УДК 681.5

М.Л. МАЛИНОВСКИЙ

Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Украина

МОДЕЛИ И МЕТОДЫ УПРАВЛЕНИЯ ОБЪЕКТАМИ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ НА ОСНОВЕ БЕЗОПАСНЫХ ПЛИС-КОНТРОЛЛЕРОВ С ПАРАЛЛЕЛЬНОЙ АРХИТЕКТУРОЙ

Разработаны: модели и методы синтеза безопасных логических автоматов параллельного действия (БЛП-автоматов) для ПЛИС-контроллеров, которые защищены от опасных искажений входных, внутренних и выходных состояний за счет применения резервирования, динамического кодирования информации и использования методов многократного контроля правильности реализации алгоритмов; табличный язык THDL и технология программирования безопасных ПЛИС-контроллеров; методы и средства безопасного формирования управляющих воздействий для объектов критического применения, в которых используется принцип последовательного преобразования параметров сигналов, динамически изменяющихся во времени.

Ключевые слова: *ПЛИС-контроллер, БЛП-автомат, табличный язык THDL, объекты критического применения, функциональная безопасность, безопасный генератор гармонических сигналов.*

Введение

Положение дел в области разработки и создания систем управления объектами критического применения (ОКП) коротко можно охарактеризовать следующим образом:

– релейные системы, которые на сегодняшний день во многих отраслях явно преобладают, устарели и требуют замены;

– внедряемые и уже находящиеся в эксплуатации микропроцессорные (МП) системы по некоторым важным показателям (в том числе экономическим и показателям безопасности) зачастую явно уступают релейным.

Многие преимущества, которые принято приписывать МП-системам, могут быть подвергнуты сомнению, в том числе такие (на первый взгляд, очевидные), как высокое быстродействие и надежность. Одновременно с этим, в силу ряда объективных причин (сложившейся монополии на рынке производства реле 1-го класса надежности, тенденции роста стоимости релейных средств и снижения стоимости МП средств, смены поколений специалистов и т.д.) актуальность разработки и внедрения МП-систем управления ОКП не вызывает сомнений.

1. Анализ состояния проблемы

Принято выделять три уровня, на которых требуется решение задач обеспечения безопасности МП-систем управления ОКП: программный, аппаратный на уровне сопряжения с исполнительными механизмами, аппаратный на уровне реализации алгоритмов управления. Выделим недостатки, присущие каждому из уровней.

Методы сопряжения микроэлектронных структур с исполнительными механизмами:

– как правило, ориентированы на двухканальную реализацию микроэлектронных структур и плохо согласуются с трех и 4-х канальными системами;

– требуют выделения ведущего и ведомого каналов и жесткой синхронизации их функционирования, в результате этого их работу можно считать независимой лишь условно, и при расчетах безопасности делать соответствующие допущения;

– формирование выходных сигналов каждого канала осуществляется по идентичным алгоритмам с одинаковой формой сигналов на выходе каждого канала, что ограничивает возможности введения многоверсионности в алгоритмы реализации устройств управления ОКП.

Для описания алгоритмов логического управления широко применяются различные автоматные модели.

Среди известных автоматных моделей систем управления ОКП следует выделить следующие:

1. Автоматные модели безопасных систем железнодорожной автоматики и телемеханики [1] – позволяют выполнить синтез безопасных автоматов на так называемых h_1-надежных элементах, т.е. элементах с несимметричными отказами. Такими элементами, в частности, являются реле 1-го

класса надежности.

2. Автоматные модели многоверсионных информационно-управляющих систем [2] – позволяют решать задачи оптимального выбора методов многоверсионного резервирования.

Известные модели не учитывают:

1. Использование методов временного кодирования входных и выходных сигналов.

2. Реализацию безопасных переходов автоматов, реализованных на элементах с симметричными отказами, из одного состояния в другое.

3. Синтез элементов памяти, реализующих функцию многократного контроля правильности реализации алгоритмов.

Обеспечение безопасности управления ОКП в значительной степени зависит от качества программного обеспечения (ПО). В настоящее время для программирования ПЛИС используются следующие подходы: стандартные, с текстовым или визуальным вводом описаний – они применяются наиболее широко; а также перспективные, которые можно разделить на две группы: ориентированные на архитектуру логических управляющих автоматов, и на способы описания алгоритмов [3].

