

УДК 381.3

Система динамического контроля обработки данных методом степ-резервирования

В работе предложен новый подход к проектированию отказоустойчивых систем, основанный на представлении задачи декомпозиции системы и парирования отказов как специального случая задачи степ-резервирования.

**А. П. Мартынов, С. Н. Колтаков,
Д. Б. Николаев, М. И. Похлебаев,
А. А. Скоробогатый**

Стремительное развитие программируемых логических интегральных схем (ПЛИС) в последние десять лет привело к тому, что в настоящее время ПЛИС стали одними из основных элементов специализированных вычислительных систем. ПЛИС позволяют наиболее эффективно реализовать достаточно простые алгоритмы, требующие высокой вычислительной производительности. В настоящее время ПЛИС широко используются в аппаратуре для высоконадежных комплексов управления. К такой аппаратуре предъявляются самые жесткие требования по надежности. Одним из основных методов повышения надежности является создание систем, которые при отказах элементов сохраняют свою работоспособность или восстанавливают ее в течение заданного отрезка времени. Для создания отказоустойчивой системы всегда необходимо введение в нее избыточных (резервных) элементов, которые в случае отказа способны заменить отказавшие элементы системы. Основными причинами отказов устройств являются дефекты разработки (ДР) (development faults), физические дефекты (ФД) (physical faults) и дефекты взаимодействия (ДВ) (interaction faults).

Обычно применяется резервирование на уровне системы в целом, например, дублирование, т. е. введение запасной системы. Для больших систем может применяться резервирование на уровне крупных элементов (например, введение резервных процессоров в многопроцессорную систему [1, 2]). Резервирование на уровне мелких элементов, таких как логические элементы, счетчики и т. п., как правило, оказывается неэффективным, поскольку при одинаковой надежности стоимость такой системы оказывается намного выше, чем стоимость системы с резервированием на более крупном уровне.

Появление высокопроизводительных ПЛИС способно изменить ситуацию. Для резервирования на низком уровне не требуется введения в ПЛИС дополнительных кросскоммутаторов, поскольку ПЛИС их уже содержит. Вместо введения резервных элементов в ПЛИС требуется лишь оставить некоторое количество незадействованных ячеек, которые в случае отказа путем перепрограммирования связей заменят отказавшие ячейки. Таким образом, ПЛИС представляет собой почти идеальную аппаратную базу для создания отказоустойчивой системы на кристалле.

Преимущества ПЛИС могут быть использованы:

- 1) для расширения структуры обеспечения отказоустойчивости и обеспечения широкого охвата ошибок вычислительного процесса на базе кристалла;
- 2) обеспечения последовательности восстановления типа «остановка–фиксация–перезапуск»;
- 3) отключения не всего вычислителя, а его частей, являющихся причиной ошибок.

Перечисленные выше решения являются также удобными из-за большой гранулярности ПЛИС, благодаря чему можно достичь высокой элементарности действий. Такие элементарные действия являются алгоритмическими средствами, с помощью которых еще при проектировании разработчик системы может определить, какие взаимодействия и пересечения процессов нужно предотвратить (по возможности), чтобы сохранить целостность работы системы. Таким образом, разделяя главный вычислительный процесс и формируя его в определенной последовательности элементарных действий, проектировщик получает возможность создавать сложные вычислители с необходимой степенью обнаружения ошибок в его вычислительном процессе и управления их распространением.

С учетом гибкости проектирования при использовании ПЛИС-технологии становится возможным и удобным не только построение условно-распределенного вычислительного комплекса, но и построение модуля обнаружения неисправности и управления переключением на базе одного кристалла. Это, в свою очередь, позволит реализовать аппаратно-управляемое восстановление, которое не будет выходить за рамки кристалла (системного модуля) [3].

На сегодняшний день фундаментальным решением задачи защиты от ДР вычислительных систем является принцип многоверсионности [3]. Руководствуясь им, можно достичь высоких показателей отказоустойчивости систем за счет использования N-версионных ПЛИС-проектов, которые будут базироваться на различных вариантах реализации многопроцессорных схем, основанных на технологии «soft» и «зашиваемых» в кристалл в виде IP-ядер [4].

Такой подход позволит частично устранить чрезмерную аппаратную избыточность за счет «усовершенствования» алгоритма вычислений по сравнению с простым «копированием» вычислительных каналов. Также за счет независимо разработанных, отличных друг от друга симплексных блоков решения и выполнения перекрестного контроля и/или приемо-сдаточного теста станет возможным получение частичной отказоустойчивости благодаря отладке или маскировке неправильных исходных результатов, которые могут быть произведены одним из блоков. Выполнение такого подхода на одном кристалле позволяет достичь высокой скорости передачи данных и избавиться от дополнительных роутеров и синхронизаторов сигнала.

