УДК 681.32

В.А. ГОРБАЧЕВ, канд. техн. наук, М.А. ВОЛК, канд. техн. наук, С.Н. САРАНЧА

МЕТОДЫ СЕРТИФИКАЦИИ МИКРОПРОЦЕССОРНЫХ КОМПОНЕНТОВ

На современном этапе развития электронных систем все большую роль играет информация. Именно поэтому вопросам защиты информации сейчас уделяется все больше внимания.

Однако достаточно большой класс потенциальных угроз безопасности остался вне рассмотрения специалистов по защите информации – это класс аппаратно реализуемых угроз. Интенсивно развиваются методы и способы электронного терроризма – несанкционированного доступа к информации, расположенной в компьютере, с целью ее кражи, разрушения, взлома защиты и использования не по назначению.

Особенности, способствующие данному феномену:

- Компьютер, как средство сберегания, обработки и передачи информации, сделался объектом электронного терроризма;
- Стремительное развитие технологий производства ИС сделало возможным использование аппаратных закладок с большими возможностями;
- Бесконтрольные закупки импортной вычислительной и оргтехники.

Исследования показали, что наиболее вероятным местом расположения источников таких угроз (ИУ) является центральный процессор, поскольку он имеет доступ практически ко всем ресурсам персонального компьютера и может проникать под любые слои защиты систем безопасности. Способом реализации угрозы в данном случае выступают не специфицированные для данного компонента функции.

Для защиты от угроз данного типа предлагается перед установкой компонентов в ПЭВМ производить процедуру *сертификации*. Под сертификацией понимается комплекс организационно-технических мероприятий, в результате которых подтверждаются показатели и характеристики образца.

При сертификации аппаратных средств решаются такие задачи:

- оценка соответствия технических показателей аппаратуры установленным техническим нормам;
- определение уровня физических полей, возникающих при работе устройств, и степени их опасности с точки зрения появления КНСД к информации;
- наличие закладных устройств, предназначенных для снимания и передачи информации;
- обеспечение заданного уровня защищенности информации, циркулирующей в программно-аппаратной среде.

Задача сертификации средств вычислительной техники решается в рамках технической диагностики, основные функции которой как науки определяются обеспечением качества средств и эффективности их использования по назначению на этапах проектирования, производства и эксплуатации. Процесс диагностирования включает в себя два этапа:

а) проверка того, что устройство работает исправно;

б) поиск дефектов, если проверка дала негативный результат.

С точки зрения сертификации электронных средств на наличие источников угрозы необходимо выполнить такие процедуры:

а) сертификация на соответствие специфицированным функциям;

б) сертификация на наличие не специфицированных функций;

в) анализ этих функций при позитивном результате второго этапа.

С точки зрения нормального функционирования микропроцессора не специфицированная функция может рассматриваться как неисправное поведение чипа. В таком случае для поиска не специфицированных функций может быть применен весь имеющийся на сегодняшний момент аппарат диагностирования неисправностей в микропроцессорах.

Трудность диагностирования неисправностей в микропроцессорных структурах определяется следующими факторами:

–все современные микропроцессоры представляют собой интегральные схемы сверхбольшой степени интеграции, в которых нельзя наблюдать сигналы на внутренних точках системы. В то же время введение многочисленных контрольных выводов явно нерационально. Следовательно, необходимы такие тест-процедуры, при использовании которых для информации о наличии неисправностей требовались бы только нормальные вводы и выводы схемы;

–отсутствие детальной информации об объекте диагностики;

–большое число выводов и высокие частоты функционирования компонентов требуют использования специального технического обеспечения в виде комплексов диагностики.

Микропроцессор с точки зрения теории автоматов может быть рассмотрен как последовательностный автомат. Однако для последовательностных автоматов не разработано единых и универсальных методов построения и оценки качества тест-последовательностей. Это связано с тем, что, во-первых, каждый возможный проверочный вход, как правило, можно вычислять для каждого возможного состояния схемы. Таким образом каждый элемент памяти, содержащийся в схеме, удваивает объем вычислений, необходимых для отыскания теста. Во-вторых, существует проблема начальной установки. Прежде, чем мы сможем применить некоторый тест к последовательностной схеме, мы должны суметь установить ее в известное фиксированное состояние или в крайнем случае мы должны знать, в каком состоянии она находится. Это может быть сделано, если первому тесту предшествует *установочная последовательность*. Необходимо также чтобы эти процедуры были в значительной мере автоматизированными.

