УДК 681.3.06

В.В. Скляр[1], А.А. Резуненко[1], О.Н. Одарущенко[1], А.С. Гудзь[2], С.С. Щербаченко[2], А.А. Сенаторов[2], Е.Д. Вовк[2]

[1] *НПП «Радий», Украина*
[2] *Полтавский национальный технический университет имени Юрия Кондратюка, Украина*

ОБЕСПЕЧЕНИЕ ТЕСТОВОГО ПОКРЫТИЯ ДЛЯ ЭЛЕКТРОННЫХ ПРОЕКТОВ FPGA ПРИ ОЦЕНИВАНИИ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ ПО КРИТЕРИЯМ SIL3

Рассмотрены вопросы верификации электронных проектов для FPGA при оценивании функциональной безопасности по критериям SIL3. Предложен подход к обеспечению тестового покрытия для цифрового аппарата с памятью, основанный на формальной модели утверждений и направленный на уменьшение количества входных тестовых комбинаций. Также разработан способ автоматизированного формирования верификационных отчетов с целью сокращения времени тестирования и увеличения точности результатов.

Ключевые слова: *верификация, тестовое покрытие, функциональная безопасность, критерии безопасности.*

Введение

В современных системах технических комплексов критического применения (ТККП) сегодня активно применяются функционально сложные сверх большие интегральные схемы (СБИС). Среди множества различных СБИС наиболее перспективными с точки зрения быстродействия, перепрограммируемости и большого количества линий ввода-вывода являются программируемые логические интегральные схемы (field-programmable gate array – FPGA) [1, 2]. Одним из средств автоматизации проектирования цифровых систем с использованием FPGA фирмы Altera выступает система Quartus II. Файл проекта в этом случае строится с использованием языка описания аппаратуры HDL (Hardware Description Language) [1 – 3]. Примерами языков описания аппаратуры являются VHDL и Verilog.

Платой за гибкость и универсальность проектов на базе FPGA является их постоянное усложнение. Сложность создаваемых систем приводит к появлению логических и других ошибок на различных этапах проектирования. Анализ статистических данных позволяет говорить о том, что до 70% ошибок возникает на начальных этапах проектирования, при этом на этапе отладки готового изделия удается устранить только лишь около 70% ранее внесенных ошибок [4, 5]. Позднее выявления ошибок влечет за собой финансовые и временные потери для компаний-разработчиков.

Именно поэтому вопросы верификации электронных проектов очень актуальны.

Функциональное тестирование является неотъемлемой частью верификации сложных электронных проектов [6]. На этой стадии процесса симулируется поведение автомата или комбинационной схемы и проверяется на соответствие требованиям, описанным в функциональной спецификации электронного проекта FPGA.

Одной из метрик функционального тестирования есть тестовое покрытие. Тестовое покрытие рассматривается в двух основных аспектах: как покрытие требований и как кодовое покрытие (т.е. покрытие компонентов кода).

Если рассматривать тестирование как проверку соответствия между реальным и ожидаемым поведением автомата или комбинационной схемы, которая осуществляется при конечном наборе тестов, то именно это множество тестов и будет определять тестовое покрытие. Чем выше полнота тестового покрытия, тем больше тестов будет выбрано для проверки тестируемых требований и кода.

Важность и необходимость процессов тестирования ТККП, созданных с использованием FPGA, подчеркивается в третьей части стандарта IEC 61508-3:2010 [7]. Стандарт предлагает осуществлять проектирование платформы ТККП на основе требований к функциональной безопасности (ФБ). Вместо того, чтобы проектировать систему "настолько хорошо, насколько это возможно", а затем считать ее достаточно безопасной, стандарт предлагает подход, основанный на анализе рисков [6, 8].

Стандарт подразделяет меры по снижению риска на два компонента:

– требования к интегрированности безопасности (Safety integrity requirements);

– функциональные требования (Functional requirements).

В качестве критериев интегрированности безопасности в IEC 61508 вводится понятие уровней интегрированности безопасности (Safety Integrity Level – SIL). В зависимости от степени влияния ТККП на здоровье людей и окружающую среду, устанавливаются уровни SIL (от SIL1 до SIL4). Например, систе-

мы безопасности АЭС относятся к SIL3. Для квалификации компонентов систем управления ТККП на соответствия уровням SIL для таких компонентов устанавливаются требования к продукту (показатели надежности) и требования к процессам разработки [7].

