УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 3, pp. 224-231

АНАЛИЗ РЕАЛИЗАЦИИ МЕТОДА РЕГИСТРАЦИИ АКТИВНОСТИ БЛОКОВ LUT В СОСТАВЕ FPGA-БАЗИРОВАННЫХ УСТРОЙСТВ

К.В. Защелкин, А.В. Дрозд

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail:const-z@te.net.ua

Рассмотрена проблема контроля целостности FPGA-базированных компонентов компьютерных систем критического применения. Отмечено, что одним из наиболее опасных видов нарушения целостности FPGA проектов является злонамеренное внедрение в проект вредоносных аппаратных закладок. Также отмечено, что вероятным сценарием является внедрение закладки в систему в моменты плановой модификации системы, т.е. тогда, когда не действует контроль целостности, основанный на применении контрольных хэш-сум. Исходя из этого, перед запуском контроля целостности необходима уверенность в том, что закладка не была внедрена в систему во время очередной плановой модификации. Рассмотрен метод, предназначенный для выявления возможных областей локализации вредоносных закладок в пространстве FPGA-базированных компонентов компьютерных систем критического применения. Метод выполняет предварительную обработку проекта с целью выявления подмножества элементарных вычислительных блоков FPGA-базированной системы – блоков LUT (Look Up Table), в которых возможно локализованы схемы закладок. Указанный метод основан на анализе активности блоков LUT. Метод позволяет получить статистику активности блоков LUT, что дает возможность анализировать изменение динамики участия этих блоков в вычислительном процессе в нормальном и аварийном режимах работы системы критического применения на характерных наборах входных слов. Метод предполагает добавление в проект дополнительной схемы регистрации активности блоков LUT. Выполнен анализ возможных способов построения указанной схемы. Предложены два базовых варианта схемы анализа активности блоков LUT. Эти варианты отличаются способом фиксации активности и сохранения зафиксированной информации во внутренней памяти схемы. Проанализированы достоинства, недостатки и ограничения вариантов реализации схемы. Выполнено сравнение предложенных схем и оценка целесообразности их использования.

Ключевые слова: FPGA, LUT, компьютерные системы критического применения, контроль целостности.

Введение

Микросхемы FPGA находят значительное применение в качестве элементной базы для построения компьютерных систем, управляющих техническими объектами повышенного риска. Компьютерные системы такого рода принято называть системами критического применения [1]. Выбор FPGA для построения систем критического применения обусловлен, во-первых, возможностью изменения функций системы путем ее перепрограммирования, во-вторых, более высокими показателями производительности, чем у микропроцессоров и микроконтроллеров [2]. Первый из указанных факторов позволяет выполнять функциональную оптимизацию системы без необходимости ее долговременного вывода из рабочего состояния. Это упрощает следующие процессы: обновления функций системы; устранения выявленных в процессе эксплуатации системы дефектов; выполнения оптимизации отдельных функций системы.

Одним из важных первичных атрибутов гарантоспособности для систем критического применения является целостность – свойство исключать непредусмотренные изменения системы и предоставляемых ею сервисов [3].

Изменения функционирования микросхем типа FPGA возможно только путем модификации их программного кода, из чего следует определение программного кода как основного носителя целостности FPGA-базированных устройств. Таким образом, контроль целостности программного кода FPGA-базированных компонентов находится в наборе наиболее существенных составляющих обеспечения гарантоспособности систем, построенных из таких компонентов.

Обзор публикаций и цель работы

Для систем критического применения одним из наиболее опасных видов нарушения целостности [4] является скрытая злонамеренная имплантация в систему аппаратных закладок (HardwareTrojans) [5]. Для FPGA-базированных систем закладки представляют собой скрытно внедренные в систему фрагменты вредоносного программного кода. Эти фрагменты создают в пространстве FPGA схему, которая обеспечивает вредоносную функцию закладки. Указанная схема может создавать искусственные неисправности в работе системы или осуществлять утечку конфиденциальной информации, обрабатываемой системой [6].

