УДК 004.052.42

Визуализация причин несоответствия спецификации формальной модели киберфизической системы

Терещук М.А., Университет ИТМО, Санкт-Петербург
Научный руководитель – Вяткин В.В., д.т.н., профессор факультета информационных технологий и программирования, Университет ИТМО, Санкт-Петербург

Введение

Проверка моделей — эффективный метод формальной верификации. При несоответствии системы формальным требованиям, его выходными данными является последовательность состояний формальной модели, показывающая наличие ошибки (контрпример). Локализация проблемы в системе — задача, предполагающая анализ такого контрпримера вручную, что в силу его длины и сложности требует временных затрат и досконального знания верифицируемой системы. Целью работы является разработка метода автоматического объяснения контрпримера и программного средства для визуализации причин несоответствия спецификации формальной модели киберфизической системы для формальных моделей стандарта IEC 61499.

Основная часть

Формальная модель стандарта IEC 61499 представляет собой систему функциональных блоков; блоки бывают трех типов: базовые, композитные и сервисные. Базовый блок имеет входы и выходы для потоков данных и событий, и является, по сути, конечным автоматом. Композитный блок представляет собой комбинацию базовых, а сервисный — необходим для работы с оборудованием.

Для нахождения путей в модели, приводящих к невыполнению проверяемого свойства, предлагается использовать обратный обход системы. Началом обхода служит выбранная переменная на определенном шаге контрпримера. Путем рекурсивного спуска внутрь композитных блоков, осуществляется поиск базового блока, на выходе которого заданная переменная приняла значение из контрпримера. Далее, в автомате найденного базового блока осуществляется поиск события, повлиявшего на переменную. Затем, осуществляется обход системы с целью объяснения найденного на предыдущем шаге события, что является рекурсивным вызовом настоящего алгоритма. Обход продолжается до достижения переменных, принадлежащих входному интерфейсу системы. Результатом работы алгоритма является набор путей на блок-диаграмме и внутри автоматов.

Выводы

Предлагаемый метод позволяет локализовать проблему в формальной модели стандарта IEC 61499. Метод имеет временную сложность O(NM), где N – число состояний в системе, а M – количество шагов в контрпримере. Разработанное программное средство позволяет сократить временные затраты, необходимые для отладки системы и устранения причин, влекущих ее нестабильность.

Автор _____ Терещук М.А.
Научный руководитель _____ Вяткин В.В.