Эти два подхода, по сути, образуют тезис и антитезис, т.е. два противоположных направления в совершенствовании методов программирования; разрешение противоречий, возникающих при движении в этих направлениях, может быть положено в основу стратегии создания языков и технологий программирования ПЛИС.

Общий недостаток известных подходов состоит в том, что все они ориентированы на пользователей с высокой квалификацией, имеющих профессиональные навыки в программировании.

Целью данного исследования является повышение безопасности систем управления объектами критического применения путем создания безопасных ПЛИС-контроллеров с параллельной архитектурой и информационной технологии проектирования для них программного обеспечения.

Концепция, положенная в основу исследований, и учитывающая упомянутые выше стратегии совершенствования методов программирования, формулируется следующим образом:

Поиск эффективных решений по созданию систем автоматизированного управления объектами критического применения следует искать на пересечении подходов, которые будем называть «от архитектуры» и «от первичных форм описания», подразумевая архитектуру логических управляющих автоматов и первичные слабоформализованные формы описания алгоритмов управления технологическими процессами.

2. Синтез БЛП-автоматов

БЛП-автоматы - это безопасные логические автоматы параллельного действия, защищенные от опасных искажений входных, внутренних и выходных сигналов за счет применения резервирования, динамического кодирования входных и выходных состояний и использования методов многократного контроля правильности реализации алгоритмов.

Разработаны БЛП-автоматы Мили и Мура, получившие эти названия в силу традиции различать автоматы, в которых выходные состояния зависят или не зависят от входных; БЛП-автоматы М- и Р-типа, которые отличаются способом выбора безопасных состояний; а также БЛП-цикломаты, настроенные на реализацию циклических алгоритмов.

Метод задания БЛП-автоматов предполагает описание всех его компонентов: Z, C, D, E, F, G, H, W, φ, ω, δ, χ, λ, ψ в табличном или графическом виде, причем для задания функций δ и λ могут использоваться те же методы, которые применяются для задания соответствующих функций традиционных конечных автоматов. Таким образом, метод описания компонентов БЛП-автомата сводится к описанию функций δ и λ традиционного автомата, а также функций:

– φ – преобразования состояния $z \in Z$ с временными признаками в состояние $c \in C$, где в качестве признака используются логические уровни сигналов (задается в соответствии с условиями временного кодирования входных сигналов);

– ψ – преобразования состояния $g \in G$, где в качестве признака используются логические уровни сигналов, в состояние $w \in W$ с временными признаками (задается в соответствии с условиями временного кодирования выходных сигналов);

– ω и χ – преобразования внутренних состояний (задаются в соответствии с условиями, определяющими безопасность функционирования БЛП-автомата).

В результате синтеза БЛП-автоматов получены их HDL-модели, которые могут использоваться разработчиками, как готовые программные компоненты (мегафункции), настраиваемые на реализацию различных алгоритмов управления ОКП.

3. Язык и технология программирования безопасных ПЛИС-контроллеров

Исходя из указанного выше общего недостатка существующих методов и средств программирования ПЛИС, связанного с их ориентацией на профессиональных пользователей, предложена концепция разработки языка и технологии программирования безопасных ПЛИС-контроллеров, которая основана

на трех положениях: простота и наглядность; психологическая естественность; минимум конструкций и элементов.

Как показал анализ разработанных моделей БЛП-автоматов, широкий класс цифровых устройств для управления ОКП может быть реализован с использованием всего трех конструкций: логический преобразователь, блок переходов и блок микроциклов. Для описания этих блок-операторов могут использоваться таблицы определенной формы. Именно эти три блок-оператора и соответствующие им таблицы легли в основу создания языка программирования ПЛИС-контроллеров, поскольку им одновременно свойственны и типичные конструкции, применяемые при реализации цифровых устройств на ПЛИС, и удобные, естественные формы представления алгоритмов логического управления. Таким образом, они составляют точку пересечения подходов «от архитектуры» и «от первичных форм описания», которые были обозначены в базовой концепции данных исследований.

