УДК 004.67:621.3.049.77

ПРОБЛЕМЫ ЛОКАЛИЗАЦИИ ОШИБОК ПРИ ПРОЕКТИРОВАНИИ СПЕЦИАЛИЗИРОВАННЫХ БИС^{1,3}Черников Б.В., ²Можжухина А.В., ³Борисова Е.А.¹ООО «Газпром ВНИИГАЗ», Москва, e-mail: bor-cher@yandex.ru;²МИЭТ, НПК «Технологический центр», Зеленоград, e-mail: reania@rambler.ru;³РЭУ им. Г.В. Плеханова, Москва, e-mail: lb20062006@yandex.ru

В статье рассматривается проблема локализации ошибок в процессе функционально-логического моделирования на этапе разработки специализированных больших интегральных схем, а также маршрут проектирования в НПК «Технологический центр». Разработка современных микросхем – длительный, сложный и дорогостоящий процесс. Для сокращения времени и затрат на разработку и производство больших интегральных схем используются различные системы автоматизированного проектирования, которые позволяют эффективно решать различные задачи в течение всех этапов, входящих в маршрут проектирования. В ходе логического проектирования могут возникать ошибки различного характера. При их локализации без помощи вспомогательного программного обеспечения тратится значительное количество времени. В настоящее время в отечественных системах автоматизированного проектирования отсутствует подсистема локализации ошибок на этапе функционально-логического проектирования. Использование же зарубежного программного обеспечения напрямую может угрожать безопасности и качеству проектируемых микросхем. В статье представлена характеристика основных этапов вывода микросхем на рынок, в частности дана характеристика функционально-логического моделирования и, в качестве примера, описания подсистем, входящих на данный момент в состав отечественной системы автоматизированного проектирования «Ковчег». Кроме того, выделены и обоснованы основные требования к методике локализации ошибок и, в соответствии с ними, проведен анализ некоторых существующих методик в составе различных систем автоматизированного проектирования. Приводится описание основных типов аппаратных закладок, методов их активизации, примеры их встраивания в микросхемы, приведен простейший вариант аппаратной закладки. На основании проведенного анализа выбрано наиболее перспективное направление проведения работы, а также сформулированы цель и основные задачи дальнейших исследований.

Ключевые слова: функционально-логическое моделирование, большие интегральные схемы, системы автоматизированного проектирования

PROBLEMS OF ERROR LOCALIZATION DURING SPECIALIZED LSI DEVELOPING^{1,3}Chernikov B.V., ²Mozhzhukhina A.V., ³Borisova E.A.¹LLC «Gazprom VNIIGAZ», Moscow, e-mail: bor-cher@yandex.ru;²MIET, SIC «Technological Center», Zelenograd, e-mail: reania@rambler.ru;³Plekhanov Russian University of Economics, Moscow, e-mail: lb20062006@yandex.ru

The problem of localization of errors during functional logic modeling in the process of developing specialized large integrated circuits and the design route at the SIC «Technological Center» is considered in this paper. The development of modern microcircuits is a long, complicated and expensive process. To reduce the time and cost of developing and production large integrated circuits, various computer aided design systems are used that can effectively solve various problems during all the stages included in the design route. At the stage of logical design often occur errors of various kinds. Their localization without the help of auxiliary software spends a significant amount of time. Currently, domestic computer aided design systems lack the error localization subsystem at the stage of functional-logical design. The use of foreign software directly threatens the safety and quality of the designed chips. The article provides a brief overview of the general stages of introducing microcircuits to the market, in particular, the characteristic of the functional logic modeling, and, as an example, describes the subsystems that are currently part of the national computer aided design system «Kovcheg». The basic requirements for the error localization technique are also identified and substantiated, and, in accordance with them, an analysis of some existing methods for localizing errors in computer aided design systems. In addition, a description of the main types of hardware bookmarks, methods for their activation and examples of their integration into microcircuits and the simplest version of the hardware bookmark is given. Based on the analysis, the most promising direction area of work was chosen, and the goal and main tasks of further research were formulated.

