УДК 681.3 DOI 10.31114/2078-7707-2018-2-136-143

Способ организации автомата Мура с повышенной устойчивостью к мягким отказам

И.В. Егоров

Санкт-Петербургский политехнический университет Петра Великого, г. Санкт-Петербург
ig-ego@mail.ru

Аннотация: снижение проектной нормы в производстве полупроводниковых структур повышает чувствительность цифровых устройств к попаданию частиц высоких энергий (в частности, при работе в условиях радиации), что приводит к возникновению мягких отказов – искажению информации при сохранении работоспособности аппаратуры. Известно, что наиболее действенным средством защиты от мягких отказов является периодическая перезапись искаженных данных корректными (восстановление информации). По этой причине традиционные способы повышения надежности, основанные на использовании структурной избыточности, оказываются малоэффективными в условиях мягких отказов. *Цель:* разработка новых способов структурной организации автомата Мура, работающего при потоке мягких отказов. *Результаты*: разработана структура автомата Мура с троированием памяти, мажорированием выходных сигналов памяти и восстановлением информации на каждом такте, а также оснащенная средствами регистрации количества мягких отказов, произошедших в ходе работы автомата.

***Ключевые слова* — автомат с памятью, комбинационная схема, анализ надежности, синхронизация, мягкие отказы, структурное резервирование, восстанавливаемые системы, вероятность безотказной работы.**

I. Введение

Под мягким отказом понимается явление, при котором в элементе памяти вычислительной системы происходит искажение бита данных. Элемент памяти при этом остается работоспособным. Возникновение мягких отказов наиболее характерно при работе устройства в условиях повышенной радиации [1].

В опубликованных работах [2–4] проанализированы процессы в логических элементах и триггерах, выполненных по технологии КМОП (CMOS Fabrication), протекающие при воздействии радиации. Выявлено, что основной причиной возникновения мягких отказов является попадание частицы высокой энергии в МОП-транзистор, в результате которого происходит ионизация подзатворной области полупроводника, что в свою очередь приводит к проскакиванию импульса тока на выходе вентиля, в схему которого входит транзистор. Длительность импульса зависит от величины заряда неосновных носителей, а он – от энергии частицы и технологических параметров вентиля. Обычно длительность импульса находится в диапазоне до 1–2 нс. При микронной и субмикронной технологии производства ИС эти импульсы были неопасны вследствие инерционности элементов. При современной нанотехнологии производства ИС с проектной нормой меньше 0,1 мкм, такие наведенные ложные импульсы сравнимы с полезными импульсными сигналами и могут привести к искажению полезной информации в СБИС. Статистически установлено [5], что на текущем уровне технологии именно мягкие отказы наиболее часто (примерно в 95% случаев) являются причиной выхода из строя космических аппаратов.

Известны [6] методы борьбы с мягкими отказами на различных уровнях организации системы:

а) на уровне проектирования и изготовления ИС;

б) на уровне стандартных элементов, входящих в библиотеку САПР;

в) на уровне функциональной организации СБИС.

Установлено, что текущие средства защиты на уровне изготовления ИС (технология SOI) и на уровне библиотек элементов (путем искусственного снижения быстродействия триггеров или использования DICE-ячеек) приносят количественный эффект, но не позволяют решить проблему мягких отказов на качественном уровне.

Также для повышения надежности широко применяются способы структурного троирования с мажорированем – triple modular redundancy (TMR) [7], однако они приводят к увеличению структурной сложности схемы и уменьшению ее быстродействия. Рост структурной сложности ведет к увеличению площади, занимаемой схемой на кристалле, что в условиях повышенной радиации повышает вероятность попадания в нее частицы высокой энергии и возникновения мягкого отказа. Это понижает эффективность данного метода защиты [8].