Язык получил название THDL – Table Hardware Design Language. Он может эффективно использоваться наряду с известными языками описания аппаратуры, такими как AHDL, VHDL и другими. Программа на языке THDL представляет собой таблицу или набор таблиц определенной формы, табличных конструкций всего 4. Первая из них – таблица логических преобразований. В ней выделены ячейки для задания наименования компонента, если компонент параметризируемый, то вводится описание соответствующих параметров, имеется возможность установки приоритетности проверки условий и поля для заполнения состояний входных и выходных сигналов. В таблице переходов, описывающей компоненты с памятью, имеется возможность указания периода и кратности проверки правильности реализации алгоритмов. Таблица микроциклов описывает циклические алгоритмы. Таблица соединений используется при иерархическом описании проектов, содержащих несколько компонентов.

Язык THDL относится к классу языков с ограниченной варьируемостью. Использование языков с ограниченной варьируемостью является одним из методов повышения безопасности ПО. При этом считается, что уменьшение свобод разработчика влияет на вероятность внесения им ошибки в программный код.

Ограничение варьируемости в языке THDL достигается за счет того, что некоторые элементы цифровых устройств заранее определены: сигнал синхронизации всегда один для данного устройства и всегда подается на вход clk примитивов триггеров; в качестве примитивов триггеров всегда используется DFF – D-триггер с одним входом синхронизации, одним информационным входом и одним информационным выходом, входы асинхронного сброса и установки игнорируются.

Эти ограничения позволяют пользователю не углубляться в детали реализации элементов памяти и воспринимать их не как отдельные компоненты устройства, а как внутренние переменные, кодирующие некоторые состояния. Усилия разработчика сосредотачиваются на описании правил управления состояниями; нет необходимости удерживать в сознании связи между отдельными компонентами, обеспечивающими хранение информации, и заботиться о корректном построении триггерных схем с учетом рекомендаций производителей ПЛИС.

Разработанная процедура проектирования ПО для безопасных ПЛИС-контроллеров предполагает использование как стандартных средств, так и специальных, к которым относятся редактор для ввода табличного описания устройства на языке THDL Table editor, редактор настройки функций обеспечения безопасности Safe-providing Editor, редактор настройки параметров интерфейса Interface Editor и автоматический транслятор в HDL-код.

4. Модели и методы безопасного формирования выходных управляющих воздействий для ОКП

Как показывает практика, задача безопасного сопряжения микроэлектронных структур с исполнительными механизмами зачастую становится одной из наиболее сложных при построении систем управления ОКП. В данном исследовании предложены модели и методы формирования гармонических сигналов, которые, в отличие от известных, основаны на последовательном преобразовании параметров сигналов, динамически меняющихся во времени. Например, фаза сигнала может быть преобразована в амплитуду, амплитуда – в скважность и т.д. Рассмотрим пример реализации предлагаемого подхода, в котором фаза сигнала φ преобразуется в скважность s, а скважность – в амплитуду A.

Устройство содержит два генератора, которые формируют ВЧ-сигналы с близкими частотами, поступающими на преобразователь, реализующий логическую функцию «исключающее ИЛИ», обеспечивая таким образом преобразование одного параметра в другой: сдвига фазы между сигналами в скважность (рис. 1). Нагружая выходной сигнал с переменной скважностью на фильтр высоких частот, получаем результирующий гармонический низкочастотный сигнал g.

Исследование модели устройства показало, что форма выходного сигнала зависит от скважности

ВЧ-сигналов p_{11} и p_{12}, формируемых генераторами. Так, при скважности 50 %, форма выходного сигнала является треугольной и имеет коэффициент нелинейных искажений около 12 %. Для снижения коэффициента искажений достаточно уменьшить скважность одного из ВЧ-сигналов, тогда форма выходного сигнала становится трапецеидальной.