В данной статье рассматривается подход к обеспечению тестового покрытия для проектов на базе FPGA при оценивании ФБ по критериям SIL3. Согласно стандарту IEC 61508 для SIL3 показатель тестового покрытия должен быть больше чем 99%.

Постановка задачи исследования. Существует два подхода к обеспечению тестового покрытия:

1. Обеспечение покрытия требований – это покрытие тестами функциональных и диагностических требований к автомату или комбинационной схеме путем построения матриц трассировки (тестирование «черного ящика» [7]).

2. Обеспечение покрытия кода тестами, отслеживает непроверенные в процессе тестирования части кода (тестирование «белого ящика» [7]).

Для решения задачи обеспечения тестового покрытия требований в проектах на базе FPGA с использованием языков HDL следует сначала составить тестбенчи (testbenches). Тестбенч – это спецификация в HDL, которая играет роль замкнутой среды моделирования для анализируемой системы. Иными словами, тестбенч служит средой для проведения тестирования отдельного цифрового автомата или комбинационной схемы.

Созданный тестбенч должен ответить на два вопроса: «Это работает согласно установленным требованиям?» и «Всё ли протестировано?». Ответ на первый вопрос можно получить, реализовав в тестбенче те же функции, что и в основном проекте, и, сравнивая результаты, точно определить, правильно ли работает проект. Ответ на второй вопрос получить гораздо сложнее, и он всецело зависит от таланта тестировщика. Одним из стандартных инструментов, помогающих оценить степень завершённости тестбенча, как раз и является анализ полноты покрытия требований и кода.

Существует несколько способов анализа полноты покрытия, реализованных в разных средах [9]:

- Animation of specification and design;
- Static analysis;
- Dynamic analysis and testing etc.

К сожалению, использование таких способов не всегда обеспечивает полноту тестового покрытия, тогда следует обратиться к формальным моделям оценки. Формальная модель может описываться совокупностью утверждений и может быть реализована несколькими способами. Рассмотрим пример решения данного подхода.

Основная часть

Самым простым решением обеспечения тестового покрытия цифрового автомата с памятью (ЦАсП) есть перебор всех возможных комбинаций входных сигналов. Однако полный перебор входных комбинаций *не гарантирует отсутствие ошибок!* Например, отказ может возникать *только* в случае специфического сочетания внутренних состояний и при полном заполнении входного буфера. Для проверки этого состояния потребуется сначала смоделировать заполнение буфера, а только потом предусмотреть создание необходимого сочетания внутренних состояний. Вероятность того, что подобное сочетание возникнет вследствие случайной или псевдослучайной генерации тестов, очень низкая. Чтобы возникло нужное сочетание, может потребоваться большое количество тестов.

Известные подходы требуют нахождения такой входной последовательности, которая вызовет несоответствие результатов функционирования ЦАсП результатам эталонной модели. Решение такой задачи полным перебором всех возможных входных значений может затянуться во времени, а в худшем случае – не дать результата.

Поэтому предлагается один из подходов к верификации ЦАсП (на примере блока записи/чтения микросхемы EEPROM, служащей для загрузки FPGA) с использованием ряда утверждений, направленных на сокращение количества тестовых последовательностей при обеспечении полного тестового покрытия.

Рассмотрим структуру входов и выходов схемы блока записи/чтения EEPROM (рис. 1). Входы r_1, r_2,…, r_i – управляющие сигналы, которые служат для разрешения (запрещения) изменения внутренних состояний ЦАсП. Как правило, эти сигналы одноразрядные. Сигналы DI (Data Input) и DO (Data Output) – 8-ми разрядные шины ввода и вывода данных соответственно. Сигналы *Adr* (Address) – 16-разрядные адресные шины ввода/вывода.