При разработке сложных информационных систем с повышенной устойчивостью к мягким отказам особое распространение получил подход, называемый "доменной организацией" системы [9, 10]. Его суть заключается в декомпозиции системы на

"отказоустойчивые ячейки" – структурные блоки, надежность которых повышается за счет применения различных методов резервирования (в частности, TMR) и организации восстановления таким образом, что отказы в каждом из блоков происходят независимо друг от друга. По функциональному назначению эти блоки разделяют на два типа: автомат с памятью и запоминающее устройство. Для типовой организации отказоустойчивой ячейки опубликован метод оценки надежности [11], из которого следует важный вывод: частота возникновения мягкого отказа восстанавливаемого блока обратно пропорциональна организованному в нем периоду восстановления. Эта зависимость обосновывает актуальность задачи организации блоков обоих типов, обеспечивающей периодическое восстановление их состояния, так как это позволит значительно повысить устойчивость блока к мягким отказам и, следовательно, надежность устройства при воздействии радиации. Данная работа посвящена организации структуры конечного автомата с памятью с периодическим самовосстановлением.

В ходе предварительных исследований автором были получены оценки вероятности возникновения мягкого отказа при попадании частицы высокой энергии в транзистор для различных известных реализаций конечного автомата со структурной избыточностью [12, 6]. Эти оценки могут быть использованы для дальнейшего их сравнения с характеристиками надежности разработанной автором отказоустойчивой структуры конечного автомата с восстановлением на каждом такте и регистрацией отказов, описываемой в данной работе.

II. Модель и традиционная структура автомата Мура

Традиционно модель абстрактного конечного автомата S представляется следующей математической структурой:

$S = <A,B,R,\delta,\lambda,r_0>$, где

A – множество состояний входа (входной алфавит),

B – множество состояний выхода (выходной алфавит),

R – множество внутренних состояний,

$r_0 \in R$ – начальное состояние, в которое автомат приводится сигналом начальной установки,

$\delta: A \times R \rightarrow R$ – функция переходов,

$\lambda: R \rightarrow B$ – функция выходов.

В проектировании цифровых устройств используются три типа абстрактных конечных автоматов: автоматы Мили, Мура и Медведева [13]. Для всех трех типов автоматов функция переходов имеет одинаковое теоретико-множественное представление: $\delta: A \times R \rightarrow R$.

Типы автоматов различаются представлением функции выхода λ. Для автомата Мили $\lambda: A \times R \rightarrow B$, для автомата Мура: $\lambda: R \rightarrow B$, для автомата Медведева: $\lambda: B=R$.

Как средства формализованного представления алгоритма эти модели равномощны: для каждого автомата одного типа можно построить эквивалентный автомат другого типа. С точки зрения реализации на электронных схемах типы автоматов имеют различия в двух отношениях: по качеству выходных сигналов; по затратам триггеров на память автомата.

Наилучшее качество выходных сигналов имеет автомат Медведева. В этих автоматах значение выходного сигнала устанавливается сразу после переключения триггера синхронно с фронтом либо спадом тактового импульса и сохраняется в течение всего такта.

В автоматах Мура качество выходных сигналов несколько хуже, так как при их формировании выходные сигналы триггеров подвергаются некоторым функциональным преобразованиям, соответствующим функциям выходов λ. Но следует отметить, что глубина распространения сигналов в соответствующей комбинационной схеме невелика, поэтому переходные процессы распространения сигналов быстро завершаются в начале такта после переключения триггеров.

В автоматах Мили качество выходных сигналов хуже, чем в других типах автоматов. Это связано с тем, что при их формировании глубина распространения сигналов по сети элементов наиболее велика. Она включает процессы во внешней схеме, формирующей входные сигналы автомата, переключение триггеров и процессы в схеме, реализующей функции выходов λ. Эта схема имеет существенно большую сложность и глубину распространения сигналов в сравнении с автоматом Мура. У функций выхода автомата Мили больше число аргументов, как это видно из приведенного выше теоретико-множественного представления функций λ для разных типов автоматов. В связи с этим выходные сигналы в автомате Мили устанавливаются только в конце такта.

По затратам триггеров минимальное число имеет автомат Мили, максимальное – автомат Медведева. Таким образом, с точки зрения рассмотренных показателей автомат Мура дает компромиссное решение. Следует отметить, что автоматы Мура чаще всего и применяются при проектировании цифровой аппаратуры.

Традиционная структурная схема автомата Мура представлена на рис. 1.