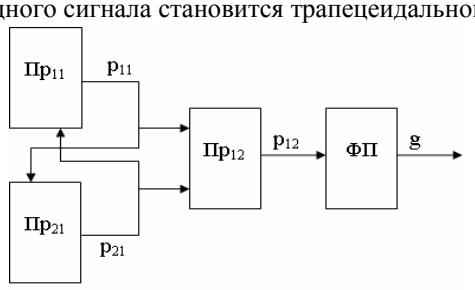

Рис. 1. Структурная схема устройства безопасного формирования гармонических сигналов с последовательным преобразованием параметров $\varphi \rightarrow s \rightarrow A$

Получена зависимость коэффициента нелинейных искажений Ku от скважности ВЧ-сигналов, исследование её на экстремум позволило определить оптимальное значение скважности s одного из ВЧ-сигналов, которое составляет примерно 34 %. В этом случае Ku не превышает 5 %. Разработана и исследована модель для безопасного трехфазного генератора и методика расчета её параметров и HDL-модель устройства управления стрелочным электроприводом на основе безопасного трехфазного генератора, причем описание модели выполнено на предложенном языке THDL. При этом проявились явные преимущества в компактности и наглядности данного языка по сравнению с традиционными.

5. Оценка эффективности выполненных исследований

При оценке эффективности исследований выполнена сравнительная оценка безопасности ПО, реализованного на разработанном языке THDL и на стандартных языках описания аппаратуры (на примере AHDL), а также функциональной безопасности устройств формирования управляющих воздействий для ОКП (разработанных и известных).

Безопасность, как известно, может быть оценена косвенно, через сложность ПО. В связи с этим, сравнительная оценка безопасности ПО, разработанного на THDL и традиционных языках описания аппаратуры, может быть выполнена путем сопоставления сложности программ.

В качестве базовой используется метрика количества ошибок в программе B, предложенная Холстедом. Получены расчетные и экспериментальные значения метрики B для некоторых типовых задач различной сложности. Предложен метод оценки снижения количества ошибок в программе при использовании языка THDL как альтернативы известным текстовым языкам описания аппаратуры. Установлено, что применение языка THDL позволят снизить количество ошибок в программе в 2-5 раз. При расчете функциональной безопасности устройств формирования управляющих воздействий для ОКП получена зависимость интенсивности восстановлений μ от интенсивности отказов устройств формирования управляющего сигнала λ_a и контрольных средств $\lambda_к$ $\mu = f(\lambda_a, \lambda_к)$, определяющая область эффективного использования разработанного метода (рис. 2).

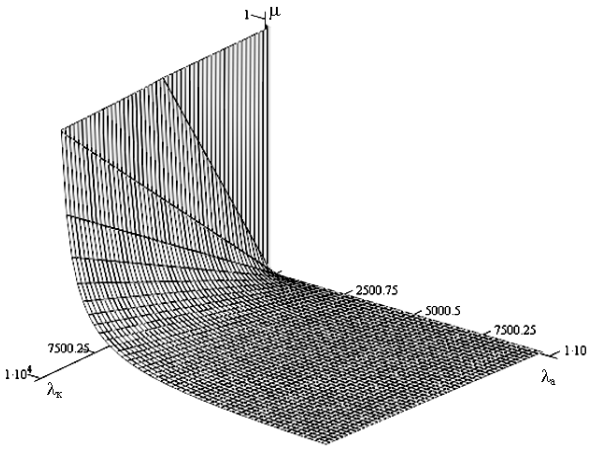

Рис. 2. Зависимость $\mu = f(\lambda_a, \lambda_к)$, определяющая область эффективного использования разработанного метода

Выводы

В работе выполнено теоретическое обобщение и получено новое решение проблемы, которая состоит в повышении безопасности управления ОКП.

Основные результаты работы:

1. Впервые предложена совокупность математических моделей и методов синтеза и описания компонентов безопасных логических автоматов параллельного действия (БЛП-автоматов), что позволяет формализовать процесс разработки цифровых устройств для управления ОКП на основе ПЛИС-контроллеров.

2. Предложен язык и технология программирования безопасных ПЛИС-контроллеров с параллельной архитектурой, которые позволяют повысить безопасность и надежность программного обеспечения и сократить долевое участие профессиональных программистов при подготовке программ путем использования упрощенных табличных

конструкций для описания алгоритмов, настройки функций обеспечения безопасности и кодирования входных и выходных сигналов.

3. Получили дальнейшее развитие методы безопасного формирования выходных управляющих воздействий за счет использования принципа последовательного преобразования параметров сигналов, динамически изменяющихся во времени.

