УДК 621.3

Н.В. Якимец, В.С. Харченко

Национальный аэрокосмический университет им. Н.Е. Жуковского, «ХАИ», Харьков

ОТКАЗОУСТОЙЧИВЫЕ ЦИФРОВЫЕ СИСТЕМЫ УПРАВЛЕНИЯ С ПРОГРАММИРУЕМОЙ ЛОГИКОЙ НА ОСНОВЕ ЧАСТИЧНО РАБОТОСПОСОБНЫХ АВТОМАТОВ: МОДЕЛИ И РЕАЛИЗАЦИЯ

В работе рассматриваются понятия определенности и корректности цифрового автомата. Предлагаются методы проектирования отказоустойчивых цифровых систем с программируемой логикой на основе частично определенных и частично корректных автоматов, которые синтезируются с помощью генетических алгоритмов.

системы управления, отказоустойчивость, диверсификация, генетические алгоритмы, цифровые автоматы

Введение

Темпы наращивания функциональности цифровых устройств на сегодняшний день значительно опережают развитие существующих методов повышения их надежности. В такой ситуации эффективным средством защиты от сбоев в работе является построение отказоустойчивых систем. В первую очередь это касается систем управления (СУ) для ядерной, военной и авиационной промышленности, поскольку к ним предъявляются жесткие требования по надежности [1]. Анализ методов и средств создания цифровых СУ показал, что основные характеристики таких систем – надежность, стоимость/производительность, масштабируемость – закладываются уже на этапе проектирования посредством выбора качественной элементной базы, а также архитектурных решений, способных обеспечить высокий уровень отказоустойчивости будущей СУ. При этом программируемая логика, с учетом ее быстродействия, надёжности, вычислительной мощности, представляется разумным выбором для создания отказоустойчивых цифровых СУ.

Высокий уровень отказоустойчивости СУ может быть достигнут за счет использования различных видов избыточности, в частности, аппаратной версионной избыточности. Ключевая идея такого подхода состоит в получении минимально коррелированных вариантов одного и того же проекта. При создании многоверсионных отказоустойчивых цифровых СУ с программируемой логикой (ЦСУПЛ) наиболее эффективным представляется использование различных подходов к проектированию, поскольку в данном случае значительно увеличивается мощность множества вариантов получения менее коррелированных версий.

В данном аспекте можно выделить подход, который основывается на применении систем автоматизированного проектирования (САПР) [1], и подход, использующий логику работы генетических алгоритмов (ГА) [2]. Однако, часто при проектировании цифровых СУ с программируемой логикой (ЦСУПЛ) с помощью ГА формируются версии, у которых работоспособное состояние сохраняется не для всех наборов входных данных [3]. При этом информация о текущем работоспособном или неработоспособном состоянии версии известна заранее. Распространенной практикой в данном случае является построение дублированной или мажоритарной схемы, где версии включены таким образом, чтобы суммарное множество их работоспособных состояний покрывало все множество входных данных.

Анализ работ в данной области показывает, что широкое распространение получили отказоустойчивые многоверсионные цифровые системы, выполненные на полностью работоспособных версиях, и существует детально разработанная методология создания таких систем [1]. В то же время приводятся примеры реализации мажоритарных и дублированных систем с частично работоспособными версиями [1, 3]. Однако, отсутствуют методики синтеза отказоустойчивых систем такого класса на основе частично работоспособных версий. На сегодняшний день опубликованы примеры реализации простых проектов цифровых устройств с помощью ГА [3], однако, не разработана методика, позволяющая синтезировать более сложные цифровые системы.

Целью данной работы является разработка моделей и методов синтеза отказоустойчивых ЦСУПЛ, выполненных на основе цифровых частично работоспособных автоматов.

1. Определения и свойства

Каждый цифровой автомат может быть описан с позиций уровня его определенности и корректности. Понятие корректности характеризует степень соответствия логики функционирования автомата тем требованиями, которые были изложены в техническом задании при проектировании автомата. Следовательно, чем выше степень соответствия логики работы цифрового автомата требованиям технического задания, тем выше его корректность. Понятие определенности подразумевает степень предварительной информированности разработчика о корректности цифрового автомата. Основываясь на таких понятиях как корректность и определенность цифрового автомата, введем определения: полностью и частично корректного автомата, а также полностью и частично определенного автомата.

