ОБНАРУЖЕНИЕ ОТКАЗОВ НА ОСНОВЕ ДОСТУПНОСТИ АДРЕСНЫХ ДАННЫХ

Б. В. Сивко
Лаборатория «Безопасность и электромагнитная совместимость технических средств»,
Белорусский государственный университет транспорта
Гомель, Республика Беларусь
E-mail: bsivko@gmail.com

Рассматривается предложенный автором метод, позволяющий проектировать отказоустойчивые и безопасные системы, которые способны обнаружить отказы аппаратного обеспечения, выполняющего функцию адресации. В докладе излагаются способы разработки подсистем по обнаружению любых константных отказов адресных регистров и отказов короткого замыкания смежных разрядов микропроцессорных систем. К характерным адресным элементам относятся: программный счетчик микропроцессора, адресные регистры общего назначения и регистр стека, программные указатели на таблицы и массивы данных. Приводятся примеры использования метода и доказательство его корректности. Предложенный метод отличается тем, что он является простым в реализации, гибким в применении и обладает математически доказанной эффективностью.

Введение

В современных системах, критичных к безопасности (safety-critical systems, СКБ), широко используются микропроцессорные аппаратно-программные комплексы, позволяющие с помощью программного обеспечения (ПО) предоставить широкие функциональные возможности. Вместе с тем, к данным системам предъявляются повышенные требования по безопасности и надежности функционирования. Для таких систем в настоящее время одной из актуальных задач является создание эффективных методов и средств, позволяющих решать ключевые проблемы безопасности [1].

Адресные регистры и переменные являются неотъемлемыми элементами микропроцессорных систем, а отказы в них часто приводят к непредсказуемому поведению и соответствующим последствиям. Верификация СКБ относительно рассматриваемых отказов является трудоемким процессом, и в ряде случаев доказательство является сложным или проводится с рядом допущений. Предлагаемый метод позволяет решить данные проблемы для широкого класса систем.

Рассматриваемый метод является дополнением к существующим методам: он позволяет проверять элементы определенного класса с высоким качеством и с минимальными требованиями как к аппаратному, так и программному обеспечению. Данная цель согласуется с результатами исследований [2], согласно которым отказы в адресных элементах ведут к потере программного управления (invalid program flow), к чтению и записи по неправильным адресам, к попыткам доступа отсутствующей памяти и др. Таким образом, обнаружение отказов данного рода рассматриваются как одна из ключевых проблем отказоустойчивости и безопасности микропроцессорных систем, что требует решения.

I. Описание метода

Метод разработан на основании аксиоматико-базисного подхода [3] и сформулирован в общем случае. Для его применения рассматривается две базовые модели отказов цифровых систем: модель константных отказов (stuck-at fault model, SA) и модель отказов короткого замыкания (bridging fault model, B) [4]. Отказы в рамках данных моделей считаются наиболее вероятными в микропроцессорных устройствах [5]. При необходимости, метод может быть адаптирован к другим моделям отказов.

Для представления отказа рассматривается адресный регистр и его адресное отображение. Регистр представляет собой некоторое число n битовых значений (как вектор a), а отображение $A(a)$ является функцией, которая показывает, на какой реальный адрес регистр выполняет обращение (1).

$$A(a) = \sum_{i=0}^{n-1} a_i \cdot 2^i \qquad (1)$$

Отображение для работающей системы, подверженной отказам, обозначается как $R(a)$ для адреса и $r(a_i)$ для одиночного бита (2).

$$R(a) = \sum_{i=0}^{n-1} r(a_i) \cdot 2^i \qquad (2)$$

Когда в системе не происходит отказов, то выполняется условие (3).

$$\forall a \; A(a) \; = \; R(a) \qquad (3)$$

Если регистр подвергается отказам, то его отображение изменяется. В данных определениях SA-отказы рассматриваются так, как показано на рисунке 1.

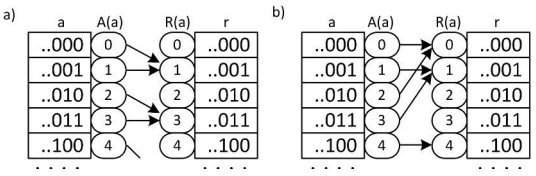

Рис. 1 – Отказ SA1 для младшего бита bit (a) и SA0 для второго младшего (b)

Условие недоступности по адресу A можно записывается как (4).

$$\forall a \; A \neq R(a) \tag{4}$$

Ключевой идеей метода является выбор таких адресов, когда некоторые из них гарантированно переходят в недоступное состояние в случае отказа. Например, в простейшем случае может быть выбрано два таких адреса A_1 и A_2, для одного из которых в случае отказа гарантированно выполняется условие (4). Следующим шагом по методу является размещение по данным адресам информации или команд, наличие доступа к которым позволяют сделать вывод о корректности работы системы. В случае доступности делается заключение об отсутствии отказов описанного типа, а в случае недоступности определяется факт наличия отказа и происходит соответствующая реакция.

