МАТЕМАТИЧНЕ ТА КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

MATHEMATICAL AND COMPUTER MODELLING

УДК 681.5.015

Агибалов А. П.[1], Поляков М. А.[2]

[1]Магистрант Запорожского национального технического университета
[2]Канд. техн. наук, доцент Запорожского национального технического университета

ТРАНСЛЯТОР ПАРАМЕТРОВ МОДЕЛИ КОНЕЧНОГО АВТОМАТА ИЗ СРЕДЫ MATLAB В ПРИЛОЖЕНИЕ ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА

Предложена технология и средства автоматического переноса параметров модели конечного автомата из приложения Matlab в приложение человеко-машинного интерфейса. Рассмотрен пример применения технологии к модели электрического аппарата.

Ключевые слова: stateflow, конечный автомат, DDE-диалог, человеко-машинный интерфейс, тег.

ВВЕДЕНИЕ

В настоящее время приложения, созданные с помощью программных средств человеко-машинного интерфейса (HMI, англ. – Human Machine Interface), являются неотъемлемой частью SCADA-систем и контроллерных систем управления техническими объектами и процессами [1, 2]. В среде этих приложений выполняется часть логики пользователя, которая формализуется с помощью конечных автоматов [3, 4].

В ряде случаев, в процессе проектирования этих автоматов, прибегают к их моделированию в среде универсальных пакетов моделирования, например приложения Simulink пакета MATLAB [5]. Библиотека Stateflow этого пакета позволяет графически интерпретировать конечный автомат проектируемой системы управления как событийно-управляемую модель.

В существующей технологии проектирования операция переноса результатов моделирования логики управления пользователя в приложение HMI выполняется вручную, является трудоемкой, требующей высокой квалификации исполнителя.

Целью данной работы является сокращение трудоемкости проектирования приложений HMI путем создания технологии и средств автоматического переноса параметров модели конечного автомата из приложения Matlab в приложение HMI.

ТЕХНОГОЛИЯ И СРЕДСТВА ПЕРЕНОСА

Предлагаемая технология автоматического переноса параметров модели включает анализ файла модели Simulink и создание матричных эквивалентов элементов модели; инициацию DDE-диалога между приложениями Matlab и HMI; перенос созданных матричных эквивалентов в приложение HMI. Для реализации этой технологии созданы скрипты и функции Matlab, а также VBA-модули, встроенные в проект приложения HMI. Совокупность разработанных средств будем называть транслятором параметров модели конечного автомата из среды MATLAB в приложение человеко-машинного интерфейса, далее – транслятор. Транслятор предназначен для приложений HMI, созданных с помощью программного пакета RSVIEW32 компании Rockwell Automation (США) [2], но предлагаемая технология трансляции может быть использована при разработке трансляторов в другие пакеты HMI.

Программная структура транслятора представлена на рис. 1. Ядро транслятора – скрипт *analysis.m.* В процес-

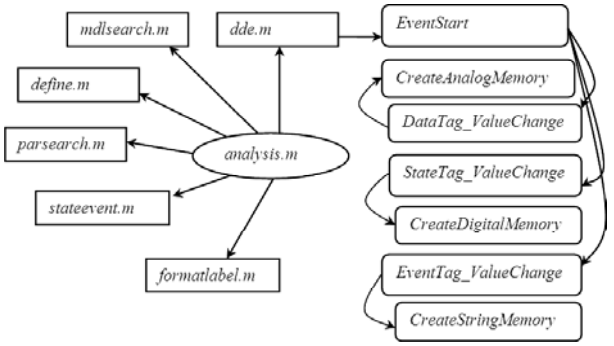

Рис. 1. Программная структура транслятора

се его выполнения вводится имя анализируемой Simulink-модели и имя проекта RSVIEW32, выбранного для генерации параметров модели, вызываются функции и скрипты для осуществления процесса трансляции.

Скрипт *mdlsearch.m* предназначен для поиска координат описания элементов модели. Скрипт *define.m* создан для формирования массивов элементов модели. Скрипт *parsearch.m* служит для поиска вышеназванных параметров в сформированных массивах. Скрипт *stateevent.m* создан для анализа меток состояний. Скрипт *formatlabel.m* отвечает за форматирование анализируемых данных для использования в SCADA-проекте. Скрипт *dde.m* инициализирует DDE-диалог с программой RSVIEW32 и посылает данные в проект; при этом VBA-модуль *EventStart* осуществляет процесс генерации тегов проекта при помощи пар модулей *DataTag_ValueChange, CreateAnalogMemory* и *StateTag_ValueChange,CreateDigitalMemory.* Скрипт *ddeexcel.m* служит для переноса результатов анализа в таблицу MS Excel для наглядного отображения структуры всей модели Simulink.