Рассмотрим микропроцессор как объект диагностики.

С точки зрения теории автоматов микропроцессор может быть описан как

$$Y = A(X;S;\delta;\gamma) \qquad (1)$$

где Y - множество выходов

X - множество входов

S - множество состояний

$\delta : S \times X \to S$ функция переходов

$\lambda : S \times X \to Y$ функция фыходов

Однако при таком представлении возникает проблема в представлении данных о функционировании микропроцессора в связи с высокой сложностью выполняемых им функций.

В настоящее время существует два различных подхода к процедуре построения диагностирующих последовательностей – детерминированный и стохастический. Детерминированный метод опирается на детальное знание структуры исследуемого устройства и определенный класс обнаруживаемых неисправностей. Стохастический метод может рассматривать объект диагностики как "черный ящик" с заданными функциями (в том или ином виде).

При детерминированном способе построения диагностирующей последовательности [1] предлагается модель МП — это совокупность взаимосвязанных функций, реализуемых компонентами оборудования (называемых механизмами), каждый из которых представлен частью оборудования МП с неизвестной или частично известной структурой для реализации определенной функции. Оборудование МП дифференцируется на механизмы хранения и передачи данных, управления передачей данных, обработки данных, управления обработкой. Тест МП определяется как совокупность тестов отдельных механизмов.

1. Механизм обработки данных выполняет арифметические и логические операции, модификацию операндов и результата, выработку признаков результата, операции адресной арифметики.

2. Механизм управления обработкой данных выполняет дешифрацию операций, модификацию операций, операндов, результата, активизацию операций и их модификаций.

3. Механизм хранения и передачи данных представлен совокупностью регистров и шин.

4. Механизм управления передачей данных осуществляет адресацию и выборку регистров, отрабатывает реакции на внутреннее состояние и переходы.

5. Механизм отработки реакций на внешние сигналы и управления вводом-выводом осуществляет взаимодействие с внешней средой.

Проектирование теста для МП есть процесс построения теста для каждого механизма. При этом будем считается, что неисправности одного механизма не влияют на проверку исправности .другого.

Преимуществом данного метода является его простота и универсальность, хорошая применимость для микропроцессоров с малой разрядностью регистров, малым числом регистров и небольшим набором операций.

В рамках стохастического подхода к проблеме генерации диагностирующих последовательностей [2] можно выделить метод построения тестов на основе аппарата цепей Маркова. При этом микропроцессор может представляться функциональной моделью – графом информационной связанности, структурно-функциональным графом или алгоритмическим описанием на основе регистровых передач. Такая методика позволяет обнаруживать неисправности типа "чувствительность к определенным последовательностям команд". Преимуществом такого подхода является отсутствие модели неисправности, недостатком – большая длина тест-последовательности (и, следовательно, большое время тестирования) и высокая сложность оценки результатов.

Общим недостатком вышеперечисленных методов является отсутствие в модели объекта временных характеристик и неприменимость к микропроцессорам с суперскалярной архитектурой. В то же время все современный микропроцессоры широкого применения построены именно по суперскалярной архитектуре. Рассмотренные выше методы не могут обнаруживать ошибки в устройствах, функционирующих на основе алгоритмов с нечеткой логикой (например устройство предсказания ветвлений Branch Prediction Unit или кэш-память). Однако ошибки в кэш-памяти или блоке предсказания ветвлений никак не сказываются на правильности работы микропроцессора с точки зрения выполняемых функций, поскольку данные устройства являются программно прозрачными, однако приводят к замедлению работы микропроцессора и понижению реального iCOMP индекса по сравнению с заданным.

Ввиду отсутствия априорных знаний о структуре и функционировании ИУ мы можем производить тестирование только с точки стохастического подхода. Вопросы детерминированного тестирования без модели неисправности в настоящее время только начинают рассматриваться [3], однако объектом исследования выступают комбинационные схемы, что является абсолютно неприменимо в данной ситуации.

Основными вопросами стохастического подхода являются методы моделирования объектов диагностики, методы построения тест-последовательности и методы оценки результатов тестирования.