Полностью корректным автоматом (ПКА) называется автомат, у которого каждому входному сигналу x_i из множества всех входных сигналов X соответствует корректный (требуемый) выходной сигнал y_i из множества выходных сигналов Y_c , т.е.

$$\forall\, x_i \in X: x_i \to y_i;\ y_i \in Y_c;\ Y_c = Y,$$

где x_i – текущий входной сигнал автомата; X – множество всех входных сигналов автомата; y_i – выходной сигнал автомата, соответствующий x_i; Y_c – множество корректных (требуемых) выходных сигналов автомата; Y – общее множество выходных сигналов автомата.

ПКА называют работоспособным, если каждому входному сигналу x_i из множества входных сигналов X соответствует верный выходной сигнал y_i из множества верных выходных сигналов Y_r , т.е.

$$\forall\, x_i \in X: x_i \to y_i;\ y_i \in Y_r;\ Y_r = Y_c = Y,$$

где Y_r – множество верных выходных сигналов автомата.

ПКА называют неработоспособным, если существует хотя бы один входной сигнал x_i из множества всех входных сигналов X, которому не соответствует верный выходной сигнал y_i из множества верных выходных сигналов Y_r, т.е.

$$\exists\, x_i \in X: x_i \to y_i;\ y_i \in Y_r;\ Y_r \subset Y.$$

Автомат называется частично корректным (ЧКА), если существует хотя бы один входной сигнал x_i из множества всех входных сигналов X, которому не соответствует требуемый выходной сигнал y_i из множества требуемых выходных сигналов Y_c, т.е.

$$\exists\, x_i \in X: x_i \to y_i;\ y_i \notin Y_c;\ Y_c \subset Y.$$

Утверждение 1: ЧКА является неработоспособным ПКА, поскольку в данном случае $Y_r^{\text{ПКА}} = Y_c^{\text{ЧКА}}$.

Легко заметить, что несколько ЧКА могут составлять ПКА, если каждому входному сигналу x_i из множества всех входных сигналов X для ПКА соответствует корректный выходной сигнал y_i одного из ЧКА, т.е.

$$\forall\, x_i \in X: x_i \to y_i;\ y_i \in Y_c^{\text{ПКА}};\ Y_c^{\text{ПКА}} = Y^{\text{ПКА}};$$

$$Y_c^{\text{ПКА}} = Y_c^{\text{ЧКА 1}} \cup Y_c^{\text{ЧКА 2}} \cup \ldots \cup Y_c^{\text{ЧКА n}}.$$

Таким образом, ПКА, состоящий из нескольких ЧРА, может сохранять работоспособное состояние до тех пор, пока его каждому входному сигналу x_i из множества входных сигналов X будет соответствовать верный выходной сигнал y_i из множества верных выходных сигналов Y_r одного из ЧКА.

Определим минимальный и полный функциональный базис для ЧКА:

– множество ЧКА составляет полный функциональный базис, если оно реализует требуемый работоспособный ПКА;

– множество ЧКА составляет минимальный функциональный базис, если потеря работоспособности хотя бы одного из ЧКА, составляющих ПКА, приводит к потере работоспособности ПКА.

Утверждение 2: необходимым и достаточным условием для того, чтобы получить ПКА из нескольких ЧКА, является наличие минимального функционального базиса, который должны составлять ЧКА по отношению к требуемому ПКА.

Полностью определенным автоматом (ПОА) является автомат, у которого каждому входному сигналу x_i из множества всех входных сигналов X соответствует выходной сигнал y_i такой, что информация о его корректности (принадлежит или не принадлежит множеству Y_c) заранее известна, т.е.

$$\forall\, x_i \in X: x_i \to y_i;\ y_i \in Y_s;\ Y_s = Y\ ,$$

где Y_s – множество определенных (специфицированных) выходных сигналов автомата.

ПОА называют работоспособным, если каждому входному сигналу x_i из множества всех входных сигналов X соответствует выходной сигнал y_i, значение которого совпадает с заранее известной информацией о его корректности (принадлежит или не принадлежит множеству Y_c).