Внедрение закладки в FPGA-базированную систему может происходить как на этапе эксплуатации системы, так и на этапе ее проектирования. На этапе эксплуатации закладка имплантируется в программный код микросхемы FPGA. На этапе проектирования закладка представляет собой имплантированный в проект фрагмент высокоуровневого описания (HDL и/или схемотехнического описания), которое, в конечном итоге, транслируется в программный код.

Целостность проекта FPGA-базированной системы обычно обеспечивается путем получения хэш-сум для отдельных файлов проекта или для всего проекта целиком [7]. При этом хэш-суммы (при помощи, которых выполняется мониторинг целостности) прикрепляются к соответствующим файлам проекта или помещаются в структуру проекта. На этапе эксплуатации целостность программного кода FPGA-базированной системы может обеспечиваться либо отдельным файлом хэш-сумы, либо путем встраивания хэша непосредственно в программный код в виде цифрового водяного знака [8], [9]. Имплантация вредоносной закладки в проект (систему), находящийся под мониторингом целостности, нарушает целостность и, следовательно, приводит к обнаружению факта имплантации. Однако в процессе проектирования описание системы модифицируется. В процессе эксплуатации возможно перепрограммирование системы. Такие легальные (разрешенные) изменения требуют остановки мониторинга целостности, внесения изменений, пересчета хэш-сум и повторного запуска мониторинга. Именно в моменты времени, когда из-за выполнения разрешенных изменений системы мониторинг целостности не осуществляется, возможно внедрение закладки в систему. Таким образом, перед повторным запуском мониторинга должно быть доказано, что в период приостановки мониторинга в систему не были внесены непредусмотренные изменения (например, в виде вредоносных закладок).

Процесс выявления вредоносных закладок осложнен тем, что закладки обычно: замаскированы под аппаратные ресурсы, обеспечивающие основную функцию системы; создаются таким образом, чтобы усложнить их обнаружение в процессе тестирования системы; не проявляют себя в процессе эксплуатации системы до момента наступления события активации закладки.

В работе [10] предложен метод предварительной обработки проекта FPGA-базированной системы с целью выявления вероятных областей размещения вредоносных закладок в системах критического применения. Метод позволяет уменьшить область поиска закладки в пространстве микросхемы FPGA. Указанный метод основан на анализе активности элементарных вычислительных блоков FPGA-базированной системы – блоков LUT (LookUpTable) [11], [12]. Основные положения

метода базируются на том, что системы критического применения проектируются для функционирования в двух режимах: нормальном и аварийном. При этом компоненты систем функционируют в каждом из этих режимов на разных множествах входных слов [1]. Метод ориентирован на наиболее вероятный сценарий атаки на систему, при котором закладка проявляет себя только в аварийном режиме. В этих условиях наличие статистики активности вычислительных блоков LUT дает возможность анализировать изменение динамики участия этих блоков в вычислительном процессе, в каждом из режимов работы системы на характерных наборах входных слов. Метод предполагает добавление в проект дополнительной схемы регистрации активности блоков LUT.

Цель работы состоит в анализе возможных способов схемотехнической реализации аппаратного обеспечения указанного метода, а также формировании рекомендаций относительно целесообразности применения этих способов в зависимости от требований к условиям применения метода.

Основная часть работы

Метод, предложенный в работе [10], основан на встраивании в пространство целевой микросхемы FPGA схемы, которая регистрирует активность блоков LUT в процессе функционирования FPGA-базированной системы. Информация об активности блоков LUT может быть извлечена из схемы регистрации и использована методами последующего анализа для принятия решения о наличии или отсутствии вредоносных закладок, а также для точного выявления областей их размещения в пространстве микросхемы FPGA.

Схема регистрации активности блоков LUT состоит из одинаковых фрагментов, подключаемых к выходам анализируемых блоков LUT (рис. 1). Каждый из фрагментов состоит из двух подсхем:

- подсхемы обнаружения активности блока LUT, которая выдает на свой выход единичный сигнал только в том случае, если имеет место изменение значения на выходе анализируемого подсхемой блока LUT;
- подсхемы фиксации активности, которая фиксирует во внутренней памяти факт наличия или отсутствия изменений выходного сигнала блока LUT. Этот факт фиксируется в виде одноразрядного значения: нулевое значение соответствует отсутствию изменений выходного сигнала блока LUT, единичное – свидетельствует о том, что такое изменение имело место.