В качестве метода описания объекта диагностики выбираем процессный метод. Преимущество данного метода заключается в том, что фактически любая современная микросхема обладает моделью, написанной на языке VHDL, где процесс является одной из основных структурных единиц. Поскольку единого определения такого понятия как процесс нет, мы под процессом понимаем аппаратно реализуемое преобразование цифровой информации. Таким образом любое цифровое устройство можно представить как совокупность параллельно протекающих процессов. Микропроцессор можно представлять на структурно-процессном уровне, когда каждому структурному блоку ставится в соответствие процесс и на функционально-процессном уровне, когда выполнению каждой команды ставится в соответствие процесс. В первом случае мы можем говорить о процессе конвейеризации, чтения-записи кэш-памяти и т.д. Во втором случае мы можем рассматривать процессы выполнения команд пересылки данных, обработки данных и управления. Таким образом процессное представление легко интегрирует в себя методы представления объекта диагностики, использующиеся как в детерминированном, так и в стохастическом методах генерации тестов.

Каждый процесс П характеризуется набором входных и выходных линий и набором внутренних состояний и фактически является автоматом (1). В множестве входных линий выделяется подмножество линий $X_a \in X$, изменение уровня сигнала на которых активизирует процесс. Данное подмножество сигналов называется списком чувствительности.

Информация передается от процесса к процессу с помощью сигналов. При этом один сигнал является выходным для одного процесса и входным для другого. Таким образом процессы формируют между собой информационные отношения типа предок-потомок. Условимся называть процесс-предок *управляющим*, если его выходные линии входят в список чувствительности процесса-потомка. В ином случае будем называть процесс-предок *информационным*.

Исходя из вышесказанного возможно построить граф информационной связанности процессов ГИСП, где вершинам будут являться процессы, а дугами – сигналы. В качестве основной вершины графа выберем процесс взаимодействия с внешней средой. Далее строим покрытие графа, активизирующее все управляющие дуги графа.

Модель для проверки процесса хранения и передачи данных представлена совокупностью регистров и связей между ними. Это определяет граф регистровых передач (ГРП), который имеет регистры-вершины $R=(R_0,..R_m)$ и две дополнительные вершины IN, OUT, отображающие внешнюю среду, $J^A=\{I_1,\ldots,I_r\}$ — множество команд пересылок и ветвлений в МП.

Модель неисправностей процесса хранения и передачи данных представлена следующими допущениями.

1. Любой разряд регистра или любая линия передачи данных может принимать константные значения 0 или 1.

2. Две любые линии передачи данных могут быть замкнуты.

3. Допускается наличие указанных неисправностей с любым числом разрядов регистров и линий передачи данных,

4. Пути передачи данных, источники и приемники информации выбираются правильно.

Таким образом допускается наличие кратных константных неисправностей и неисправностей типа "короткое замыкание" в информационных связях процессов. Построение проверяющего теста переноса должно удовлетворять условиям: для каждой пары разрядов должен существовать набор с различными значениями сигналов в этих разрядах; для каждого разряда должны существовать по крайней мере два набора с различными значениями сигналов в атом разряде. Таким образом, минимальной длины тест переноса содержит $\log_2 n+1$ наборов, где n — число разрядов.

Процедура 1 построения минимизированного теста путем составления неизбыточной совокупности путей ГРП, покрывающей все дуги, представляет собой задачу покрытия: для каждого пути выбирается кратчайшая последовательность команд, активизирующая этот путь; при этом каждому ребру пути ставится в соответствие дизъюнкция команд, помечающих это ребро; составляется некоммутативная конъюнкция дизъюнкций всех ребер пути от IN до OUT; выполняется переход от КНФ к ДНФ, раскрывая скобки с сохранением порядка конъюнкций, применяя, где это возможно, операцию поглощения; выбирается терм полученного выражения, состоящий из минимального числа команд.

Минимальные термы, активизирующие все участки выбранных путей представляют собой искомое решение, состоящее из набора команд, выполнение которых с операндами и адресами теста переноса обеспечит проверку процесса хранения и передачи данных тестируемого микропроцессора. Процедура 1 может быть адаптирована к проверке любых информационных связей между процессами.

В качестве модели для проверки процесса управления передачей данных рассматривается некоторое множество n-разрядных регистров $R=\{R_0,..,R_{m-1}\}$. Выборка регистра приемника или источника информации обеспечивается дешифрацией номера этого регистра, явно или неявно адресуемого в команде МП. Для этого применяются дешифраторы регистровых файлов, мультиплексоры, демультиплексоры.