ПОА называют неработоспособным, если существует хотя бы один входной сигнал x_i из множества всех входных сигналов X, которому соответствует выходной сигнал y_i, значение которого не совпадает с заранее известной информацией о его корректности (принадлежит или не принадлежит множеству Y_c).

Автомат называется частично определенным (ЧОА), если существует хотя бы один входной сигнал x_i из множества всех входных сигналов X, которому соответствует выходной сигнал y_i такой, что информация о его корректности (принадлежит или не принадлежит множеству Y_c) заранее не известна, т.е.

$$\exists\, x_i \in X: x_i \to y_i;\ y_i \notin Y_s;\ Y_s \subset Y.$$

Множество ЧОА может образовывать ПОА, если каждому входному сигналу x_i из множества всех входных сигналов X для ПОА соответствует выходной сигнал y_i одного из ЧОА такой, что информация о его корректности (принадлежит или не принадлежит множеству Y_c для ПОА) заранее известна.

$$\forall\, x_i \in X: x_i \to y_i;\ y_i \in Y_s^{\text{ПОА}};\ Y_s^{\text{ПОА}} = Y^{\text{ПОА}};$$

$$Y_s^{\text{ПОА}} = Y_s^{\text{ЧОА 1}} \cup Y_s^{\text{ЧОА 2}} \cup \ldots \cup Y_s^{\text{ЧОА n}}.$$

Таким образом, ПОА, состоящий из нескольких ЧКА, может сохранять работоспособное состояние до тех пор, пока его каждому входному сигналу x_i из множества входных сигналов X будет соответствовать выходной сигнал y_i одного из ЧКА, значение которого совпадает с заранее известной информацией о его корректности (принадлежит или не принадлежит множеству Y_c).

Определим минимальный и полный функциональный базис для ЧОА:

– множество ЧОА составляет полный функциональный базис, если оно реализует требуемый работоспособный ПОА;

– множество ЧОА составляет минимальный функциональный базис, если потеря работоспособности хотя бы одного из ЧОА, составляющих ПОА, приводит к потере работоспособности ПОА.

Утверждение 3: необходимым и достаточным условием для того, чтобы получить ПОА из нескольких ЧОА, является наличие минимального функционального базиса, который должны составлять ЧОА по отношению к требуемому ПОА.

Основываясь на определениях корректных и определенных автоматов, легко заметить, что автомат может быть: полностью определенным полностью корректным; полностью определенным частично корректным; частично определенным полностью корректным; частично определенным частично корректным.

Полностью определенным полностью корректным (ПОПК) автоматом называется автомат, у которого каждому входному сигналу x_i из множества всех входных сигналов X соответствует выходной сигнал y_i такой, что

$$\forall\, x_i \in X:\ x_i \to y_i;\ \ y_i \in Y_s \text{ и } y_i \in Y_c;\ Y_s = Y_c = Y.$$

Автомат называется полностью определенным частично корректным (ПОЧК), если существует хотя бы один входной сигнал x_i из множества всех входных сигналов X, которому соответствует выходной сигнал y_i такой, что

$$\exists\, x_i \in X:\ x_i \to y_i;\ \ y_i \in Y_s \text{ и } y_i \notin Y_c;\ Y_s = Y;\ Y_c \subset Y.$$

Частично определенным полностью корректным (ЧОПК) автоматом называется автомат, у которого каждому входному сигналу x_i из множества входных наборов X_s соответствует выходной сигнал y_i такой, что

$$\forall\, x_i \in X_s:\ x_i \to y_i;\ \ y_i \in Y_s \text{ и } y_i \in Y_c;$$
$$Y_s = Y_c,\ Y_s \subset Y;\ Y_c \subset Y;\ X_s \subset X.$$

Автомат называется частично определенным частично корректным (ЧОЧК), если существует хотя бы один входной сигнал x_i из множества входных сигналов X_s, которому соответствует выходной сигнал y_i такой, что

$$\exists\, x_i \in X_s:\ x_i \to y_i;\ \ y_i \in Y_s \text{ и } y_i \notin Y_c;$$
$$Y_c \subset Y_s;\ Y_s \subset Y;\ X_s \subset X.$$