II. Обнаружение отказов

Для обнаружения SA и B-отказов были сформулированы и доказаны теоремы 1 и 2 соответственно.

Теорема 1. Если рассмотреть вектор a из n бит, и адресацию $A(a)$ как как целое неотрицательное число в виде суммы степеней числа 2, то необходимым и достаточным условием обнаружения отказа константного нуля на основании (4) для i-го бита будет $a_i = 1$, а для обнаружения константной единицы того же бита условие $a_i = 0$.

Теорема 2. Для обнаружения отказов короткого замыкания для пары бит вектора a, который состоит из n бит и адресуется как целое неотрицательное число в виде суммы степеней числа 2, то следующее условие является необходимым и достаточным. Как минимум один адрес должен иметь разные значения в паре бит. Т. е., для пары бит a_i и a_j условие может быть записано как (5).

С помощью выведенных утверждений по методу решается задача обнаружения отказов заданного типа для определённых элементов, когда для них подбираются такие адреса, которые покрывают все требуемые пары. Например, для зашиты от SA-отказов для всех бит и B-отказов смежных бит могут быть выбраны адреса 01010101 и 10101010, а для обнаружения всех B-отказов адреса 01010101, 11001100 и 00001111.

Метод имеет строгое доказательство для постоянных отказов. Вместе с тем, это не исключает его применение с привлечением вероятностных подходов, например, когда с большой вероятностью один из рассматриваемых адресов становится недоступным. Для СКБ это должно согласовываться с соответствующими требованиями по безопасности и отказоустойчивости.

$$a_i \neq a_j \tag{5}$$

III. Применение

Метод применяется для разработки безопасных и отказоустойчивых систем с применением диверситетных аксиоматических базисов и метода взаимной проверки аксиоматических базисов [6, 7]. В настоящее время разработаны: безопасный генератор импульсов для систем СКБ [6] и типичное железнодорожное устройство (система, выполняющая счёт осей подвижного состава) [8]. Данные устройства были верифицированы в лаборатории посредством имитационных испытаний, которые подтвердили, что метод обнаруживает 100 % отказов для целевых адресных элементов.

Заключение

В докладе рассматриваются основные положения метода, доказательства теорем, применение метода для различных архитектур микропроцессора, альтернативные примеры интеграции с ПО, преимущества и недостатки различных способов применения метода, а также интеграция с другими подходами.

1. Бочков, К. А. Микропроцессорные системы автоматики на железнодорожном транспорте : учеб. пособие / К. А. Бочков, А. Н. Коврига, С. Н. Харлап; М-во образования Респ. Беларусь, Белорусский государственный университет транспорта. – Гомель. – 2013.
2. Majzik, I. Concurrent error detection using watchdog processors // Fault Tolerant Computing Systems. – 1996. – p. 283.
3. Сивко, Б. В. Аксиоматико-базисный подход для разработки безопасных и отказоустойчивых систем. / Б. В. Сивко; Автоматика на транспорте: Санкт-Петербург. – 2015. – № 4.
4. Grout, I. A. Integrated circuit test engineering: modern techniques // Springer Science & Business Media. – 2005.
5. Kodandapani, K. L. Undetectability of bridging faults and validity of stuck-at fault test sets // IEEE Transactions on Computers. – 1980. – p. 55-59.
6. Харлап, С. Н. Разработка высоконадежных систем на основе метода взаимной проверки аксиоматических базисов / С. Н. Харлап, Б. В. Сивко // Надёжность, М. – 2016. – № 1 (56).
7. Сивко, Б. В. Диверситетные аксиоматические базисы для разработки безопасных и отказоустойчивых систем / Б. В. Сивко // Вестник БелГУТа: Наука и Транспорт. – 2014. – № 1 (28). – С. 19–23.
8. Бочков К. А., Разработка отказоустойчивых систем на основе диверситетных аксиоматических базисов / К. А. Бочков, С. Н. Харлап, Б. В. Сивко // Автоматика на транспорте: ПГУПС. – 2016. – № 1 , т. 2. – С. 47–64.