Keywords: functional-logical modeling, large integrated circuits, computer-aided design systems

Сложность и степень интеграции больших интегральных схем (БИС) растет с каждым годом. Наиболее приоритетными и сложными в разработке в настоящее время являются специализированные микросхемы для датчиков различного назначения [1] и интеллектуальных сенсоров, в частности

используемых в робототехнике [2]. На настоящий момент развитие технологий по созданию таких «органов чувств» для цифровых систем является важным направлением в микроэлектронике. Такие сенсоры востребованы во многих отраслях, в том числе в медицине (глюкометры, устройства

для помощи астматикам, датчики исследования функции сердца), в различных исследованиях (космические исследования, исследования в расщелинах и впадинах Мирового океана), в обеспечении безопасности (датчики радиации, дальномеры, фотобарьеры, портативные средства обнаружения оружия, взрывчатых веществ, датчики для автопилотирования, компьютерное зрение, обработка видео и изображений, видеонаблюдение), автомобилестроение (адаптивное торможение, помощь при парковке, мониторинг препятствий и людей на пути следования транспортного средства, системы автопилотажа) и многие другие [3].

Таким образом, в настоящее время одним из приоритетных направлений в изготовлении отечественных БИС является совершенствование средств автоматизированного проектирования (САПР). Одним из факторов совершенствования считается улучшение подсистем тестирования и отладки.

По данным сайта tadviser.ru, на настоящий момент на рынке САПР присутствует в основном зарубежное программное обеспечение (ПО) от таких крупных компаний, как Autodesk, Dassault Systemes, Siemens PLM Software и других. Обращаясь к российскому рынку, многие отечественные САПР на данный момент не могут в полной мере удовлетворить все потребности в сфере разработки БИС. В качестве примера наиболее полной и доступной отечественной САПР, включающей в себя основные подсистемы проектирования современных БИС, можно привести САПР «Ковчег». В основе САПР «Ковчег» лежит маршрут проектирования БИС от НПК «Технологический центр», характеристика этапов которого рассматривается ниже. Однако отсутствие подсистемы локализации ошибок для этапа логического проектирования заставляет разработчиков обращаться к дорогостоящим зарубежным аналогам, которые могут нести в себе скрытый программный функционал, обеспечивающий внедрение вредоносной аппаратной логики или утечку информации о разрабатываемых проектах. В связи с этим чаще всего обращаются к наиболее подходящему для разработки интегральных микросхем ПО компаний Cadence, Synopsys, Aldec или Xilinx.

Таким образом, одной из проблем является отсутствие российских аналогов ПО для локализации ошибок на этапе функционально-логического моделирования (ФЛМ). Кроме того, отсутствие подсистемы локализации ошибок и исключение возможности применения зарубежного ПО при создании некоторых специализированных БИС особого назначения значительно усложняет

и замедляет процесс вывода микросхемы на рынок. Еще одной проблемой, безусловно связанной с первой, является (в связи с вынужденностью использования зарубежного ПО) вероятность встраивания в электрическую схему аппаратных закладок, утечки информации и разрабатываемых проектов. В частности, авторы работы [4] описывают скрытый метод внедрения вредоносной логики в микросхему, и как такая атака может работать на практике. В работе доказывается, что после внедрения подобных изменений в микросхему их обнаружить весьма затруднительно.

В связи с возможностью проявления подобных проблем целесообразно разработать собственную методику и построить на ее основе подсистему локализации ошибок в проектах разработки специализированных БИС.

Целью данной статьи является анализ существующих программных методик локализации ошибок в процессе разработки микросхем, а также постановка цели и задачи на последующее исследование.

Характеристика существующего маршрута проектирования

В процессе разработки БИС используется большое количество различных систем проектирования, которые обеспечивают решение широкого спектра разноплановых задач на каждом из этапов проектирования микросхем. В маршрут проектирования микросхем входят следующие этапы, предложенные НПК «Технологический центр»:

- системное проектирование – разработка системной спецификации и требований к БИС, которым должна удовлетворять будущая микросхема;

- функциональное проектирование – на базе поведенческой модели создается RTL-описание (register transfer level – уровень регистровых передач, в разработке интегральных микросхем – описание работы синхронной цифровой схемы) проектируемой микросхемы, а также проводятся его моделирование;

- логическое проектирование – генерируется структурное описание схемы, состоящее из логических вентилей и их соединений – netlist, проводится логический синтез, ФЛМ;

- физическое (топологическое) проектирование – выполняется размещение ячеек на поле БМК (базовый матричный кристалл), синтез топологии с учетом списков цепей, расчет задержек цепей топологии БИС, оценивается устойчивость проекта БИС при различных внешних воздействиях, проводится анализ влияния параметров

топологии на правильность функционирования и устойчивость проекта;

- производство БИС;
- тестирование БИС в составе пластины и в составе корпуса;
- квалификационные испытания БИС – испытания на надежность, радиационную стойкость и др.;
- испытания БИС в составе аппаратуры заказчика.