Элементы внутренней памяти подсхем фиксации образуют сдвиговый регистр, из которого считывается двоичный вектор зарегистрированных активностей блоков LUT. Каждый разряд этого вектора закреплен за конкретным блоком LUT, что позволяет локализовать активные и пассивные блоки проекта.

В работе [10] обосновываются теоретические положения метода и предлагается обобщенная структура схемы регистрации активности блоков LUT. В данной же работе предлагается два базовых варианта схемотехнической реализации данной структуры в среде FPGA. Подсхемы обнаружения активности в обоих вариантах совпадают. Эти подсхемы состоят из синхронного D-триггера и элемента суммирования по модулю два. Данные элементы подключены таким образом, что на выходе элемента суммирования по модулю два формируется логическая единица только в случае изменения значения на выходе блока LUT.

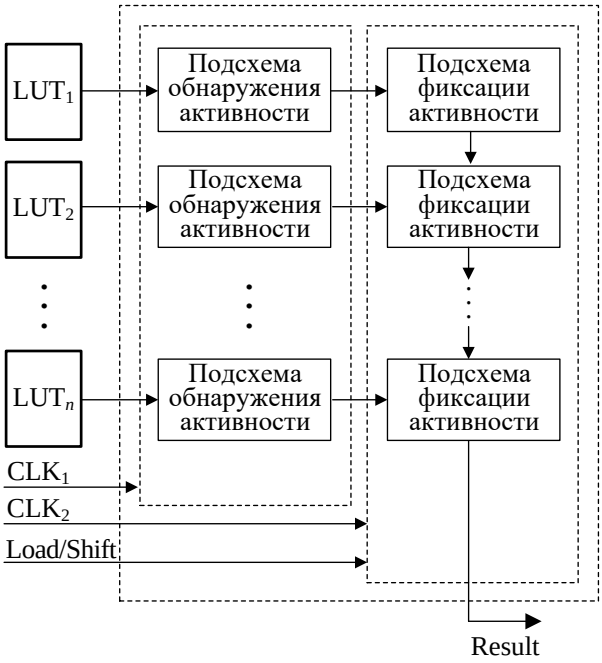

Рис. 1. Обобщенная структура схемы регистрации активности блоков LUT

Базовые варианты схем отличаются способом построения схем фиксации активности. На рис. 2 представлен базовый вариант схемы, обеспечивающий фиксацию активности блока LUT посредством входа установки синхронного D-триггера (далее – первый вариант). В случае, если имеет место изменение входного значения, на выходе элемента суммирования по модулю два возникает единичное значение, которое передается на вход установки триггера подсхемы фиксации. В результате триггер подсхемы фиксации переходит в состояние логической единицы. После этого состояние данного триггера уже не зависит от изменений значения на выходе элемента суммирования по модулю два.

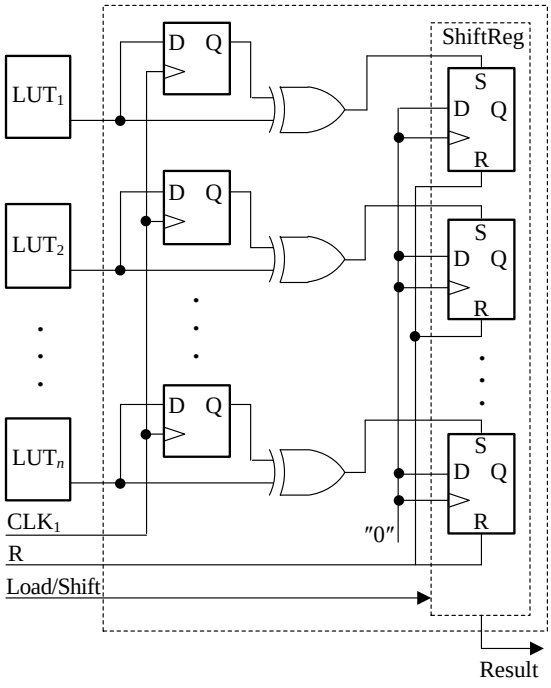

Рис. 2. Вариант схемы с обеспечением фиксации активности посредством входа установки триггера (первый вариант)

Второй базовый вариант схемы, обеспечивающий фиксацию активности блока LUT посредством информационного входа триггера подсхемы фиксации (рис. 3.). На информационном входе указанного триггера размещается элемент ИЛИ, охваченный обратной связью с выходом триггера. Такое подключение необходимо для невозможности перевести триггер в состояние логического нуля после его перехода в состояние логической единицы, которое фиксирует факт активности блока LUT.