Комбинационная схема КС1 реализует функцию переходов δ, КС2 реализует функцию выходов λ. Для реализации блока памяти (П) автомата использовано *s* триггеров (ТТ) типа D, синхронизируемых спадом тактового сигнала *C*. Входы триггеров: R – сигнал сброса, D – входные данные, C – вход синхронизации. НУ – сигнал начальной установки. Связи между блоками соответствуют функциям в автомате Мура: δ:

{**X**}×{Q}→ {Q}; λ: {Q}→{**Y**}, где разрядность вектора **X** равна *m*, а разрядность вектора **Y** равна *n*. τ_1, τ_2, τ обозначают задержки в электронных схемах, реализующих блоки КС1, КС2 и П, соответственно.

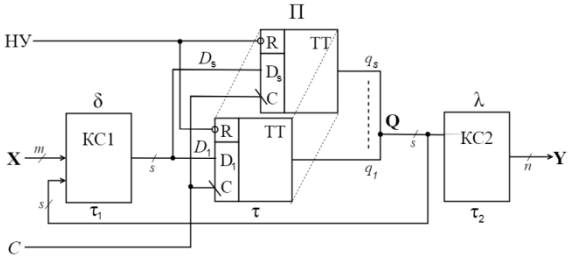

Рис 1. Структурная схема автомата Мура

Для данной структуры в [6] автором получена формула, позволяющая вероятность отсутствия мягких отказов $\overline{P}_{\text{м.о.а}}$ в автомате в течение некоторого времени выполнения задачи $T_з$ при известной частоте $q_{\text{п.ч.т}}$ попадания заряженных частиц в один из транзисторов конечного автомата:

$$\overline{P}_{\text{м.о.а}} = e^{-(q_{\text{м.о.п}}+q_{\text{м.о.КС1}})T_з},$$

где $q_{\text{м.о.п}}$ – частота возникновения мягкого отказа автомата по причине попадания заряженной частицы в область памяти; $q_{\text{м.о.КС1}}$ – частота возникновения мягкого отказа автомата по причине попадания заряженной частицы в область КС1.

При оценке вероятности возникновения мягкого отказа необходимо учитывать, что ложный импульс, распространяющийся с выходов КС1, влечет за собой изменение состояния П (мягкий отказ) только в том случае, если он совпадет по времени с моментом записи данных (спадом синхроимпульса С) в один из триггеров П. Этот интервал времени занимает незначительную долю периода синхронизации автомата. Таким образом, с точки зрения надежности КС1 имеет меньшую структурную значимость, нежели П, где ложное изменение состояния любого из триггеров непосредственно приводит к мягкому отказу. Однако КС1 может содержать большее по сравнению с П число логических элементов, что увеличивает вероятность попадания заряженных частиц в ее область и приводит к необходимости разработки механизма борьбы с ложными импульсами на выходах КС1.

III. Структура автомата Мура с троированием, мажорированием и самовосстановлением

Применительно к рассматриваемой задаче построения автомата с повышенной устойчивостью к мягким отказам автором было определено расширение функций автомата дополнительно к основной функции реализации алгоритма:

а) блокирование прохождения мягкого отказа на выход автомата;

б) восстановление состояния отказавшего экземпляра автомата без прерывания выполнения основной функции;

в) выявление, регистрация и подсчет числа мягких отказов в автомате.

Перечисленные расширения реализованы в разработанной автором и защищенной патентом [14] структурной схеме автомата Мура с троированием, мажорированием и самовосстановлением, приведенной на рис. 2. Принцип реализации этих расширений применим для последовательностных схем, соответствующих не только автомату Мура, но также автоматам Мили и Медведева. Отличия в обеспечении защиты от мягких отказов для других типов автомата несущественны, и предложенные способы защиты могут быть в них использованы очевидным образом.

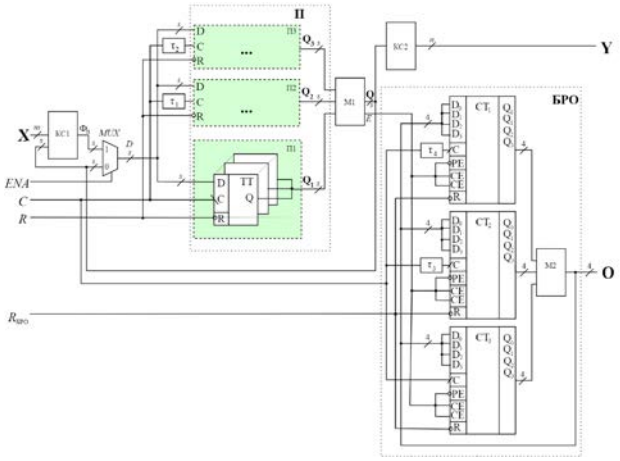

Рис. 2. Структурная схема автомата Мура с троированием, мажорированием и самовосстановлением

Рассмотрим состав схемы и ее отличительные особенности в сравнении с традиционной (рис. 1) структурой автомата Мура без резервирования.