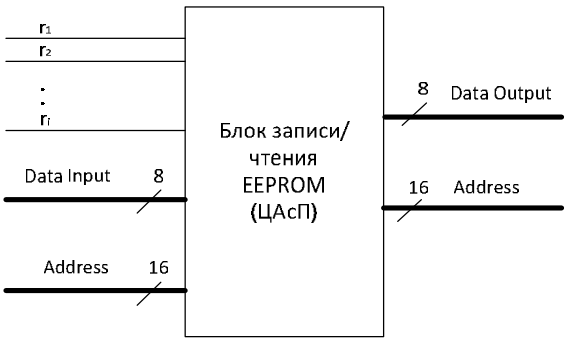

Рис. 1. Блок записи/чтения данных EEPROM для FPGA

Рассчитаем количество тестов, необходимых для верификации данного блока, путем полного перебора входных значений при 5 управляющих сигналах r. В этом случае общее количество тестов будет равно N_{gen}:

$$N_{gen} = r^5 \times DI^8 \times Adr^{16} = 2^5 \times 2^8 \times 2^{16} = 536\ 870\ 912 \text{ шт.} \quad (1)$$

Для r=8 количество тестов будет равно:

$$N_{gen}=r^8\times DI^8\times Adr^{16}=2^8\times 2^8\times 2^{16}=4\ 294\ 967\ 296 \text{ шт.} (2)$$

Итак, при 5 управляющих сигналах, 8-разрядной шине данных и 16-разрядной шине адресов общее количество тестов составит более 536 млн. штук. Если увеличить количество управляющих сигналов на 3, то N_{gen} возрастет до 4,3 млрд. штук.

Применим правила утверждений для сокращения количества входных тестовых комбинаций.

Утверждение 1.

Управляющие сигналы r_i имеют строго определенное значение и изменение любого из этих сигналов приведет к заведомо ошибочной комбинации на выходе ЦАсП. Стабильность сигналов r_i позволяет сократить количество входных комбинаций с 2^i до одной.

Утверждение 2.

Сигналы шины DI, являясь информационными, могут принимать любые значения, поэтому количество входных тестовых комбинаций останется неизменным и будет равно $DI^8=2^8$.

Утверждение 3.

Входная адресная шина *Adr* 16-разрядная (2-х байтная), она позволяет задать 2^{16} адресов EEPROM. При использовании EEPROM емкостью 2 Мбайта (2 Мбайта=2^{14} бит) с диапазоном адресов от 0×0000 до 0×3FFF, становится возможным сократить общее количество входных комбинаций на адресной шине с 2^{16} до 2^{14}.

Принимая во внимание утверждения 1 – 3, количество тестовых комбинаций при формализованном подходе будет равно N_{for}:

$$N_{gen}=r^5\times DI^8\times Adr^{14}=1^5\times 2^8\times 2^{14}=\ 4\ 194\ 304 \text{ шт.} (3)$$

Следует отметить, что N_{for} не зависит от r_i, так как управляющие входы не реконфигурируются.

Рассчитаем выигрыш рассмотренного подхода оценки тестового покрытия электронных проектов FPGA при оценивании функциональной безопасности для выражений (1) и (2). В первом случае выигрыш составит:

$$\frac{N_{gen}}{N_{for}}=\frac{536\ 870\ 912}{4\ 194\ 304}=128 \text{ раз},$$

во втором

$$\frac{N_{gen}}{N_{for}}=\frac{4\ 294\ 967\ 296}{4\ 194\ 304}=1024 \text{ раз}.$$

Соответственно в первом случае количество тестовых комбинаций уменьшится в 128 раз, а во втором в 1024 раза, что, несомненно, уменьшит время тестирования.

Несмотря на значительное уменьшение количества тестовых комбинаций, ручное тестирование остается невозможным (4 194 304 тестов!). Кроме того, в соответствии с требованиями SIL3 [8, 9] процесс верификации должен быть автоматизирован.

Задача автоматизации процесса верификации решалась следующим образом.

1. Формировалось множество входных и эталонных тестовых комбинаций. Производилась запись наборов комбинаций в текстовые файлы.

2. Подавались входные тестовые комбинации на тестируемый блок.

3. Проводилась симуляция работы тестового блока с подачей выходных и эталонных комбинаций сигналов на схему сравнения.