Анализ рассмотренных базовых схем состоял в их синтезе и временном моделировании с последующим сравнением и оценкой затрат оборудования, а также результатов постсинтезного моделирования. Синтез и моделирование производились в системе проектирования IntelQuartus для целевых микросхем FPGA семейств AlteraCycloneII – CycloneIV.

Затраты оборудования в среде FPGA оценивались в виде количества элементов памяти и вычислительных блоков LUT, использованных в соответствующих синтезированных схемах. В результате синтеза схем было установлено, что количество элементов памяти для обеих схем совпадает и составляет два элемента на каждый фрагмент схемы. Количество вычислительных блоков LUT для первого (V_1) и второго варианта схемы (V_2) составляет соответственно:

$$V_1 = 2 + 5n;\ V_2 = 1 + n,$$

где n – количество фрагментов схемы.

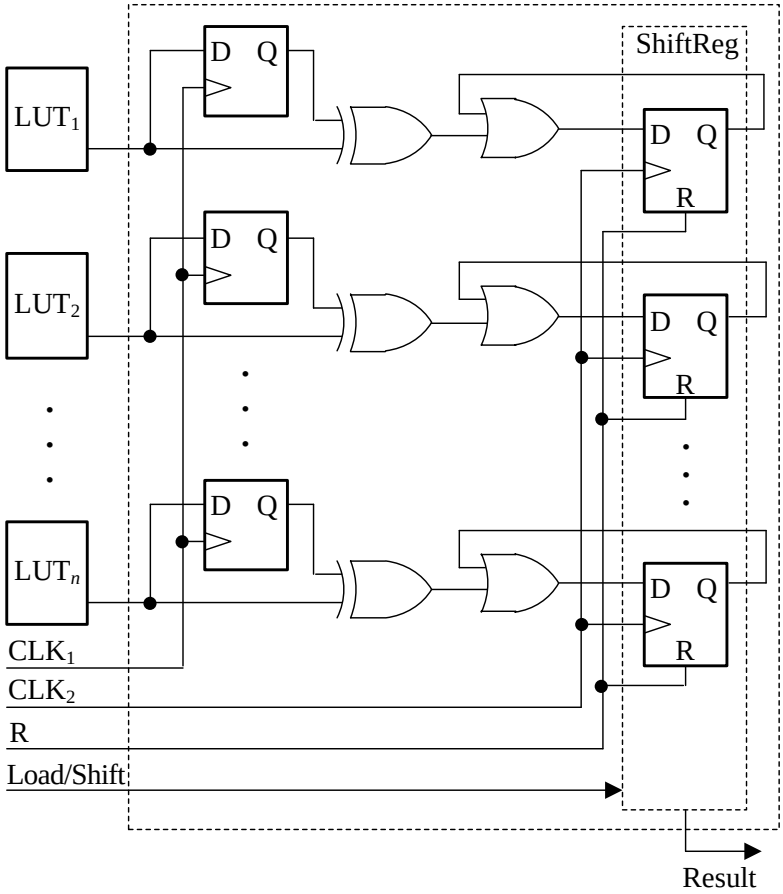

Рис. 3. Вариант схемы с обеспечением фиксации активности посредством информационного входа триггера (второй вариант)

Больший объем оборудования первого варианта схемы обусловлен спецификой реализации входа асинхронной установки триггеров в структуре микросхем FPGA.

Такой вход отсутствует в явном виде в триггерах микросхем FPGA рассматриваемых семейств. Функциональность триггера, обеспечиваемая асинхронным входом установки, искусственно реализуется через вход приема данных триггера при помощи дополнительной подсхемы, занимающей 4 блока LUT.

