

В. М. Барбашов

ОСОБЕННОСТИ ПРОГНОЗИРОВАНИЯ БЕЗОПАСНОЙ РАБОТЫ ИС
ПРИ ВОЗДЕЙСТВИИ РАДИАЦИИ

Задача разработки радиационно-стойких цифровых больших интегральных схем (БИС) является весьма сложной вследствие наличия широкого спектра радиационных эффектов в элементах БИС, сильной зависимости характера их проявлений в схеме от режима и алгоритмов ее работы. Исследования особенностей радиационного поведения БИС, анализ системы критериальных отношений для цифровых схем различных типов позволили предложить функционально-логическую модель радиационных отказов — модель нечеткого цифрового автомата Брауэра [1]:

$$AB = \langle X, Y, M, Q, F_B, F_n \rangle, \quad (1)$$

где X и Y — вектора входов и выходов соответственно; M — вектор критериальной функции принадлежности; Q — вектор внутренних состояний; F_B и F_n — функции выхода и перехода соответственно.

Основным параметром в модели автомата Брауэра (АБ) является критериальная функция принадлежности (КФП), определяемая аналитически через метрические критериальные соотношения. Такие КФП заданы на языке моделей электрического уровня, обеспечивая взаимосвязь между электрическим и функционально-логическим уровнями модельного описания.

Модель автомата Брауэра простейших цифровых устройств на основе их таблицы или таблицы переходов, дополненной соответствующими КФП, представляется в виде логических выражений или логической схемы, в которых операции конъюнкции и дизъюнкции заменены на операции минимума и максимума соответственно. При нулевом уровне воздействия модель АБ однозначно переходит в булеву модель логического устройства.

Например, формально последовательностный автомат Брауэра (AB_n) отличается от комбинационного АБ необходимостью рассмотрения полной системы выражений (2)–(3) с переменными, зависящими от предыдущих состояний автомата.

$$\vec{y}(t) = f_B[\vec{x}(t), \vec{q}(t_0), \vec{\mu}(t)], \quad (2)$$

$$\vec{q}(t) = f_n[\vec{x}(t), \vec{q}(t_0), \vec{\mu}(t)], \quad (3)$$

где t, t_0 — момент времени ($t_0 \leq t$), $\vec{x}(t) = (x_1(t), \dots, x_n(t))$, $\vec{q}(t) = (q_1(t), \dots, q_k(t))$, $\vec{\mu}(t) = (\mu_1(t), \dots, \mu_r(t))$, $\vec{y}(t) = (y_1(t), \dots, y_m(t))$.

Специфика анализа AB_n определяется особенностями моделирования последних вследствие возможности представления любой системы с памятью в виде совокупности базовых комбинационных схем и триггерных элементов. При этом принцип построения комбинационного АБ можно распространить на случай триггерных систем, за исключением способа задания начального значения переменных в итерационной процедуре. Различие в процедуре выбора начальных условий связано с наличием в триггерах режимов, отличающихся векторами $\vec{Y}$ и $\vec{q}$ при одинаковых входных сигналах (в режиме хранения), что приводит к отличию в итоговых μ_y при решении системы уравнений (2)–(3) [2].

Проиллюстрируем вычисление выражения (4)

$$\vec{y}(t) = f[\vec{x}(t), \vec{\mu}(t)]. \quad (4)$$

на примере асинхронного RS-триггера (дизъюнктивные и конъюнктивные бистабильные ячейки (БЯ)), реализуемого на двух ЛЭ (рис. 1). Функции выходов и переходов для триггера имеют вид:

$$y_{11} = f(x_{11}, x_{12}, \vec{\mu}_1), \quad (5)$$

$$y_{21} = f(x_{21}, x_{22}, \vec{\mu}_2), \quad (6)$$

где $x_{12} = y_{21}, x_{21} = y_{11}$.



По аналогии с преобразованием циклической комбинационной схемы в ациклическую получим:

$$\bar{y} = f(\bar{x}, \bar{q}, \bar{\mu}), \quad (7)$$

где $\bar{q} = \bar{y} = (y_1, y_2)$, $\bar{x} = (x_1, x_2)$, $\bar{\mu} = (\bar{\mu}_1, \bar{\mu}_2)$.

Состояния RS-триггера в двоичном виде, характеризующие его работу, приведены в таблице 1.

