МЕТОД МНОГОУРОВНЕГО ВНЕДРЕНИЯ ИНФОРМАЦИИ В ИСХОДНЫЕ ТЕКСТЫ ПРОЕКТОВ ЦИФРОВЫХ УСТРОЙСТВ С МИКРОПРОГРАММНЫМ УПРАВЛЕНИЕМ

Брель А. В.
Кафедра ПОИТ, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: alexandervbrel@gmail.com

Эта статья описывает метод многоуровнего внедрения информации в исходные тексты проектов цифровых устройств с микропрограммным управлением, а такаже автоматизацию этого метода с помощью прикладного программного средства.

Введение

За прошедшее десятилетие стоимость производства интегральных микросхем кардинально снизилась. Для снижения трудозатрат на разработку цифровых устройств в цифровом проектировании начал активно применяться модульный подход к разработке и повторное использование компонентов. Модульные компоненты цифровых устройств получили название блоков интеллектуальной собственности в разработке цифрового аппаратного обеспечения(Intellectual Property blocks, IP blocks).

Постепенно возник рынок IP blocks. Проекты цифровых компонентов устройств теперь не могли находится только в защищённом окружении, так как сама бизнес–модель требовала их продажу третьим сторонам. После продажи эти компоненты могут быть использованы с нарушением авторских прав, например перепроданы или использованы в других, не лицензированных продуктах. В настоящее время для подтверждение авторских права, а также для подтверждения прав на использование IP blocks в цифровом проектировании широко применяется технология внедрения «водяных знаков» и «отпечатков пальцев» [1].

I. Описание проблемы и постановка задачи

Цифровые устройства с микропрограммным управлением представляют собой устройства, вырабатывающие последовательности сигналов, необходимых для достижение результата путём реализации микропрограммы.

Основными задачами при разработке данного метода были: возможность использование с другими методами внедрения информации, наименьшее воздействие на исходное описание устройства, простота извлечения данных на всех уровнях разработки устройства.

Данный метод предлагает использовать каждый из компонентов цифрового устройства с микропрограммным управлением и микропрограммный код для внедрения информации, как отдельно так и в комплексе.

II. Внедрение информации с использованием избыточности микропрограммного кода

Микропрограммное управление подразумевает наличие набора команд и соответствующего формата инструкций. Длина инструкции зависит от реализуемой устройством архитектуры и обрабатываемых данных. В силу специфики реализуемых в инструкции операций, не все её разряды могу быть использованы устройством управления.

Рассмотрим формат, операции INC, которая инкрементирует регистр в архитектуре с 4 адресуемыми регистрами с длиной команды 8: 3 старших бита отводятся для кода операции, затем два бита отводятся для обозначения инкрементируемого регистра. Остальные же три бита никак не задействованы. Эти биты могут быть использованы для внедрения части информации.

Избыточность кода присуща практически любым архитектурам микропрограммного управления и позволяет внедрять достаточные для доказательства авторских прав данные. Средняя избыточность и некоторые другие характеристики набора инструкций различных модификаций микроконтроллеров PIC сопоставлены в таблице 1 [2,3,4].

Таблица 1 – Средняя избыточность набора инструкций микроконтроллеров семейства PIC

Модель	Кол–во инструкций	Длина инструкции	Средняя Избыточность
PIC16F87X	35	14	3 %
PIC17CXXX	60	16	1.1 %
PIC16C672A	35	14	1.6 %

Данный тип внедрения информации в микропрограммный код легко поддаётся автоматизации. Для внедрения данных необходимо задать формат и описание команд, информацию для внедрения и начальную микропрограмму. Результатом работы этого этапа внедрения яв-

ляется микропрограмма с внедрённой на уровне инструкций информацией.

III. Внедрение в микрокод неиспользуемых инструкций

В большинстве наборов команд устройств с микропрограммным управлением имеются команды условных и безусловных переходов. Это означает, что часть микропрограммы может быть не исполнена и даже не прочитана из ПЗУ при определённых условиях. Используя это свойство, можно осуществить внедрение информации в микропрограмму добавлением в программу не исполняемых участков, ограниченных безусловным(или контролируемым условным) переходами.