Однако, несмотря на указанный недостаток, первый вариант схемы имеет следующие преимущества по сравнению со вторым:

- дает возможность организовать более простую и обеспечивающую меньшую задержку конструкцию сдвигового регистра для извлечения результатов регистрации активности;
- в первом варианте схемы фиксация активности происходит асинхронно относительно функционирования подсхемы обнаружения активности. Во втором же варианте фиксация выполняется под управлением синхросигнала CLK_2, длина периода которого должна быть не больше длины регистрируемого изменения сигнала на выходе блока LUT.

Таким образом, в зависимости от требований условий применения рассмотренных схем регистрации активности блоков LUT может быть выбран один из базовых вариантов схем: вариант требующий меньших затрат оборудования (второй вариант) или вариант, не требующий тактирования подсхем фиксации активности и обладающий меньшей задержкой сдвига при получении результирующих данных (первый вариант).

Выводы

В работе выполнен анализ возможных способов схемотехнической реализации аппаратного обеспечения метода[10], предназначенного для получения информации об активности блоков LUT в FPGA-базированном устройстве. Назначение метода состоит в решении задачи предварительной обработки проекта при поиске места локализации вредоносных аппаратных закладок. Предложены два варианта схемы регистрации активности блоков LUT, отличающиеся затратами оборудования, способом фиксации обнаруженной активности и сложностью сдвигового регистра, необходимого для получения результирующих данных. Выполнено сравнение предложенных схем, а также оценка возможных областей их использования. Сформированы рекомендации относительно целесообразности применения этих вариантов схем в зависимости от требований к условиям применения метода.

Список литературы

1. Drozd, A. Checkability of the digital components in safety-critical systems: problems and solutions / A. Drozd, V. Kharchenko, S. Antoshchuk, J. Sulima, M. Drozd // IEEE East-West Design & Test Symposium. – Sevastopol, Ukraine, 2011. – Pp. 411-416.
2. Vanderbauwhede, W. High-performance computing using FPGAs / W. Vanderbauwhede, K. Benkrid. – New-York: Springer, 2016. – 774 p.
3. Kharchenko, V. Safety of information and control systems and infrastructures / V. Kharchenko, V. Sklyar, E. Brezhniev. – Palmarium Academic Publishing, 2013.
4. Zashcholkin, K. LUT-object integrity monitoring methods based on low impact embedding of digital watermark / K. Zashcholkin, O. Ivanova // Proceedings of 2018 IEEE 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 2018. – Pp. 519-523.
5. Mukhopadhyay, D. Hardware Security: Design, Threats, and Safeguards / D. Mukhopadhyay, R. Chakraborty. – Boca Raton: Chapman and CRC, 2014. – 542 p.
6. Tehranipoor, M. Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection / M. Tehranipoor, H. Salmani, X. Zhang.– Springer, 2013. – 224 p.
7. Vacca, J. Computer and information security / J. Vacca. – USA, Waltham: MK Publishers, 2013. – 1280 p.

8. Shih, F. Digital Watermarking and Steganography: Fundamentals and Techniques, 2nd edition / F. Shih. – CRC Press, 2017. – 292 p.
9. Защелкин, К.В. Метод внедрения цифровых водяных знаков в аппаратные контейнеры с LUT-ориентированной архитектурой / К.В. Защелкин, Е.Н. Иванова // Информатика и математические методы в моделировании. – Одесса, 2013. – Том. 3, № 4. – С. 369-384.
10. Zashcholkin, K. The detection method of probable areas of hardware trojans location in FPGA-based components of safety-critical systems / K. Zashcholkin, O. Drozd // Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT'2018.– Kyiv, 2018. Pp. 220-225.
11. Угрюмов, Е.П. Цифровая схемотехника. 3-е издание / Е.П. Угрюмов. – СПб.: БХВ, 2011. – 816 с.
12. Andina, J. FPGAs: Fundamentals, Advanced Features, and Applications in Industrial Electronics / J. Andina. – CRC Press, 2017. – 266 p.

