Анализ поведения реактивных систем методом интерливинговой развертки параллельного взаимодействия

Тумуров Эрдэм Гармаевич
Институт систем информатики имени А.П. Ершова СО РАН (Новосибирск), Россия
e-mail: erdemus@gmail.com

Аннотация

Реактивная система представляет собой комплекс параллельных процессов, взаимодействующих между собой и внешним окружением с помощью сообщений и через разделяемые переменные. Результат работы системы - последовательность реакций на события.

Тестирование реактивных систем является трудоемким - число возможных комбинаций состояний процессов, событий и входных данных, как правило, очень велико. Для повышения надежности часто строят математические модели, на которых либо доказывают, что нужные свойства удовлетворяются (дедуктивная верификация), либо используют методы автоматизированного перебора большого количества вариантов исполнения (проверка на модели).

Данная работа представляет метод интерливинговой развертки для построения упрощенной модели реактивной системы в виде недетерминированного последовательного автомата. Исполнение одного процесса формализуется некоторым автоматом, состоящим из вершин-состояний и переходов-действий. Интерливинг - это такая модель параллельной работы нескольких процессов, где общее исполнение представляет собой последовательность действий, полученную интерливингом (перемежением) действий процессов.

В работе используется язык предикатного программирования P [1]. С помощью логики программы [2] строится формальная модель в виде параллельных взаимодействующих автоматов, соответствующих каждому процессу. Далее строится машина метасостояний, где каждому метасостоянию соответствует инвариант, описывающий комбинации состояний всех процессов. Машина метасостояний строится таким образом, чтобы количество метасостояний было невелико, но достаточно для поиска ошибок. Полученная машина анализируется на соответствие темпоральным свойствам безопасности, живости. Метод демонстрируется на сетевом протоколе передачи данных ABP.

Разрабатываемый метод ориентирован на разработку, тестирование, моделирование и верификацию программной и аппаратной части встроенных систем аэрокосмической отрасли, энергетики, медицины и др. приложений, где необходима предельная надежность систем.

Работа выполнена при поддержке РФФИ, проект 12-01-00686.

Список литературы

[1] Карнаухов Н.С., Першин Д.Ю., Шелехов В.И. Язык предикатного программирования P. Новосибирск, 2010. Стр. 42. (Препр. / ИСИ СО РАН; N 153).

[2] Шелехов В.И., Тумуров Э.Г. Логика невзаимодействующих программ и реактивных систем. // Вестник Бурятского Государ-

ственного Университета. Секция: математика, информатика, Вып.9 / 2012. Улан-Удэ, Стр. 81-90.