Входные сигналы, аналогичные рис.1:

X – m-разрядный вектор входных информационных сигналов;

C – тактовый импульс синхронизации;

R – сигнал сброса (начальной установки).

Дополнительные входные сигналы:

ENA (enable) – сигнал разрешения работы автомата: при ENA=1 работа разрешена; при ENA=0 автомат остановлен, при переходе сигнала ENA 0→1 автомат продолжит работу с того состояния, в котором был остановлен;

$R_{\text{БРО}}$ – сигнал сброса блока регистрации ошибок БРО. В восстанавливаемых системах периодически проводится мониторинг состояния блоков (проверка количества отказов, зарегистрированных БРО), в конце каждого цикла мониторинга производится сброс состояния БРО на начальное.

Выходные сигналы автомата:

Y – n-разрядный вектор информационных выходных сигналов (аналогично сигналам на рис.1);

O – код числа мягких отказов в автомате за период мониторинга.

Перечень блоков структуры:

КС1 – комбинационная схема, реализующая функцию переходов δ, аналогичная рис.1;

КС2 – комбинационная схема, реализующая функцию выходов λ, аналогичная рис.1;

П – блок памяти автомата, содержащий 3 экземпляра П1, П2, П3 (каждый аналогичен блоку памяти П на рис.1);

М1 – блок мажорирования троек соответствующих выходных сигналов блоков П1, П2, П3;

MUX – мультиплексор, переключающий на информационные входы блоков памяти (D) сигнал $\Phi_п$ перехода с выходов комбинационной схемы КС1, либо сигнал Q с выходов блока М1;

БРО – блок регистрации ошибок (мягких отказов в автомате);

СТ1, СТ2, СТ3 – три экземпляра синхронных счетчиков для подсчета числа мягких отказов;

М2 – блок мажорирования сигналов с выходов счетчиков и формирования сигнала О – числа мягких отказов за период мониторинга;

τ_1, τ_2, τ_3, τ_4 – элементы задержки.

IV. Принцип работы автомата Мура с троированием, мажорированием и самовосстановлением

Раскроем функции новых по сравнению с традиционной структурой автомата Мура (рис. 1) блоков.

Отличие данного структурного решения от TMR заключается в применении троирования не устройства памяти, а памяти как части конечного автомата. Такие автоматы в вычислительных системах играют роль управляющих блоков и операционных блоков. Особенность троирования состоит в том, что троируется не весь автомат, а только память состояний и предусмотрено периодическое (каждый такт) восстановление информации в ней, а влияние мягких отказов в комбинационной схеме КС1 устраняется другим оригинальным способом, описанным ниже.

Блок мажорирования М1 содержит s (s – число триггеров в памяти автомата) мажоритарных элементов. Возможная схема, реализующая мажоритарный элемент, представлена на рис. 3.

Помимо этого блок М1 содержит схему, реализующую функцию E(**Q_1, Q_1, Q_3**) выявления мягкого отказа, возвращающую логическую 1 в том случае, если сигналы на x_1, x_2, x_3 на входах М1 не одинаковы.

