УДК – 004.4'233

OERITTE: ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ОБЪЯСНЕНИЯ КОНТРПРИМЕРОВ ДЛЯ МЕТОДА ФОРМАЛЬНОЙ ВЕРИФИКАЦИИ ПОСРЕДСТВОМ ПРОВЕРКИ МОДЕЛЕЙ

Овсянникова П.А. (Университет ИТМО)
Научный руководитель – к.т.н. Чивилихин Д.С. (Университет ИТМО)

В данной работе представлено программное средство Oeritte, предназначенное для уменьшения временных затрат на верификацию модульных систем с помощью метода проверки моделей. Главная особенность Oeritte – возможность автоматического визуального объяснения контрпримеров и результатов темпоральных свойств.

Введение. Убедиться в правильности поведения формальной модели промышленной кибер физической системы можно с помощью метода проверки моделей, который он предполагает проверку всего пространства состояний системы на соответствие спецификации. Для этого на вход программного средства, называемого верификатором, подается формальная модель верифицируемой системы и набор высказываний темпоральной логики образующих ее спецификацию. Выходными данными верификатора являются последовательности состояний, приводящие к нарушению определенных свойств (контрпримеры) в случае, если требования не удовлетворены.

Последующая отладка системы включает в себя анализ контрпримера, который может включать в себя десятки состояний. Кроме того, каждое состояние – это набор значений всех переменных системы на определенном временном шаге, что делает невозможным его расшифровку для сложных систем без вспомогательных средств.

Основная часть. В данной работе было разработано программное средство – для визуального объяснения контрпримера - Oeritte. Будем называть *присвоением* значение определенной переменной на определенном шаге контрпримера. Под объяснением контрпримера подразумевается нахождение путей в модульной системе, приводящих к тому, что определенная переменная на определенном шаге контрпримера имеет определенное значение, или к определенному присвоению. Переменная и шаг задаются пользователем, объяснение выполняется автоматически. Так же программное средство включает в себя реализацию разработанного ранее метода объяснения значения темпоральной формулы. Таким образом, пользователь может сначала получить присвоения, являющиеся причинами невыполнения формулы, а затем их объяснения в виде подсвеченных переходов на диаграмме.

Объяснение присвоения выполняется следующим образом. Вначале вся система, заданная в формате NuSMV транслируется во внутреннее представление Oeritte: сеть из комплексных блоков, в свою очередь являющимися сетью базовых блоков, которые представляют собой атомарные операции или простые функции. У каждого блока есть набор входных и выходных переменных. Каждая переменная системы является входом или выходом блока. Таким образом объяснение присвоения выполняется рекурсивно: (1) по входящим переходам находится выходная переменная базового блока, соединенная с переменной рассматриваемого присвоения, (2) происходит объяснение выходного присвоения этого блока, результатом которого является набор присвоений-причин. Далее происходит объяснение новых присвоений. Процедура повторяется до тех пор, пока все полученные на предыдущем шаге присвоения не будут иметь входящих переходов. На каждом шаге рекурсии запоминаются новые присвоения, которые вместе со связями между ними отображаются на модульной диаграмме системы.

Выводы. Разработанное программное средство снижает затрачиваемое количество времени и усилий необходимых для локализации проблемы в системе и было успешно применено в процессе верификации логики подсистемы атомного реактора.

Овсянникова П.А. (автор)

Чивилихин Д.С. (научный руководитель)