Утверждение 4: ПОПК автомат может быть составлен из ЧОЧК (и/или ПОЧК, ЧОПК) автоматов, если каждому входному сигналу x_i из множества всех входных сигналов X для ПОПК автомата соответствует корректный (требуемый) выходной сигнал y_i одного из ЧОЧК (ПОЧК, ЧОПК) автоматов, при этом информация о его корректности (принадлежит или не принадлежит множеству Y_c для ПОПК автомата) заранее известна (рис. 1), т.е.

$$\forall\ x_i \in X:\ x_i \to y_i;\ y_i \in Y_s^{\text{ПОА}} \text{ и } y_i \in Y_c^{\text{ПОА}};$$
$$Y_s^{\text{ПОА}} = Y_c^{\text{ПОА}} = Y^{\text{ПОА}};$$
$$Y_s^{\text{ПОА}} = Y_s^{\text{ЧОА 1}} \cup Y_s^{\text{ЧОА 2}} \cup \ldots \cup Y_s^{\text{ЧОА n}};$$
$$Y_c^{\text{ПОА}} = Y_c^{\text{ЧОА 1}} \cup Y_c^{\text{ЧОА 2}} \cup \ldots \cup Y_c^{\text{ЧОА n}}.$$

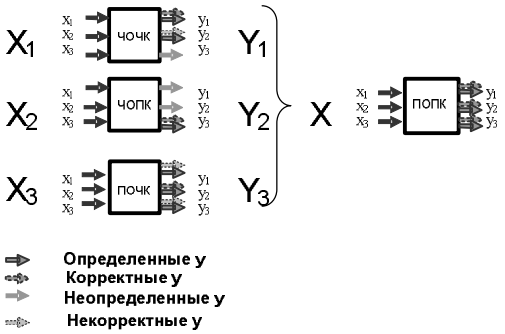

Рис. 1. Полностью определенный полностью корректный автомат, составленный из частично определенных и частично корректных автоматов

2. Синтез отказоустойчивых ЦСУПЛ на основе частично определенных и частично корректных автоматов

Процесс создания ЦСУПЛ на ЧОА и ЧКА, в рамках ГА-проектирования подразумевает два аспекта: выбор и обоснование типа автоматов, на которых будет реализована ЦСУПЛ; выбор уровня корректности и определенности автоматов.

Так простые системы, для которых основным требованием является компактность и при этом временные затраты на создание не критичны, рекомендуется строить на основе ПОПК автоматов ввиду их простоты. Если же требования компактности и быстроты реализации являются первоочередными, то целесообразно строить систему на ПОЧК либо ЧОПК автоматах. При этом в случае использования ЧОПК автоматов будет наблюдаться экономия времени за счет возрастания сложности ЦСУПЛ, а в случае ПОЧК автоматов простота системы будет достигнута за счет увеличения времени, требуемого для ее синтеза. На основе ЧОЧК автоматов рекомендуется строить сложные ЦСУПЛ, для которых фактор времени, затрачиваемого на синтез, является критичным, поскольку, уменьшая время тестирования автоматов, мы тем самым ускоряем процесс их создания.

В процессе синтеза ЦСУПЛ на основе ПОПК автоматов выполняется серия последовательных запусков ГА до тех пор, пока не будет получена работоспособная полностью корректная версия системы. При вычислении приспособленности индивидуумов тестируются все наборы входных и выходных данных.

Для построения ЦСУПЛ на основе ПОЧК автоматов, во-первых, формируется множество ПОЧК автоматов путем последовательных запусков ГА (в процессе вычисления приспособленности индивидуумов тестируются все наборы входных и выходных данных); во-вторых, для каждого ПОЧК автомата выполняется анализ заранее известной информации о множестве входных минтермов, которым соответствуют корректные или некорректные выходные сигналы. При этом ЧКА подбираются таким образом, чтобы они составляли по крайней мере минимальный функциональный базис системы (ПОПК автомата). В противном случае производится дополнительная серия запусков ГА до выполнения данного условия. Реконфигурация системы осуществляется в зависимости от наборов входных данных на основании известной информации о рабочем состоянии ПОЧК автоматов или в случае отказа одного или нескольких ПОЧК автоматов.