В результате работы программы создается база данных тегов SCADA-проекта, наиболее точно отвечающая параметрам элементов Simulink-модели.

ПРИМЕНЕНИЕ ТРАНСЛЯТОРА ДЛЯ ОБРАБОТКИ МОДЕЛИ

Рассмотрим использование транслятора на примере моделирования повторно-кратковременного режима работы электрического аппарата, при котором температура его частей за время нагрузки не достигает установившегося значения, а за время паузы не достигает температуры холодного состояния [6].

Ставится задача трансляции модели электрического аппарата из приложения моделирования в приложение мониторинга RSView32.

Simulink-модель электрического аппарата изображена на рис. 2. Параметрами модели являются время нагрузки *tw* и паузы *tp*, постоянные времени нагрева и охлаждения *tay* и *tay1* соответственно, температура окружающей среды T и граничная температура нагрева аппарата T_1. В примере приняты следующие значения констант: $tw = 1$ с, $tp = 2$ с, $tay = 7$ с, $tay1 = 15$ с, $T = 20$ град., $T_1 = 120$ град. Наблюдаемыми величинами являются мгновенная температура нагрева аппарата *Th* и режим его работы *mode*.

Блок Stateflow *Chart* реализует функцию конечного автомата. Диаграмма его состояний и переходов изображена на рис. 3.

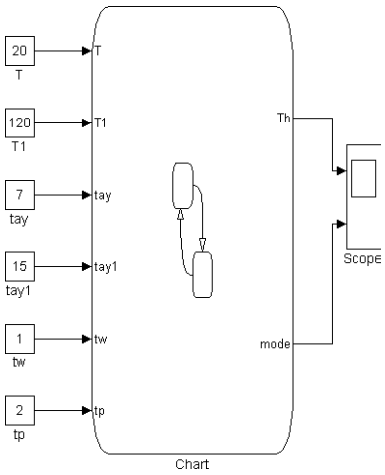

Рис. 2. Simulink-модель электрического аппарата

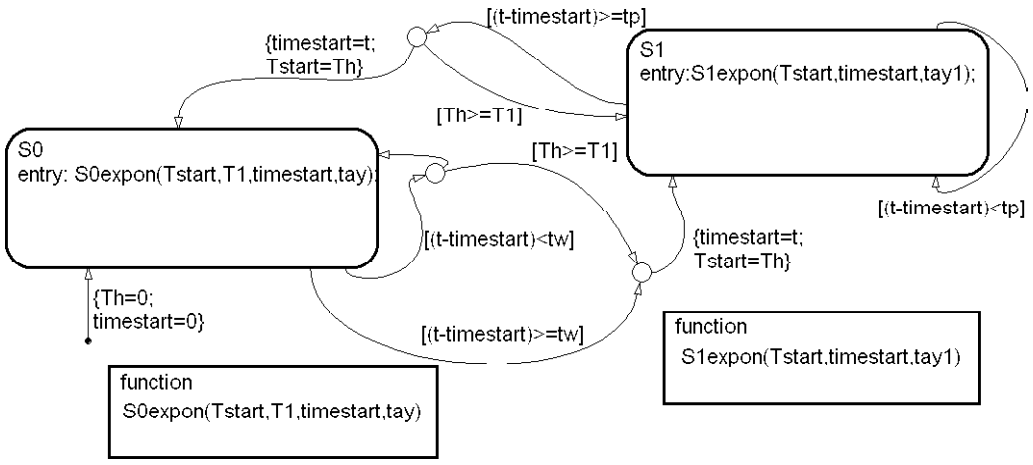

Рис. 3. Диаграмма состояний автомата и переходов блока Stateflow Chart

Автомат находится в одном из двух состояний: *S0* (под нагрузкой) и *S1* (без нагрузки). Каждое состояние характеризуется действием при входе в него (*entry:*), а именно – изменением температуры частей аппарата в зависимости от времени симуляции.

Действие при входе описывается графическими функциями *S0expon* и *S1expon*. Входными переменными функций являются константы модели.

Состояния модели связаны системой переходов, описываемых условиями и действиями, а также соединительных узлов для упрощения диаграммы Stateflow (рис. 3). В процессе симулирования температура аппарата образует экспоненциально нарастающий и спадающий процесс.

Результатами работы транслятора являются:

1) матричные эквиваленты элементов модели в рабочей области Matlab (рис. 4);

2) база данных тегов в HMI-проекте (рис. 5);

3) таблица на листе Excel с параметрами модели автомата (рис. 6).