4. Результат побитового сравнения двух массивов записывался в отчет по верификации.

Процесс автоматизированного формирования отчета по верификации показан на рис. 2. Реализация автоматизации процесса верификации может быть осуществлена с использованием программных продуктов, например, Quartus II и ModelSim [10]. Фрагмент реализации автоматизированного подхода к верификации ЦАсП изображен на рис. 3.

Особенностью данного подхода есть то, что изменение состояния шин DI и Adr происходит тогда и только тогда, когда положительный фронт сигнала управления r_i совпадает с фронтом синхроимпульса.

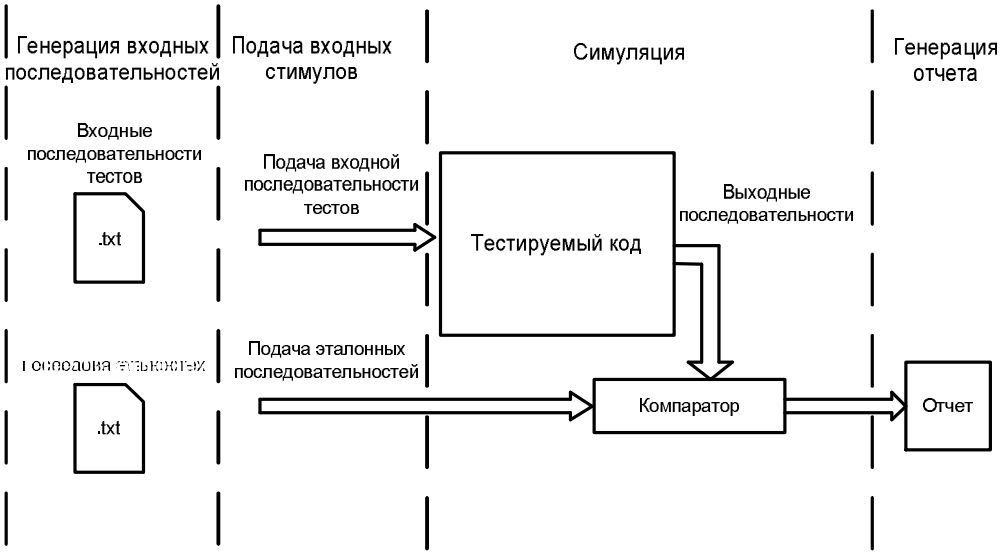

Рис. 2. Автоматизированный процесс формирования отчета по верификации

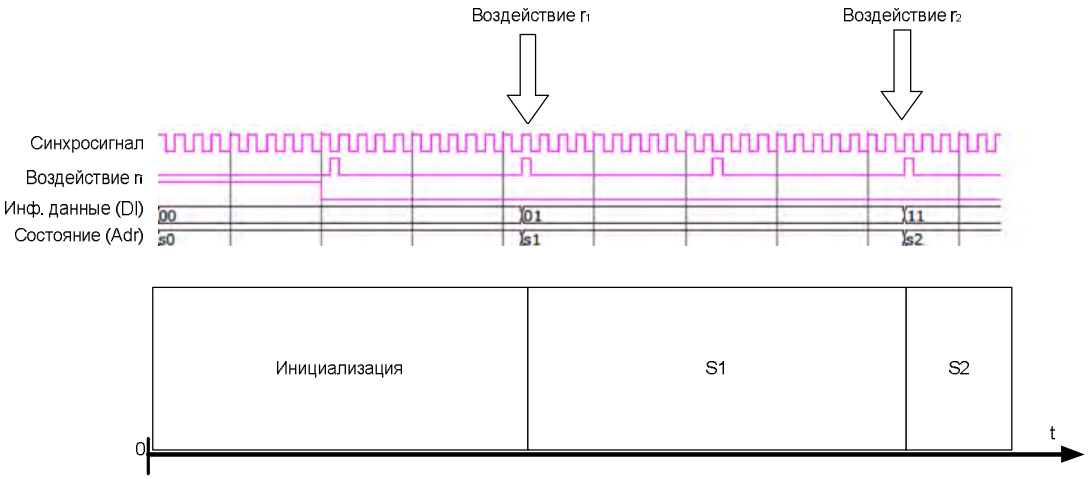

Рис. 3. Реализация автоматизированного подхода к верификации с использованием ModelSim

Заключение

В результате проведенных исследований сформулирован подход к обеспечению тестового покрытия для электронных проектов FPGA при оценке функциональной безопасности по критериям SIL3.