Данная методика построения ЦСУПЛ обеспечивает ее высокую надежность, во-первых, за счет реализации гибкого управления ПОЧК автоматами в случае, когда информация об их корректности для каждого из наборов входных данных известна заранее. При этом вся система остается полностью работоспособной до тех пор, пока суммарное множество работоспособных состояний ПОЧК автоматов покрывает все множество входных данных для ПОПК автомата. Во-вторых, значительное возрастание уровня надежности ЦСУПЛ, построенной на основе ПОЧК автоматов, выполняется за счет автоматического частичного резервирования системы на тех наборах входных данных, которым соответствует большее число определенных корректных состояний ПОЧК автоматов, чем необходимо для сохранения корректности всей системы. Таким образом, можно говорить о своего рода коэффициентах избыточности ПОПК автомата, построенного на основе ЧКА, для каждого минтерма его входных данных, которые определяются избыточностью определенных корректных состояний всех ПОЧК автоматов для текущего минтерма. Легко заметить, что эти коэффициенты могут быть неодинаковы для всего множества наборов входных данных системы.

Для синтеза ЦСУПЛ на основе ЧОПК автоматов, во-первых, выполняется серия последовательных запусков ГА, пока не будет сформировано такое множество ЧОПК автоматов, чтобы ЧОА составляли по крайней мере минимальный функциональный базис требуемой ЦСУПЛ; во-вторых, при вычислении приспособленности индивидуумов используется так называемый метод «скользящего тестирования». Он заключается в том, что при вычислении приспособленности каждого индивидуума популяции тестируются не все наборы входных и выходных данных. При этом вводится понятие ширины окна нетестируемой области ε, оптимальное значение которого вычисляется по следующей формуле:

$$\varepsilon = 2^n / m, \qquad (1)$$

где 2^n – количество входных минтермов; m – количество индивидуумов в текущей популяции.

Анализируя (1), легко видеть, что при $\varepsilon < 2^n / m$ возрастает надежность такого ЧОА за счет уменьшения количества нетестируемых минтермов (увеличение степени определенности автомата); при $\varepsilon > 2^n / m$ надежность ЧОА снижется за счет снижения степени определенности автомата. Однако, максимальная ширина окна нетестируемой области должна быть такой, чтобы каждому входному минтерму соответствовало хотя бы одно определенное выходное состояние одного из ЧОА.

Таким образом, метод «скользящего тестирования» заключается в следующем:

– выбирается ширина окна нетестируемой области ε;

– для каждого индивидуума позиция окна нетестируемой области устанавливается в позицию [i, i + ε), где i – номер индивидуума в текущей популяции;

– определяется приспособленность каждого индивидуума текущей популяции, равная количеству минтермов, которым соответствуют верные выходные сигналы автомата, при этом минтермы, ограниченные окном нетестируемой области не проверяются;

– ГА выполняет свою работу, пока не будет сформировано множество работоспособных полностью корректных версий системы, которые на основании предварительного анализа объединяются в дублированные или мажоритарные структуры таким образом, чтобы ЧОА образовывали минимальный функциональный базис системы.

Реконфигурация системы осуществляется в зависимости от наборов входных данных на основании известной информации о ширине и позиции неопределенных областей ЧОПК автоматов или в случае отказа одного или нескольких ЧОПК автоматов.

Разработка цифровой системы на основе ЧОЧК автоматов объединяет в себе два рассмотренных выше метода построения системы на ПОЧК и ЧОПК автоматах. В рамках данного метода, как и при синтезе системы на ЧОПК автоматах, также используется «скользящее тестирование» с тем различием, что ГА выполняет свою работу до тех пор, пока не будет сформировано множество работоспособных частично корректных и частично определенных версий системы таких, что оба подмножества ЧОА и ЧКА должны представлять минимальный функциональный базис. Реконфигурация системы осуществляется в зависимости от наборов входных данных на основании известной информации о ширине и позиции неопределенных областей ЧОЧК автоматов, а также информации о рабочем состоянии ЧОЧК автоматов, или в случае отказа одного или нескольких ЧОЧК автоматов. Данный метод построения

ЦСУПЛ включает в себя все достоинства обоих методов построения системы на ПОЧК и ЧОПК автоматах, поскольку здесь реализуется гибкое управления автоматами в случае, когда информация о корректности и определенности каждого набора входных данных известна заранее; выполняется автоматическое частичное резервирования системы на тех наборах входных данных, которым соответствует большее число определенных корректных состояний автоматов, чем необходимо для сохранения корректности всей системы; значительно сокращается время синтеза автоматов за счет использования метода «скользящего тестирования», что позволяет создавать сложные ЦСУПЛ в сжатые сроки.