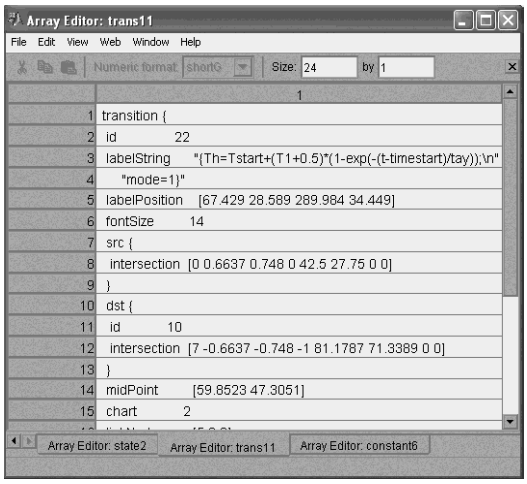

Рис. 4. Массив, отвечающий переходу диаграммы

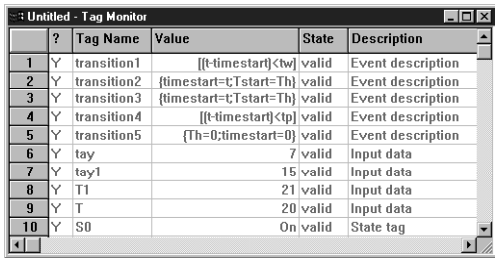

Рис. 5. Монитор тегов RSView32

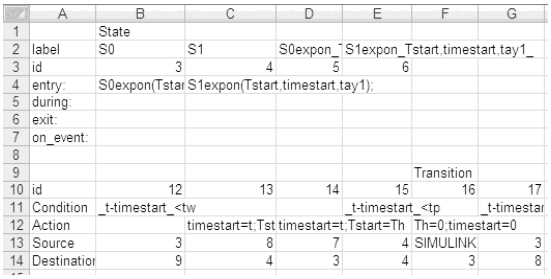

Рис. 6. Отчет по трансляции на листе Excel

ВЫВОДЫ

Для создания HMI-проектов с клиент-серверной или распределенной архитектурой используются SCADA-системы. Логика пользователя приложений HMI формализуется в виде конечного автомата и может быть смоделирована в программе Simulink пакета Matlab. Основными элементами модели являются входные и выходные параметры, состояния автомата и переходы между ними.

Разработанный транслятор параметров модели является комплексом программ, выполняемых в среде Matlab и VBA-надстройке RSView32. Трансляция основана на механизме DDE. Трансляции подвергаются:

1) параметры состояний: название, id-номер, действия при входе, выходе, во время активности состояния и при совершении установленного события;

2) параметры переходов: id-номер, условие совершения, параллельное действие, начальная и конечная точка;

3) входные и выходные данные: id-номер, имя переменной, тип данных, тип переменной, величина.

Автоматическое отображение результатов анализа модели на листе Excel упрощает восприятие сложных систем. Разработанный инструмент удачно прошел тестирование на demo-примерах приложения Simulink, в частности, на модели нагревателя, инфракрасной системы наведения ракеты, системы подачи топлива в автомобиле. В то же время предложенная технология имеет ограниченную функциональность, поскольку не генерирует автоматически события проекта RSView32, не создает дисплеи и сигналы тревоги для мониторинга контролируемых величин, и потому имеет перспективу улучшения.

СПИСОК ЛИТЕРАТУРЫ

1. *Олсон, Г.* Цифровые системы автоматизации и управления / Г. Олсон , Д. Пиани. – С. Пб. : Невский Диалект, 2001. – 557 с. : ил.
2. RSView32 : руководство пользователя [Електронний ресурс] / Rockwell Software Inc. – Электрон. дан. – М., [2000]. — Режим доступу: www.eskovostok.ru/_docs/9399-2se32ug-ru.pdf, вільний. – Загл. с экрана.
3. *Поляков, М. А.* Теоретико-множественная модель интегрированной контроллерной системы управления / М. А. Поляков // Системні технології. – 2009. – № 4. – С. 131–137.
4. *Поляков, М. А.* Логическое управление объектами электрических систем в среде приложения человеко-машинного интерфейса / М. А. Поляков // Наукові праці Донецького національного технічного університету. – 2009. – № 9(158). – С. 197–201.
5. *Дэбни, Д.* Simulink 4. Секреты мастерства / Д. Дэбни , Т. Харман. – М. : БИНОМ. Лаборатория знаний, 2003. – 404 с.
6. Электрические и электронные аппараты : учебник для вузов / под ред. Ю. К. Розанова. – 2-е изд., испр. и доп. – М. : Информэлектро, 2001. – 420 с. : ил.

Стаття надійшла до редакції 16.12.2010.
Після доробки 01.02.2011.

Агібалов О. П., Поляков М. О.