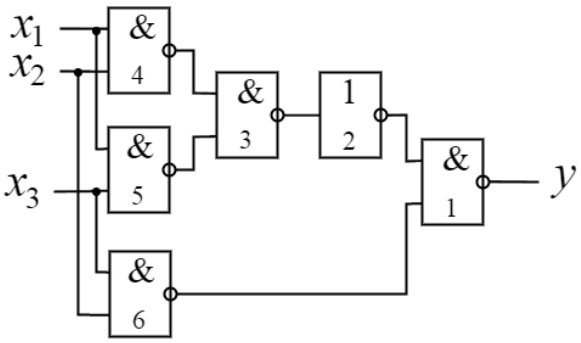

Рис. 3. Структурная схема мажоритарного элемента

Сигнал E поступает на вход блока регистрации ошибок БРО. В БРО для подсчета числа мягких отказов (ошибок) используется синхронный счетчик, например, соответствующий стандартному счетчику К1533ИЕ10. Счетчик имеет информационные входы записи ($D_0D_1D_2D_3$), вход PE разрешения записи (при PE=0), входы CE разрешения прибавления единицы (при CE=1), вход синхронизации C и вход сброса R. Поскольку в самом счетчике под воздействием радиации могут возникать мягкие отказы, то в блоке БРО применяется троирование счетчика и мажорирование. Блок мажорирования М2 содержит 4 мажоритарных элемента соответственно числу разрядов в счетчике. Выходы блока мажорирования подключены к внешнему выходу О автомата и к информационным входам ($D_0D_1D_2D_3$) всех 3-х счетчиков. Управляющие входы PE и CE всех трех счетчиков соединены и подключены к выходу E блока мажорирования М1. Таким образом, при E=1 в счетчиках по спаду C прибавляется 1, при E=0, по спаду C записывается код с выхода М2, и каждый такт в счетчиках БРО происходит самовосстановление информации.

При работе автомата в режиме реализации алгоритма каждый такт выполняется переход в новое состояние. В случае возникновения отказа в одном из экземпляров памяти он не проявляется на выходе Q мажоритара, и на информационные входы элементов П каждый такт поступает верная информация. Таким образом, каждый такт осуществляется самовосстановление данных в П.

В некоторых случаях в системах организуется работа автомата в стартстопном режиме. Для этого используется сигнал ENA (enable), вырабатываемый управляющим блоком системы. Режим временной приостановки работы автомата может быть достаточно длительным. За это время в памяти автомата также могут возникать мягкие отказы. С целью организации самовосстановления памяти автомата в этом режиме выходные сигналы **Q** с выхода блока М1 поступают не только на входы комбинационной схемы КС1, но и на вход мультиплексора MUX. При этом, если ENA=0,

каждый такт происходит самовосстановление памяти П.

В работе [8] аргументирована необходимость борьбы с ложными импульсами на выходе КС1, так как они являются источниками мягких отказов в памяти состояний. Также доказана низкая эффективность мажорирования на уровне КС1, поскольку в этом случае источником ложных импульсов, искажающим данные памяти состояний, становится мажоритарный элемент. Поэтому для уменьшения влияния ложных сигналов на выходах КС1, подключенных к информационным входам триггеров памяти автомата, предложен следующий способ. Как отмечено в [8], ложный импульс, поступающий на информационный вход триггера, может изменить его состояние, если этот импульс попадает в интервал $\tau=t_{SU}+t_H$, где t_{SU} - время предустановки триггера, t_H - время удержания триггера, на практике составляющий малую долю от периода синхронизации T_C. С учетом этого в троированной схеме памяти автомата П (рис. 2) в цепь передачи синхроимпульсов С введены элементы задержки: $\tau_1=\tau$ для экземпляра памяти П2 и $\tau_2=2\tau$ для экземпляра П3. Благодаря этому, переключение всех триггеров в П2 происходит по сравнению с П1 с задержкой τ, а в П3 – с задержкой 2τ.

Положительное влияние введенных задержек на надежность автомата проиллюстрировано на рис 4.

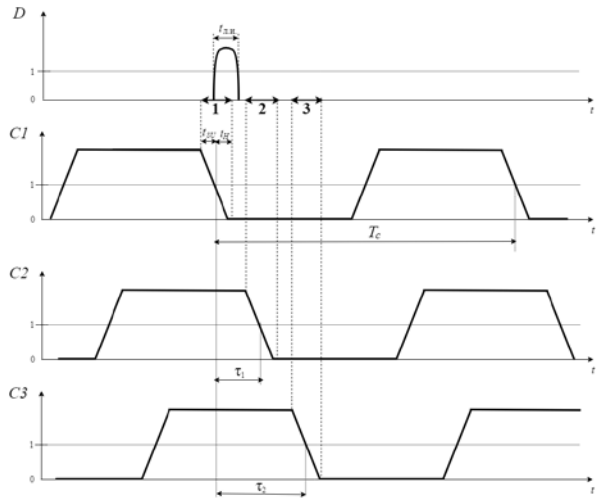

Рис. 4. Принцип уменьшения влияния ложных сигналов на выходах КС1

На рис. 4 использованы следующие обозначения:

D – сигнал на информационных входах D триггеров блока памяти П (рис. 2);

С1, С2, С3 – входы синхронизации С экземпляров блока памяти П1, П2, П3 соответственно (рис.2);

ТС – период синхронизации триггеров.