АНАЛІЗ РЕАЛІЗАЦІЇ МЕТОДУ РЕЄСТРАЦІЇ АКТИВНОСТІ БЛОКІВ LUT У СКЛАДІ FPGA-БАЗОВАНИХ ПРИСТРОЇВ

К.В. Защолкін, О.В. Дрозд

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail:const-z@te.net.ua

Розглянуто проблему контролю цілісності FPGA-базованих компонентів комп'ютерних систем критичного застосування. Відзначено, що одним з найбільш небезпечних видів порушення цілісності FPGA проектів є зловмисне вбудовування в проект шкідливих апаратних закладок. Також відзначено, що вірогідним сценарієм є вбудовування закладки в систему в моменти планової модифікації системи, тобто тоді, коли не діє контроль цілісності, заснований на використанні контрольних хеш-сум. Виходячи з цього, перед запуском контролю цілісності необхідна впевненість в тому, що закладка не була вбудована в систему під час чергової планової модифікації. Розглянуто метод, призначений для виявлення можливих областей локалізації шкідливих закладок в просторі FPGA-базованих компонентів комп'ютерних систем критичного застосування. Метод виконує попередню обробку проекту з метою виявлення підмножини елементарних обчислювальних блоків FPGA-базованої системи – блоків LUT (Look Up Table), в яких можливо локалізовані схеми закладок. Зазначений метод ґрунтується на аналізі активності блоків LUT. Метод дозволяє отримати статистику активності блоків LUT, що дає можливість аналізувати зміну динаміки участі цих блоків в обчислювальному процесі, в нормальному і аварійному режимах роботи системи критичного застосування на характерних наборах вхідних слів. Метод передбачає додавання в проект додаткової схеми реєстрації активності блоків LUT. Виконано аналіз можливих способів побудови зазначеної схеми. Запропоновано два базових варіанти схеми аналізу активності блоків LUT. Ці варіанти відрізняються способом фіксації активності і збереження зафіксованої інформації у внутрішній пам'яті схеми. Проаналізовано переваги, недоліки і обмеження варіантів реалізації схеми. Виконано порівняння запропонованих схем і оцінка доцільності їх використання.

Ключові слова: FPGA, LUT, комп'ютерні системи критичного застосування, контроль цілісності.

THE ANALYSIS OF HARDWARE REALIZATION FOR ACTIVENESS REGISTRATION METHOD OF LUT UNITS INCLUDING IN FPGA-BASED DEVICES

K.V. Zashcholkin, O.V. Drozd

Odesa National Polytechnic University,
1, Shevchenko Str., Odesa, 65044, Ukraine; e-mail: const-z@te.net.ua

The problems of the FPGA-based components integrity monitoring in safety-critical computer systems are considered. One of the most dangerous types of FPGA-based system integrity violation is the Hardware Trojans implantation. It was also noted that the likely scenario is the embedding of a Hardware Trojan into the system at the moment of the planned modification of the system, i.e. when the integrity monitoring based on the hash sum usage does not operate. Based on this, before running the integrity monitoring one should ensure that Hardware Trojans were not implanted during the regular planned modification. And a method necessary to detect the probable areas of hardware Trojans location in the space of FPGA-based components of computer systems is described. The method performs the preliminary project processing on the level of elementary computational units of FPGA-based system – LUT units (Look Up Table). The goal of the method is to detect the LUT unit subsets in which the Trojans' circuits are probably located. The presented method is based on the analysis of LUT unit activeness, i.e. the registration of value changes at these units outputs. The method allows to obtain statistics of the activity of LUT units, which makes it possible to analyze the change in the dynamics of the participation of these units in the computing process, in the normal and emergency operating modes of the safety-critical system on characteristic sets of input codewords. The method offers to enter an extra circuit of LUT unit activeness registration in a project. Two basic variants of the LUT block activity analysis scheme are proposed. These variants differ in the way of fixing activity and storing the fixed information in the internal memory of the circuit. The analysis of the possible ways of entering the mentioned circuits has been performed, and the advantages, disadvantages and restrictions of different circuit variants estimated.

Keywords: LUT-oriented architecture, FPGA, Safety-Critical Systems, Integrity Monitoring.