ТРАНСЛЯТОР ПАРАМЕТРІВ МОДЕЛІ КІНЦЕВОГО АВТОМАТА ІЗ СЕРЕДОВИЩА MATLAB У ДОДАТОК ЛЮДИНО-МАШИННОГО ІНТЕРФЕЙСУ

Запропоновано технологію та засоби автоматичного переносу параметрів моделі кінцевого автомату з додатку Matlab до додатку людино-машинного інтерфейсу. Розглянуто приклад застосування технології до моделі електричного апарата.

Ключові слова: stateflow, кінцевий автомат, DDE-діалог, людино-машинний інтерфейс, тег.

Agibalov A. P., Polyakov M. A.

TRANSLATOR OF FINITE STATE MACHINE MODEL PARAMETERS FROM MATLAB ENVIRONMENT INTO HUMAN-MACHINE INTERFACE APPLICATION

Technology and means for automatic translation of FSM model parameters from Matlab application to human-machine interface application is proposed. The example of technology application to the electric apparatus model is described.

Key words: stateflow, finite-state machine, DDE-dialog, human-machine interface, tag.

УДК 004.056.53:004.75

Андрущенко Д. М.[1], Варава М. Ю.[2], Неласа Г. В.[3]

[1]Молодший науковий співробітник Запорізького національного технічного університету
[2]Провідний спеціаліст з інформаційних технологій КБ Приватбанк
[3]Канд. техн. наук, доцент Запорізького національного технічного університету

РОЗПАРАЛЕЛЮВАННЯ ρ - І λ - МЕТОДІВ ПОЛЛАРДА РОЗВ'ЯЗАННЯ ЗАДАЧІ ДИСКРЕТНОГО ЛОГАРИФМУВАННЯ

Проведено аналіз ефективності розпаралелювання ρ - і λ -методів Полларда при вирішенні задачі дискретного логарифмування. Наводиться теоретична оцінка часу виконання завдання на паралельній системі. Проведено порівняння результатів практичних і теоретичних розрахунків. Зроблені заміри часу виконання розпаралелених методів.

Ключові слова: методи Полларда, дискретний логарифм, розпаралелювання, складність криптоалгоритма, оцінка складності.

ВСТУП

При створенні систем захисту інформації широко застосовуються асиметричні алгоритми. Надійність таких систем основана на трудомісткості виконання одного з наступних типів зворотних перетворень: розкладання великих чисел на прості множники; обчислення дискретного логарифму; обчислення коренів алгебраїчних рівнянь [1, 2]. Однак розвиток методів прискорених обчислень, в тому числі застосування багатопроцесорних систем паралельних рішень, викликає небезпеку зниження ступеню захисту криптосистем. Тому для оцінки надійності систем захисту та їх вдосконалення необхідно дослідження методів паралельних рішень для проведення названих перетворень.

ПОСТАНОВКА ЗАДАЧІ

Одними з найбільш розповсюджених асиметричних криптосистем є ті, що створені на базі еліптичних кривих $y^2 = x^3 + ax + b \bmod p$ над простим полем $GF(p)$. Якщо P є базовою точкою адитивної групи точок еліптичної кривої простого порядку n, точка Q належить заданій групі точок еліптичної кривої, то злом криптографічної системи полягає у розв'язанні рівняння $m \cdot P = Q$ відносно m, де $1 < m < n-1$ (адитивний аналог задачі дискретного логарифмування).

Надійність систем захисту інформації, злом яких оснований на розв'язанні задачі дискретного логарифмування залежить від величини n. Однак, збільшення n, окрім підвищення надійності, призводить до збільшення часу роботи криптографічних алгоритмів. Тому для побудови ефективних алгоритмів необхідний компромісний варіант, що забезпечує достатню надійність захисту при прийнятному рівні модуля n з точки зору швидкості роботи алгоритму. Поява нових методів прискорення обчислень дискретного логарифму, одним з яких є розпаралелювання, викликає необхідність збільшення параметру n. Тому оцінка ступеня надійності криптографічних систем, дослідження можливості їх злому шляхом розпаралелювання процесу розв'язання задачі дискретного логарифмування є актуальною проблемою.

Відомі різні алгоритми послідовного вирішення цього завдання, в тому числі: великих-малих кроків, Поліга-Хеллмана, ρ-Полларда, λ-Полларда, Адлемана, index-calculus [1–3]. Більшість з них піддаються розпаралелюванню. У даній роботі для перевірки працездатності системи та оцінки ефективності даного підходу були розглянуті ρ-метод і λ-метод Полларда [2].

Метод ρ -Полларда. Ідея методу полягає в побудові послідовності точок Z_i еліптичної кривої

$$Z_i = A_i P + B_i Q, \qquad (1)$$

де $1 < A_i, B_i < n-1$,