На входы D поступает кратковременный ложный импульс длительностью $t_{л.и.}$ Для каждого экземпляра блока памяти (П1, П2, П3) существует временной интервал (1, 2 и 3 соответственно) длительностью $t_{SU}+t_H$, в течение которого сигнал на входе D влияет на состояние триггеров данного экземпляра. Эти интервалы между собой не пересекаются из-за внесенных задержек τ_1, τ_2. Таким образом, ложный импульс, попадающий только в интервал 1, вызывает мягкий отказ в П1, но не оказывает влияния на П2 и П3. А поскольку выходы троированного блока памяти П подключены к мажоритару М1, мягкий отказ в одном из экземпляров блока памяти не вызывает искажения выходного вектора **Q**. Таким образом, распространение мягкого отказа заблокировано.

Искажение состояния троированной памяти может произойти только в том случае, если в течение одного такта ложный сигнал на входах D захватит минимум два интервала длительностью $t_{SU}+t_H$, отмеченных выше. Назовем это сложное событие возникновением неисправленного отказа в памяти из-за ложных сигналов на входе D. Зависимость вероятности $P_{н.о.D}$ этого события от вероятности $P_{л.с.D}$ появления ложного сигнала на информационном входе D как:

$$P_{н.о.D} = (P_{л.с.D}\frac{\tau}{T_C})^2,$$

Где выражение $P_{н.о.D}$ представляет собой вероятность появления ложного сигнала на информационном входе D в течение одного такта и попадания его в интервал τ при спаде импульса С. Очевидно, что на практике значение $P_{н.о.D} << 1$, что практически исключает воздействие ложных импульсов на входе D на работу автомата.

Аналогичный способ введения задержек ($\tau_3=\tau$, $\tau_4=2\tau$) в цепь передачи синхроимпульсов используется и в блоке БРО.

V. Анализ надежности автомата Мура с троированием, мажорированием и самовосстановлением

В работе [6] автором оценивалась вероятность сохранения конечным автоматом работоспособности в течение времени $T_з$ решения алгоритмической задачи. Для аналогичной функциональной спецификации конечного автомата проведем оценку надежности разработанной структуры автомата Мура с троированием, мажорированием и самовосстановлением.

В ходе анализа будем считать, что все отказы в элементах автомата являются мягкими (восстанавливаемыми), возникающими по причине попадания заряженных частиц в транзисторы автомата с некоторой известной интенсивностью $q_{п.ч.т.}$ Работоспособность автомата считается утраченной, если на выход автомата Y (рис. 2) поступают искаженные данные. При оценке не будем рассматривать блок БРО (рис. 2), так как он реализует

дополнительную функцию, не связанную с решением основной задачи автоматом.

Проанализируем, в результате чего может исказиться выходной сигнал автомата. Основной причиной являются мягкие отказы в элементах памяти, которые приведут к потере работоспособности, если за один такт работы автомата в одинаковых битах двух различных экземпляров памяти П произойдет мягкий отказ. В противном случае побитный мажоритар М1 по цепи обратной связи передаст корректные данные на входы П1, П2, П3, и на следующем такте состояние памяти будет автоматически восстановлено. Для получения оценки вероятности отказа в памяти ограничимся рассмотрением ситуаций, когда за такт работы автоматы возникает от нуля до трех отказов (остальными случаями пренебрежем, так как вероятность их возникновения на несколько порядков меньше). Тогда, обозначив событие мягкого отказа бита памяти за $A_{пi,j}$ (где i – номер экземпляра памяти, j – порядковый номер бита памяти в экземпляре), рассмотрим возможные комбинации событий, которые приведут к отказу блока памяти.