Продолжительность выполнения любого из этапов проектирования для создания даже простых микросхем может занимать от нескольких дней до нескольких месяцев, сопровождаясь на каждом этапе выполнением значительного количества контрольных операций.

В настоящий момент в рассматриваемый для примера отечественный САПР «Ковчег» входят подсистемы, приведенные на рис. 1.

Приведенные на рисунке подсистемы реализуют определенные ранее описанные этапы вывода микросхемы на рынок. Этап системного проектирования реализуется редактором схем со средствами прототипирования микросхем. Этапам функционального и логического проектирования соответствует подсистема функционально-логического моделирования. Подсистемы размещения ячеек на поле БМК, синтеза топологии, верификации, расчета задержек и топологический редактор используются на этапе топологического про-

ектирования. Подсистема аттестации проекта дает возможность оценить устойчивость полученного проекта БИС в зависимости от задаваемых параметров внешних воздействий, проанализировать влияние топологических параметров, оказываемое на правильность функционирования микросхемы. Полученная в ходе разработки микросхемы информация для изготовления БИС передается на последующие этапы производства.

ФЛМ проводится для проверки правильности функционирования микросхемы с учетом задержек функциональных ячеек и проверки на соответствие полученного после логического синтеза netlist и RTL-описания для выявления возможных логических ошибок, то есть проводится формальная верификация.

Анализ методик локализации ошибок в современных САПР

На основе анализа сведений о распространении различных САПР можно сделать вывод, что для разработки интегральных микросхем используются в основном ПО двух крупных фирм – Cadence и Synopsys. Кроме того, используются САПР таких производителей, как Aldec, Xilinx, Altera. В качестве бесплатного САПР рассматривается Icaqus. Результаты анализа методик САПР выбранных компаний на основе требований отечественных разработчиков и технологического процесса представлены в таблице.

Рис. 1. Состав САПР «Ковчег» 3.0 [5]

Характеристика методик поиска ошибок на этапе логического проектирования

Методика	Достоинства методики	Недостатки методики
Cadence NC-Verilog	– обширный набор средств и настроек для проверки модели микросхемы; – визуальное отображение схемы; – возможность раскрытия схемы от одного элемента; – возможность просматривать значение сигнала на входах и выходах в процессе моделирования	– работает под Unix-подобными системами; – освоение системы управления функциями среды занимает большое количество времени
Synopsys VCS и DVE	– возможность отображения информации о микросхеме в разных представлениях (ASCII таблица моделирования и диаграмма сигналов); – визуальное отображение схемы; – возможность отслеживать путь сигнала в схеме БИС в двух режимах – «Path» и «Design»	– совместимость с Unix-подобными системами; – просмотр только полной схемы без возможности свертки/развертки от элемента; – не содержит в себе всего необходимого спектра функций для сквозного проектирования микросхемы
Aldec Active-HDL	– возможность внесения изменений и правок в проекте в процессе моделирования и поиска ошибок; – визуальное отображение схемы; – возможность просматривать значение сигнала на входах и выходах элементов схемы в процессе моделирования	– просмотр только полной схемы без возможности свертки/развертки от элемента
Xilinx ISE	– возможность внесения изменений и правок в проект в процессе моделирования и поиска ошибок; – возможность отслеживать путь сигнала в схеме микросхемы	– визуальное отображение схемы без отображения сигнала; – просмотр только полной схемы без возможности свертки от одного элемента
Altera ModelSim	– возможность внесения изменений и правок в коде проекта в процессе моделирования и поиска ошибок; совместима с Windows	– все инструкции по работе со средой и сама среда только на английском языке; – просмотр только полной схемы без возможности свертки от одного элемента; – визуальное отображение схемы микросхемы через ПО Altera Quartus II
Icarus Verilog	– бесплатная версия	– правки осуществляются разными сторонними программистами, что ставит под угрозу данные проекта; – совместимость с Unix-подобными системами; – полностью отсутствует какое-либо графическое отображение схемы

Основными требованиями, предъявляемыми к методикам, используемым в рассмотренных САПР, можно считать следующие:

- визуализация – необходима для правильной и более быстрой локализации ошибок в проекте БИС;
- свертка и развертка схемы – требуются для обеспечения возможности убирать с выведенной части схемы ненужные элементы и связи, выводить нужные для анализа элементы во избежание излишней загроможденности на экране;
- удобство просмотра результатов моделирования – необходимо для облегчения визуального поиска ошибок в проекте БИС;
- доступность и дружелюбность ПО по отношению к пользователю;
- операционная система и др.