Модель дефектов представлена неисправностью записи в регистры $R\rightarrow R_i/R\rightarrow fl(R_i)$, вместо $R\rightarrow R_i$ осуществляется запись $R\rightarrow fl(R_i)$, где $fl(R_i)$ — произвольное подмножество регистров, в том числе и пустое множество. Наличие таких неисправностей допускается для нескольких регистров R_i. Неисправность чтения $R_i\rightarrow R/f2(R_i)\rightarrow R$ определяется чтением информации в приемник R из регистров $f2(R_i)$ вместо R.

Процедура 2 позволяет находить все неисправности данного типа. Она состоит из двух фаз – прямой и обратной. В прямой фазе в каждый регистр записывается последовательно, в порядке возрастания номеров, двоичный код его номера, а затем в таком же порядке читается содержимое каждого регистра. В обратной фазе, в порядке возрастания номеров, в каждый регистр R_i (i=0,m-1) записать двоичный код m-1-i и в том же порядке выполнить чтение их содержимого.

Таким образом применяются процедура 1, процедура 2 и процедура 3 детерминированного метода. Формируются входные воздействия для процесса взаимодействия с окружающей

средой и подаются на выводы микропроцессора. Полученные реакции объекта сравниваются с результатами имитационной модели. Во многом первый этап диагностирования перекликается с задачами, выполняемыми самим микропроцессором при выполнении процедуры самотестирования BIST. Однако поскольку содержание процедуры BIST различна для каждого типа микропроцессора, то необходимость проводить детерминированный этап диагностирования остается. Во время этого этапа при сравнительно небольшом количестве поданных тест-векторов проверяется весьма большое количество неисправностей.

На втором этапе производится диагностирование стохастическим методом. При этом единицей входных воздействий служит *цикл шины*. Такой подход позволяет экономить память входных воздействий (при поддержке таких функций аппаратной частью комплекса диагностирования). Для построения входной последовательности используется аппарат многосвязанных марковских цепей. Под многосвязанной марковской цепью понимается последовательность, в которой вероятность перехода в следующее состояние зависит не только от текущего состояния, но и от n предыдущих состояний (n – глубина связанности). Под состоянием будем понимать процедуру формирования того или иного цикла шины. Таким образом можно значительно уменьшить размер матрицы переходных вероятностей по сравнению с [2] ввиду того, что число разнообразных циклов шины для современных процессоров не превышает 10.

Процедура тестирования начинается с подачи сигнала сброса и приведения микропроцессора в заранее заданное состояние. Далее алгоритм представляет собой последовательное выполнение следующих шагов:

1. Вычисление нового состояния марковской цепи.
2. Доопределение необходимых параметров цикла (адрес, данные).
3. Изменение матрицы вероятностей – уменьшение вероятности перехода в наиболее часто встречающееся состояние и увеличение остальных вероятностей.
4. Повторение шагов 1-3.
5. Подача сформированных таким образом тест-векторов на реальный объект и на имитационную модель, сбор реакций и их анализ.

Данный алгоритм, полагая память входных воздействий и реакций достаточно большой для хранения сформированной таким образом последовательности, не рассматривает способы установки микропроцессора в заранее определенное состояние и методы приостановки-запуска процедуры диагностирования.

Для применения данного подхода к диагностированию микропроцессорных компонентов необходимо обладать знаниями о структурной схеме компонента, путях передачи данных, реализуемых шинных циклах и иметь процессную модель данного компонента. Аппаратной поддержкой служит комплекс диагностики, содержащий в своем составе средства подачи тестовых воздействий на объект диагностирования и средства сбора реакций объекта на данные воздействия.

Предложенный метод диагностирования является применимым для задач поиска источников аппаратно реализуемых угроз безопасности информации в микропроцессорных системах.

Список литературы: **1.** *Хаханов В.И.* Техническая диагностика элементов и узлов персональных компьютеров. К.:ИСМО, 1997. 308с. **2.** *Клисторин И.Ф., Гремальский А.А.* Функциональный контроль микропроцессорных устройств. Минск: Знание, 1990г. 90с. **3.** *Raimund Ubar, Dominique Borrione.* Design Error Diagnosis in Digital Circuits without Error Model. TIMA research report. 1999 june, pp 1-5.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 09.02.200