Использование ряда утверждений позволило сократить количество входных тестовых комбинаций, сохраняя полноту тестового покрытия.

Разработан способ автоматизированного формирования верификационных отчетов с использованием пакетов программного обеспечения Quartus II и ModelSim.

Дальнейшие исследования по усовершенствованию методов верификации цифровых автоматов с памятью целесообразно проводить по уровням покрытия кода, рассматривая их как «белый ящик».

Список литературы

1. Сергиенко А.М. VHDL для проектирования вычислительных устройств / А.М. Сергиенко. – К.: ЧП «Корнейчук», ООО «ТИД «ДС», 2003. – 208 с.

2. IEEE Standart VHDL Language Reference Manual, IEEE Std 1076-1993.

3. Бибило П.Н. Основы языка VHDL / П.Н. Бибило. – М.: СОЛОН-Р, 2002. – 224 с.

4. Липаев В.В. Обеспечение качества программных средств. Методы и стандарты / В.В. Липаев. – М.: СИНТЕГ, 2001. – 380 с.

5. Грушвицкий Р. Проектирование в условиях временных ограничений: отладка проектов / Р. Грушвицкий, М. Михайлов // Компоненты и технологии. – 2007. – №6.

6. Федоров Ю.Н. Справочник инженера по АСУТП: Проектирование и разработка. Учебно-практическое пособие / Ю.Н. Федоров. – М.: Инфра-Инженерия, 2008. – 928 с.

7. Синицын С.В. Верификация программного обеспечения. Конспект лекций / С.В. Синицын, Н.Ю. Налютин. – М.: МИФИ, 2006. – 157 с.

8. IEC 61508-3:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements.

9. IEC 61508-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures.

10. Поддержка Mentor Graphics ModelSim/QuestaSim. Volume 3: Verification / Перевод: А.В. Егоров, 2010. – 2.1-2.5 с.

Поступила в редколлегию25.04.2013

Рецензент: д-р техн. наук, проф. А.Л. Ляхов, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава.

ЗАБЕЗПЕЧЕННЯ ТЕСТОВОГО ПОКРИТТЯ ДЛЯ ЕЛЕКТРОННИХ ПРОЕКТІВ FPGA ПРИ ОЦІНЮВАННІ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ПО КРИТЕРІЯМ SIL3

В.В. Скляр, А.О. Різуненко, О.М. Одарущенко, А.С. Гудзь, С.С. Щербаченко, А.О. Сенаторов, К.Д. Вовк

Розглянуто питання верифікації електронних проектів для FPGA при оцінюванні функціональної безпеки за критеріями SIL3. Запропоновано підхід до забезпечення тестового покриття для цифрового апарату з пам'яттю, заснований на формальній моделі тверджень і спрямований на зменшення кількості вхідних тестових комбінацій. Також розроблено спосіб автоматизованого формування верифікаційних звітів з метою скорочення часу тестування і збільшення точності результатів.

Ключові слова: *верифікація, тестове покриття, функціональна безпека, критерії безпеки.*

TEST COVERAGE ASSURANCE OF FPGA DESIGN WITH FUNCTIONAL SAFETY ASSESSMENT ACCORDING TO SIL3 CRITERIA

V.V. Sklyar, A.A. Rezunenko, O.N. Odarushchenko, A.S. Gudz, S.S. Shcherbachenko, A.A. Senatorov, E.D. Vovk

Verification questions of electronic designs for FPGA are considered in case of estimation of the functional safety by criteria of SIL3. Approach to assurance of a test coverage for the digital device with the memory, based on the formal model of statements and directed on reduction of quantity of input test combinations is offered. The method of automated formation of verification reports for the purpose of abbreviation of testing time and increase in accuracy of results is also developed.

Keywords: *verification, test coverage, functional safety, safety criteria.*