Таблица 1. Состояния RS-триггера

x_1	x_2	y_1	y_2	Режим
0	0	0	1	хранение «0»
0	0	1	0	хранение «1»
0	1	0	1	установка в «0»
1	0	1	0	установка в «1»
1	1	Н	Н	неопределенный

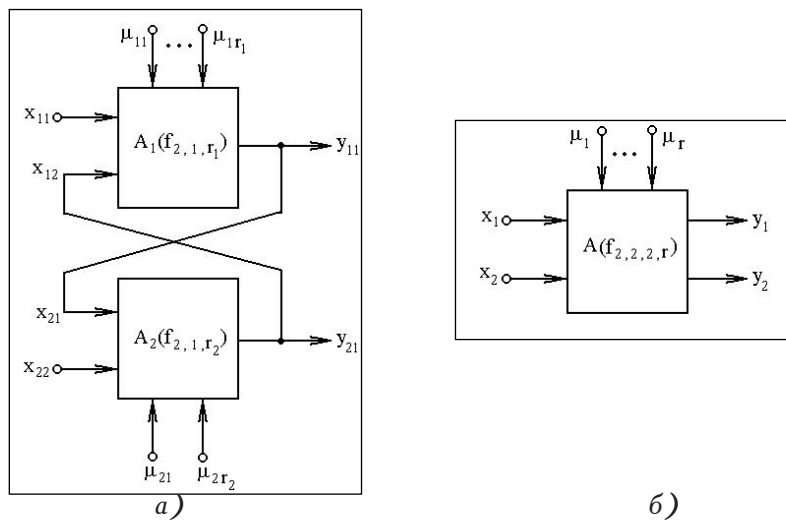


Рис. 1. Эквивалентные схемы модели автомата Брауэра (а, б)

Характер переключающих сигналов позволяет определить устойчивость состояния RS-триггера. Отсюда набор $(y_1, y_2) = (0, 1)$, $(y_1, y_2) = (1, 0)$ определяет условия чувствительности функции y переменных (x, q, μ) . Вычисления уравнения (7) дают два решения:

$$\bar{y}_1 = f_1(\bar{x}, \bar{\mu}); \quad \bar{y}_2 = f_2(\bar{x}, \bar{\mu}), \quad (8)$$

где $\bar{y}_1 \neq \bar{y}_2$ при $\bar{x} = \bar{x}_1 = \bar{x}_2$.

Комбинация входных сигналов $\bar{x} = \bar{x}_1 = \bar{x}_2$ определяет неоднозначность АБ RS-триггера и соответствует режиму «хранения информации».

Таким образом, видно, что на интервале уровней внешнего воздействия, где $\bar{y}_1 \neq \bar{y}_2$, для последовательных схем, вследствие деградации уровней логических сигналов на информационных входах ЛЭ, элементы памяти переходят в неопределенное состояние — режим хранения информации. В свою очередь, для циклических комбинационных схем возможны генерационные процессы, обусловленные попаданием под воздействием облучения всех ЛЭ в активную область работы.



СПИСОК ЛИТЕРАТУРЫ:

1. Аствацатурьян Е. Р., Беляев В. А., Скоробогатов П. К. Использование метода КФП для теоретического моделирования и экспериментального исследования радиационного поведения АПОИ на базе ИМС высокой степени интеграции // Специальная техника средств связи. 1987. Вып. 11. С. 3–12.
2. Барбашов В. М., Трушкин Н. С. Прогнозирование безопасности микропрограммных БИС в условиях возникновения информационных сбоев // Безопасность информационных технологий. 2008. Вып. 2. С. 61–64.

Е. А. Беляева

АНАЛИЗ ТЕХНИЧЕСКИХ ВОЗМОЖНОСТЕЙ МНОГОФУНКЦИОНАЛЬНЫХ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель настоящей работы заключается в анализе технических возможностей современных аппаратно-программных модулей доверенной загрузки (АПМДЗ) и подтверждении необходимости реализации дополнительных функциональных возможностей АПМДЗ в свете их влияния на функциональную безопасность автоматизированных систем в защищенном исполнении (АСЗИ) [1].

В ходе работы был выполнен анализ технических возможностей современных АПМДЗ, являющихся специальным классом многофункциональных аппаратно-программных средств защиты информации. Рассмотрены основные технические и функциональные возможности модулей, такие как: контроль целостности областей системного реестра, возможность подключения датчиков, наличие дискреционных управляющих выходов и др. Дано их сравнение по рассмотренным возможностям, в частности по управлению в режиме реального времени функционированием средства вычислительной техники с установленным аппаратно-программным модулем доверенной загрузки.

В результате работы были выделены основные дополнительные функции АПМДЗ:

- исключение возможности случайного или намеренного повреждения/вывода из строя платы АПМДЗ электрическими воздействиями (статическое электричество, электрошок) путем реализации электростатической защиты интерфейса считывателя;
- возможность контроля в режиме реального времени физической целостности и режима функционирования средства вычислительной техники, в котором установлен АПМДЗ, за счет реализации интерфейса подключения датчиков;
- возможность управления в режиме реального времени функционированием средства вычислительной техники с установленным АПМДЗ за счет реализации дискретных управляющих выходов;
- исключение возможности случайного или намеренного повреждения/вывода из строя платы АПМДЗ в случае возникновения перепадов или сбоев электропитания средства вычислительной техники с установленным АПМДЗ путем реализации контроля и восстановления целостности служебных структур данных платы АПМДЗ, а также реализации расширенных функций контроля питающих напряжений платы АПМДЗ;
- оснащение платы АПМДЗ сменной флэш-картой типа micro-SD;
- возможность диагностики неисправности по кодам ошибки с использованием индикатора диагностики силами эксплуатирующего персонала.