4. Впервые предложены математические и HDL-модели генераторов гармонических сигналов, которые, в отличие от известных, осуществляют формирование ШИМ-сигнала за счет применения логической операции «неэквивалентности» для двух сигналов с близкими частотами и исключают таким образом опасные управляющие воздействия при наличии отказов.

5. Усовершенствован метод метрической оценки сложности HDL-описаний цифровых устройств, который, в отличие от известных, учитывает возможности использования готовых программных компонентов и иерархический принцип разработки ПО.

6. Метрическая оценка и экспериментальные исследования показали, что применение языка THDL в качестве альтернативы известным языкам описания аппаратуры позволят снизить количество ошибок в программе в 2-5 раз.

7. Получена зависимость $\mu = f(\lambda_а, \lambda_к)$, определяющая область эффективного использования разработанного метода безопасного формирования гармонического сигнала для управления ОКП.

Литература

1. Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В. В. Сапожников, Вл. В. Сапожников, Х. А. Христов, Д. В. Гавзов; Под ред. Вл. В. Сапожникова. – М.: Транспорт. 1995. – 272 с.

2. . Отказобезопасные информационно-управляющие системы на программируемой логике / Е.С. Бахмач, А.Д. Герасименко, В.А. Головир, А.А. Сиора, В.В. Скляр, В.И. Токарев, В.С. Харченко. – Харьков-Кировоград: НАУ „ХАИ”, НПП „Радий”, 2008. – 380 с.

3. М. С. Долинский. Обзор современных подходов и средств к "программистской" разработке аппаратного обеспечения алгоритмически сложных цифровых систем / Долинский М. С. – [Электронный ресурс]. – Режим доступа: http://www.kit-e.ru/articles/cad/2004_1_120.php.

Поступила в редакцию 28.01.2009

Рецензент: д-р техн. наук, проф., зав. кафедрой компьютерных систем и сетей В. С. Харченко, Национальный аэрокосмический университет "ХАИ", Харьков, Украина.

МОДЕЛІ ТА МЕТОДИ КЕРУВАННЯ ОБ'ЄКТАМИ КРИТИЧНОГО ЗАСТОСУВАННЯ НА ОСНОВІ БЕЗПЕЧНИХ ПЛІС-КОНТРОЛЕРІВ З ПАРАЛЕЛЬНОЮ АРХІТЕКТУРОЮ

М.Л. Малиновський

Розроблені: моделі та методи синтезу безпечних логічних автоматів паралельної дії (БЛП-автоматів) для ПЛІС-контролерів, які захищені від небезпечних перетворень вхідних, внутрішніх і вихідних станів за рахунок застосування резервування, динамічного кодування інформації та використання методів багаторазового контролю правильності реалізації алгоритмів; таблична мова THDL і технологія програмування безпечних ПЛІС-контролерів; методи і засоби безпечного формування керуючих впливів для об'єктів критичного застосування, у яких використовується принцип послідовного перетворення параметрів сигналів, що динамічно змінюються у часі.

Ключові слова: ПЛІС-контролер, БЛП-автомат, таблична мова THDL, об'єкти критичного застосування, функціональна безпека, безпечний генератор гармонічних сигналів.

MODELS AND METHODS OF CRITICAL APPLICATION OBJECTS CONTROL ON THE BASIS OF SAFE PLD-CONTROLLERS WITH PARALLEL ARCHITECTURE

M.L. Malinovsky

The models and methods of synthesis of safe logic parallel automatic devices (SLP-devices) for PLD-controllers, which are protected from dangerous distortions of entrance, input and output states at the expense of application of reservation, dynamic coding of the information and use of methods of the repeated control of correctness of algorithms realization; tabulared language THDL and technology of programming of safe PLD-controllers; methods and means of safe formation of control influences for objects of critical application, in which the principle of consecutive transformation of parameters of signals dynamically varied in time is used are developed.

Key words: PLD-controller, SLP-device, tabulared language THDL, objects of critical application, functional safety, safe generator of harmonical signals.

Малиновский Михаил Леонидович – канд. техн. наук, доцент, докторант, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков, Украина, e-mail: w8l8w@mail.ru.