3. Эксперимент

Для иллюстрации предложенного метода проектирования ЦСУПЛ был проведен эксперимент по созданию программной модели терморегулятора для самолета АН-70 на ПЛИС с помощью ГА. Моделирование проводилось на уровне реализации схемы в кристалле. Согласно эксперименту модель терморегулятора должна комбинироваться из нескольких ЧОЧК автоматов, синтезированных с помощью ГА. Каждая частично работоспособная версия терморегулятора представляет собой граф связей между логическими ячейками ПЛИС. В качестве метрики диверсности была выбрана степень различия топологии графов версий, получаемых в результате моделирования. Исходные данные, принятые при моделировании, приведены в табл. 1.

Таблица 1

Исходные данные

Название	Значение
Площадь поля моделирования)	4×4
Требования к проекту, таблица истинности	Входные данные: 1-й бит определяет знак, 2-7 биты определяют значение температуры по °С. Выходные данные: 01 – температура ниже 15°С, 10 – температура от 15°С до 35 °С, 11 – температура выше 35°С
- размер популяции	50
- тип отбора	рулетка, ранговый, элитный
- вероятность скрещивания	0,80
- вероятность мутации	0,10
- вероятность инверсии	0,10

В результате эксперимента было получено два индивидуума в виде ЧОЧК автоматов, реализующих заданную функциональность терморегулятора (рис. 2). Сравнивая полученную модель с разработанной ранее моделью, выполненной на основе ПОЧК автоматов, следует отметить, что в данном эксперименте подходящие индивидуумы были получены в течение первых 68 итераций ГА, тогда как во втором случае – после 400 – 800.

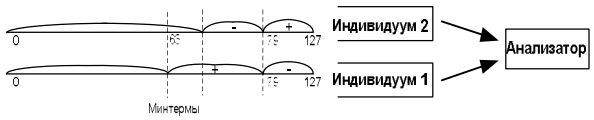

Рис. 2. Модель терморегулятора для самолета АН-70, полученная с помощью ГА

Полученная модель терморегулятора была также реализована на ПЛИС EP1K10TC144-3 (семейство ACEX 1K) в среде Quartus II v.6.0. Сравнивая проект, полученный с помощью ГА, с существующим аналогом, разработанным с помощью стандартных средств САПР, следует отметить компактность первого, поскольку общее число задействованных логических ячеек в нем равно 27 (два индивидуума и блок контроля), тогда как во втором проекте их 74.

Выводы

В данной работе были рассмотрены понятия определенности и корректности цифровых автоматов, согласно которым автоматы могут быть полностью или частично определенными, а также полностью или частично корректными. Были разработаны методы создания ЦСУПЛ на таких частично работоспособных автоматах. Использование этих методов при построении ЦСУПЛ обеспечивает высокий уровень надежности системы за счет реализации гибкого управления автоматами, а также частичного резервирования на тех наборах входных данных, которым соответствует число определенных и корректных состояний автомата больше, чем необходимо по условию сохранения функциональности всей системы. Дальнейшая работа в данной области может касаться разработки схем адаптивного резервирования отказоустойчивых систем, выполненных на основе частично работоспособных автоматов, а также создания методики проектирования ЦСУПЛ, являющихся, по сути, автоматами с памятью.

Список литературы

1. Kharchenko V.S., Tarasenko V.V., Ushakov A.A. The Fault-tolerant PLD-based Embedded Digital Systems. – Kh.: National Airspace University «KhAI», 2004. – 210 p.

2. Yakymets N., Kharchenko V. Diversification Techniques of Fault-Tolerant Systems on FPGAs Using CAD-based and Genetic Algorithm-Based Designs. // Системи озброєння і військова техніка. – 2006. – № 4(8). – С. 114-117.

3. Sverre Vigander, Evolutionary fault repair of electronics in space applications. Dissertation of the Dept. of Computer & Information Science, Norwegian University of Science and Technology (NTNU), Trondheim, 2001.

Поступила в редколлегию 12.03.2007

Рецензент: д-р техн. наук, проф. В.М. Илюшко, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.