Очевидным плюсом такого подхода является то, что таким образом можно внедрить практически неограниченное количество данных, но отрицательной стороной подхода является то, что он увеличивает требования по объёму ПЗУ для устройства.

Для автоматизации данного подхода предлагается выбрать место внедрения, ввести инструкции кода подготовки перехода, инструкцию перехода, а также инструкции восстановления состояния после перехода и данные для внедрения. Программное средство отредактирует микропрограмму с учётом введённых данных.

IV. Внедрение в ПЗУ микрокода на уровне LUT

Для реализации комбинационных схем на FPGA используются LUT–блоки, которые по своей сути являются аппаратными реализациями таблицу истинности логических функций, описанных в текстовых HDL–описаниях. В составе CLB–блоков FPGA имеется возможность использовать блоки с различным числом входов от 1 до n. При реализации с помощью одного такого LUT–блока функции с меньшим числом аргументов, чем число его входов, часть ресурсов этого блока остается невостребованной, и нет возможности эти ресурсы применить для других функций. Таким образом, эти незадействованные ресурсы LUT–блока могут быть использованы для сохранения водяного знака [5]. Кроме того на большинстве FPGA архитектур LUT имеют 4,6 входов. После мэппинга на такие LUT часть их входов может не использоваться, а значит эти входы можно использовать для считывания внедрённой информации в неиспользуемую часть LUT [6].

V. Внедрение информации в цифровой автомат устройства управления

Блок управления устройства с микропрограммным управлением содержит в себе цифровой автомат. Внедрение водяного знака в цифровой автомат возможно изменением его поведения при считывании водяного знака. Каждый цифровой автомат имеет в своём строении ROM–память, поэтому к нему применим метод внедрения на уровне LUT–блоков, приведённый в предыдущей части [5]. Также для внедрения информации в цифровой автомат может быть использована техника расширения цифрового автомата [7].

VI. Прочие возможности внедрения информации

Каждое устройство с микропрограммным управление обладает набором регистров для хранения промежуточных результатов, а также состоянии. Эти регистры имеют начальное состояние, которое устанавливается по сигналу сброса(RESET). Значение этого начального состояния может использоваться как водяной знак.

Частью некоторых устройств с микропрограммным управлением является устройство самодиагностики. Например, диагностика ПЗУ кода может представлять собой подсчёт контрольной суммы от данных в устройстве. Для инициализации подсчёта контрольной суммы обычно необходимо начальное значение, которое записывается в устройство и может рассматриваться как водяной знак.

VII. Список литературы

1. John, L. Signature hiding techniques for FPGA intellectual property protection. /L. John, H. M. William, P. Miodrag. In proceedings of ICCAD International Conference on Computer-Aided Design, California, USA, –1998 –P. 186.
2. Official datasheet for PIC16F87X [Electronic resource] / Microchip Technology Inc. –West Chandler Blvd. Chandler, 1998-2013. – Mode of access: microchip.com/downloads/en/DeviceDoc/30292D.pdf – Date of access: 10.09.2013.
3. Official datasheet for PIC17CXXX [Electronic resource] / Microchip Technology Inc. –West Chandler Blvd. Chandler, 1998-2013. – Mode of access: microchip.com/downloads/en/DeviceDoc/30289C.pdf. – Date of access: 10.09.2013.
4. Official datasheet for PIC16C62B/72A [Electronic resource] / Microchip Technology Inc. –West Chandler Blvd. Chandler, 1998-2013. – Mode of access: microchip.com/downloads/en/DeviceDoc/35008C.pdf. – Date of access: 10.09.2013.
5. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем /А. А.Иванюк //Издательство Бестпринт, 2012. – С. 262–265.
6. Teich, J. Verifying the Authorship of Embedded IP Cores: Watermarking and Core Identfication Techniques /J. Teich, D. Ziener. PROCEEDINGS OF THE 2011 INTERNATIONAL CONFERENCE ON ENGINEERING OF RECONFIGURABLE SYSTEMS AND ALGORITHMS, –2011, –P. 98.
7. Amr Talaat Abdel-Hamid. Watermarking techniques for intellectual property protection in SOC designs / Amr Talaat Abdel-Hamid // Concordia University (Canada) – 2006., – P. 17–18.