что позволяет получить их вероятностно-временные характеристики функционирования.

Применение необходимого и достаточного условия функционирования мультиверсионного программного модуля позволяет использовать эквивалентные преобразования и получать ГЕРТ-сети, которые могут быть рассчитаны, используя имеющийся математический аппарат, что расширяет сферу применения ГЕРТ-сетей для расчета мультиверсионных архитектур программного обеспечения, которые известны сейчас и могут появиться в будущем.

Список литературы

1. Аврамчук, Е.Ф., Вавилов, А.А., Емельянов, С.В. и др. Технология системного моделирования. —М.: Машиностроение; Берлин: Техник, 1988. — ISBN 5-217-00150-X.
2. Thompson, W.J. Computing for scientists and engineers. — NY: John Wiley & Sons, Inc., 1992. — ISBN 0-471-54718-2.
3. Yu, Jung-Lok, Azougagh, Driss , Kim, Jin-Soo. PROC: Process ReOrdering-Based Coscheduling on Workstation Clusters / 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Papers, 2005. p. 50.
4. Андреев, А.Н., Воеводин, В.В. Методика измерения основных характеристик программно-аппаратной среды. / ВВС ДВО РАН.