К ВОПРОСУ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ ПРОГРАММНЫХ СИСТЕМ

Стельмах В.О., Ковалев Д.И., Лайков А.Н., Реутов А.А.
Сибирский федеральный университет
Красноярск, Россия

Разработка отказоустойчивого программного обеспечения (ПО) – отдельный аспект разработки надежных информационно-управляющих систем (ИУС), так как системная надежность зависит от надежности как аппаратных, так и программных компонент [1]. Как правило, надежностное проектирование ИУС фокусируется на критичных частях аппаратного обеспечения системы. Однако во многих областях науки и производственной деятельности сбой в работе программного обеспечения может привести к значительным экономическим потерям. Поэтому одной из основных задач разработчиков программного обеспечения становится создание таких алгоритмов или методов разработки ПО, которые обеспечивали бы устойчивость системы к программным и аппаратным сбоям.

На практике существует два дополняющих друг дуга подхода, которые используются при разработке надежного программного обеспечения ИУС [2].

Предотвращение сбоев. В процессе проектирования и реализации программных систем используются такие технологии разработки ПО, которые сводят к минимуму ошибки оператора и помогают находить системные ошибки до того, как система будет запущена в эксплуатацию.

Устойчивость к сбоям. Система проектируется таким образом, что бы можно было обнаружить и исправить сбои, устраняя непредвиденное поведение системы до того, как это приведет к ее отказу.

Предотвращение сбоев, фактически, означает поставку заказчику программных систем, свободных от ошибок и сбоев. Это можно сделать двумя способами: с помощью статических и динамических методов тестирования, которые обнаруживают эти ошибки и позволяют исправить их до начала эксплуатации системы. Однако с уменьшением ошибок в системе стоимость их обнаружения возрастает экспоненциально. Это значит, что при усложнении системы обеспечить достаточный уровень ее надежности только за счет тестирования становится практически невозможным.

Устойчивость к сбоям подразумевает наличие в системе возможности исправления ошибок отдельных модулей в процессе их выполнения. В настоящее время выделяют два основных подхода к созданию отказоустойчивых программных систем. Они основаны на разработке множества версий для критичных модулей системы и различаются способами использования этих версий.

Первый подход известен как *мультиверсионное программирование* [3]. Здесь версии выполняются параллельно, как правило, на отдельных компьютерах. Результат их работы определяется с помощью какого-либо алгоритма голосования [4]. Надежность системы при этом напрямую зависит от глубины мультиверсионности. Однако улучшение характеристик надежности ПО с использованием избыточности требует дополнительных ресурсов. Поэтому основной вопрос, встающий перед разработчиком заключается в том, каким образом, используя избыточность в структуре ПО, максимизировать его надежность, при этом не превышая ограничений по остальным факторам.

Второй подход основан на использовании *блоков восстановления* [2]. В этом случае каждый критичный программный компонент содержит множество версий вычислительного модуля; тест, проверяющий его работу; и подпрограмму, которая по результатам выполнения теста либо принимает результаты вычисления, либо запускает их повторно, но уже с помощью другой версии вычислительного модуля.

Версии модулей для вышеперечисленных подходов реализуются отдельными командами разработчиков согласно заранее определенной спецификации, описывающей входную и выходную информацию, а так же детальные требования (язык программирования, алгоритм, требования к ресурсам, и т.д.) к каждой версии модуля.

Литература

1. *Ковалев И.В., Новой А.В., Штенцель А.В.* Оценка надежности мультиверсионной программной архитектуры систем управления и обработки информации // Вестник Сибирского государственного аэрокосмического университета.- 2008.- № 3.- С.50-52.

2. *Ковалев И.В., Завьялова О.И., Лайков А.Н.* Формирование избыточного программного обеспечения отказоустойчивых систем управления // Известия высших учебных заведений. Приборостроение.- 2008.- Т. 51.- № 10.- С. 30-34.

3.*Ковалев И.В., Слободин М.Ю., Царев Р.Ю.* Мультиверсионное проектирование отказоустойчивого программного обеспечения систем управления // Проблемы машиностроения и автоматизации.- 2006.- № 5.- С. 61-69.

4. К*овалев И.В., Котенок А.В. К* проблеме выбора алгоритма принятия решения в мультиверсионных системах // Информационные технологии.- 2006.- № 9.- С. 39-44.