В работе предложен новый подход к проектированию отказоустойчивых систем, основанный на представлении задачи декомпозиции системы и парирования отказов как специального случая задачи степ-резервирования. Подобный подход к задаче отказоустойчивости стал возможным благодаря применению конвейеризации, которая в данном случае позволяет решить проблему изменения задержек распространения сигналов при реконфигурации системы. Применение конвейеризации также может считаться новым подходом к проектированию отказоустойчивых систем на ПЛИС. Предложенные алгоритмы позволяют создать отказоустойчивую систему с минимальной избыточностью. При этом не требуется резервирование на уровне блоков. Согласно первому алгоритму разбиения областей для резервирования требуется резервная область, равная по размерам наименьшему блоку. Линейные размеры резервной области не могут быть меньше

минимальных размеров блоков. Алгоритм разбиения (декомпозиции) сопровождается алгоритмами реконфигурации, позволяющими находить размещение блоков для произвольного расположения отказов. Алгоритмы реконфигурации обладают низкой вычислительной трудоемкостью (которая линейно зависит от числа блоков), что может быть рассмотрено как переход от общего случая полной задачи упаковки к частному случаю, для которого вычислительная трудоемкость линейна (степ-резервирование).

Предложенная методика проектирования отказоустойчивых систем на ПЛИС, в отличие от ранее предлагаемых, сочетает в себе следующее:

- 1) сохранение длин связей при реконфигурации;
- 2) минимальную избыточность системы;
- 3) минимальное число блоков для данного коэффициента заполнения ПЛИС;
- 4) возможность создания системы, устойчивой к множественным отказам;
- 5) возможность создания отказоустойчивой системы с использованием ядер, имеющих фиксированную топологию и содержимое которых недоступно для каких-либо изменений;
- 6) рассмотрение отказов в функциональных блоках, отличных от обычных ячеек.

Важнейшим качеством предлагаемой методики является то, что она применяется на высоком (логическом) уровне (а не на физическом) и не требует какой-либо аппаратной модернизации существующих ПЛИС. Основные технологические принципы проектирования предлагаемой методики соответствуют принципам проектирования обычных систем на ПЛИС (декомпозиция системы на блоки, конвейеризация, раздельное размещение блоков в области прямоугольной формы) и поддерживаются современными системами автоматизированного проектирования (САПР).

Результаты работы могут быть использованы при проектировании систем ответственного применения, необслуживаемых систем и систем, подвергающихся воздействию ионизирующего излучения. Данная методика может быть применена при использовании кристаллов с заводскими дефектами для создания обычных, неотказоустойчивых систем.

Рассмотренный алгоритм может быть распространен на системы, способные парировать множественные отказы. Здесь подразумевается, что в случае возникновения в какой-либо подсистеме большего числа отказов, чем она способна парировать, найдется подсистема, способная парировать данное число отказов, и в результате реконфигурации эти две подсистемы поменяются местами. Предлагается алгоритм декомпозиции, ограничивающий размеры формируемых блоков таким образом, что подобная замена всегда возможна. Дается вычислительно эффективный алгоритм реконфигурации.

Предложенная методика позволит создавать отказоустойчивые системы на ПЛИС с использованием IP-ядер с фиксированной топологией, недоступных для какой-либо модификации.

В работе получены следующие результаты.

1. Сформулированы основные принципы проектирования отказоустойчивых систем на ПЛИС с использованием степ-резервирования.
2. Предложена методика создания и реконфигурации отказоустойчивых систем на ПЛИС, позволяющая сохранять неизменными длины связей в критических схемах.
3. Предложены алгоритмы формирования размеров блоков, позволяющие формировать блоки максимального размера для одно- и многоотказоустойчивых систем.
4. Даны оценки избыточности систем на ПЛИС, соответствующих предлагаемым алгоритмам.

Список литературы

1. Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Построение алгоритма для верификационных исследований и определения достоверности результатов контроля аппаратуры управления // Труды 29-й Межрегиональной научно-технической конференции «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем». – Серпухов: Изд-во СВирВ. 2010.
2. Немченко И. А., Мартынов А. П., Фомченко В. Н. Комплекс программно-аппаратных средств контроля для повышения надежности систем сопряжения // Сборник докладов 53-й научной конференции МФТИ – Всероссийской молодежной научной конференции с международным участием «Современные проблемы фундаментальных и прикладных наук». – М.: МФТИ. 2010.
3. Николаев Д. Б., Коршунов А. В., Шорохов А. Д., Медведев В. Б., Фомченко В. Н. Разработка моделей информационных систем с учетом аппарата коррекции // Сборник докладов Международной научно-практической конференции «Информационные ресурсы и системы в экономике, науке и образовании». – Пенза: Изд-во Сфера. 2011.
4. Кузьмин И. В., Кедрус В. А. Основы теории информации и кодирования – Киев: Вища шк., 1986.

The dynamic control of data processing by the method of step-reservation

A. P. Martynov, S. N. Koltakov, D. B. Nikolaev, M. I. Pohlebaev, A. A. Skorobogaty

The paper proposes a new approach to the design of fault-tolerant systems based on the idea of partitioning system and parrying failures as a special case of the problem step-reservation.