Анализ проблем защиты данных

Помимо двух наиболее общих способов внедрения аппаратной вредоносной логики путем внесения модификации на уровне VHDL ((Very high speed integrated circuits) Hardware Description Language) (рисунки), существует еще ряд различных вариантов. Кроме того, что такую закладку зачастую невозможно выявить на этапах разработки и производства, это сложно сделать и в процессе эксплуатации, так как вредоносная закладка может активизироваться не сразу [6].

На рис. 2 представлена схема простейшей аппаратной закладки. В такой схеме реальное значение сигнала на выходе будет получаться при неактивной закладке. В противном случае на выход микросхемы всегда будет поступать «ноль». Активация закладки

может осуществляться разными способами, например существуют образцы с внутренней и внешней активацией. Такие закладки активизируются при достижении определенных внутренних состояний или взаимодействуя с каким-либо источником во внешней среде. Такими источниками могут, например, являться антенны внешнего сигнала.

Рис. 2. Пример простейшей аппаратной закладки

В настоящее время не существует единого общего метода или комплекса методов обнаружения аппаратных закладок всех типов. Самым эффективным остается тщательный контроль всего цикла выведения микросхемы на рынок, а также использование собственных или проверенных САПР [7]. Кроме того, требуется детально проверять библиотеки элементов, используемых в основе разработки.

Помимо встраиваемой логики, существует угроза и со стороны программной части, то есть содержания самих зарубежных САПР, особенно при использовании в режиме реального времени через интернет. При открытии проектов микросхем в программной среде может происходить утечка важных частей кода, тестов и другой информации.

Данная проблема в настоящее время также решается использованием проверенного ПО или собственных разработок.

Направления последующего исследования

В настоящее время в России возрастает заинтересованность в специализированных микросхемах. В связи с этим целесообразно не только разработать надежную и проверенную отечественную методику локализации ошибок функционирования в проектах БИС, но и обеспечить наличие в ней современных, быстродействующих инструмен-

тов для снижения трудозатрат отечественных разработчиков и уменьшения времени процесса вывода микросхем на рынок.

В рамках достижения поставленных целей необходимо решить следующие задачи.

1. Проанализировать существующие методики локализации ошибок функционирования в микросхемах и алгоритмы различных вспомогательных инструментов с целью выявления наиболее затратных по времени и трудоемких.

2. Разработать методику и реализующие ее алгоритмы локализации ошибок функционирования в проекте БИС для снижения ресурсоемкости этапа логического проектирования.

3. Обосновать преимущество новой методики по сравнению с используемыми.

Выводы

1. На основании анализа преимуществ и недостатков применяемых в настоящее время методик локализации ошибок следует признать, что наиболее совершенным пока является зарубежное ПО производства Cadence и Synopsys.

2. В ходе анализа выявлено отсутствие единого метода выявления различных аппаратных закладок. Из этого следует необходимость создания унифицированного и наиболее полного инструмента для выявления закладок.

3. Сформулированы цели и задачи на последующее исследование, направленное на совершенствование методики локализации ошибок функционирования БИС.

Список литературы

1. Патрушева Т.Н. Сенсорика. Современные технологии микро- и нанoeлектроники. М.: ИНФРА-М, 2014. 260 с.
2. Михеев В.П., Просандеев А.В. Датчики и детекторы. М.: МИФИ, 2007. 172 с.
3. Войтович И., Корсунский В. Интеллектуальные сенсоры. М.: Бином, 2009. 624 с.
4. Georg T. Becker, Francesco Regazzoni, Christof Paar, Wayne P. Burleson Stealthy Dopant-Level Hardware Trojans. Cryptographic Hardware and Embedded Systems – CHES 2013. 15th International Workshop Santa Barbara, CA, USA, August 20-23, 2013 Springer, 2013. P. 197–214.
5. Гаврилов С.В., Денисов А.Н., Коняхин В.В. Система автоматизированного проектирования «Ковчег 2.1» / Под ред. Ю.А. Чаплыгина. М.: Микрон-Принт, 2001. 194 с.
6. Кузнецов Е., Сауров А. Аппаратные трояны. Ч. 2: Примеры реализации, способы внедрения и активации // Наноиндустрия. 2017. № 1. С. 12–20.
7. Кузнецов Е., Сауров А. Аппаратные трояны. Ч. 3: способы предупреждения и обнаружения // Наноиндустрия. 2017. № 1. С. 30–40.