В условиях текущей задачи каждый блок памяти содержит 3 информационных бита (s=3, что определяется функциональной спецификацией). В случае отсутствия искаженных бит памяти, либо при наличии только одного искаженного бита, отказа рассматриваемой структуры не происходит. При наличии двух искаженных бит к отказу приведут следующие комбинации: $A_{п1,1}A_{п2,1}$, $A_{п1,1}A_{п3,1}$, $A_{п2,1}A_{п3,1}$, $A_{п1,2}A_{п2,2}$, $A_{п1,2}A_{п3,2}$, $A_{п2,2}A_{п3,2}$, $A_{п1,3}A_{п2,3}$, $A_{п2,3}A_{п3,3}$, $A_{п1,3}A_{п3,3}$. Итого 9 комбинаций для случая двух искаженных бит. При наличии трех искаженных бит к отказу приводят 57 возможных комбинаций событий.

Общую вероятность возникновения отказа в памяти автомата оценим как сумму вероятностей возникновения рассмотренных несовместных комбинаций событий одновременного отказа двух или трех бит в блоке памяти.

$$P_{м.о.а} = 9(P_{м.о.бита})^2(1-P_{м.о.бита})^7 + 57(P_{м.о.бита})^3(1-P_{м.о.бита})^6. \quad (1)$$

Определим зависимость вероятности искажения бита данных в памяти $P_{м.о.бита}$ в (1) от интенсивности $q_{п.ч.т}$ попадания заряженной частицы в транзистор автомата. Причин, вследствие которых может возникнуть искажение, две. Первая – попадание заряженной частицы непосредственно в область памяти. Так как один бит памяти реализуется триггером, состоящим из 5 транзисторов, интенсивность возникновения этого события равна $5q_{п.ч.т.}$. Вторая причина – запись искаженной информации вследствие попадания заряженной частицы в элементы КС1 или MUX, подключенные к соответствующему биту памяти. Исходя из расчетов, произведенных в [6], интенсивность появления ложных импульсов на выходах КС1 равна $3,4q_{п.ч.т.}$, а на выходах мультиплексора – $1,25q_{п.ч.т.}$. Для оценки интенсивности появления ложных импульсов, оказывающих влияние на П, эти величины необходимо умножить на коэффициент K=0,15, так как элементы КС1 и MUX влияют на работу памяти только в момент спада синхроимпульса (обычно занимающего не больше 15% от длительности такта). Суммарная интенсивность искажений одного бита данных соответственно равна $5q_{п.ч.т}+0,15(3,4q_{п.ч.т}+1,25q_{п.ч.т})=5,7q_{п.ч.т}$. Исходя из этого, вероятность искажения бита памяти $P_{м.о.бита}$ в течение одного такта синхронизации ТС автомата выражается через интенсивность попадания заряженной частицы в транзистор $q_{п.ч.т}$ следующим образом:

$$P_{м.о.бита} = 1 - e^{-5,7 q_{п.ч.т} T_c}. \quad (2)$$

Подставив выражение (2) в (1) получим вероятность отказа всей структуры в течение одного такта работы автомата.

Поскольку в начале каждого такта происходит восстановление состояния системы, вероятность безотказной работы автомата в течение n последовательных тактов вычисляется как произведение вероятностей безотказной работы в течение каждого такта:

$$\overline{P_{м.о.а}}(n) = (1 - P_{м.о.а})^n.$$

Используя полученные выражения, построим графики функции вероятности безотказной работы на интервале $T_з$ (n=100 тактов) для исследованной структуры (структура 4) и сравним его с графиками, построенными для трех известных отказоустойчивых структур, проанализированных автором в [8]:

Структура 1 – автомат без структурного резервирования (рис. 1);

Структура 2 – автомат с троированными блоками и троированными входными мажоритарами без периодического восстановления информации;

Структура 3 – автомат с троированными блоками и троированными входными мажоритарами и периодическим восстановлением информации. Восстановление искаженного состояние происходит за счет формирования сигнала начальной установки в конце каждого цикла работы автомата (период восстановления соответствует длительности цикла алгоритма работы автомата).

Графики функций работоспособности проанализированных структур приведены на рис. 5.

Ось абсцисс обозначает текущее время t решения задачи, измеряемое в количестве тактов работы автомата. По оси Y расположена вероятность нахождения автомата в работоспособном состоянии (1 – гарантированно работоспособен, 0 – гарантированно неработоспособен).

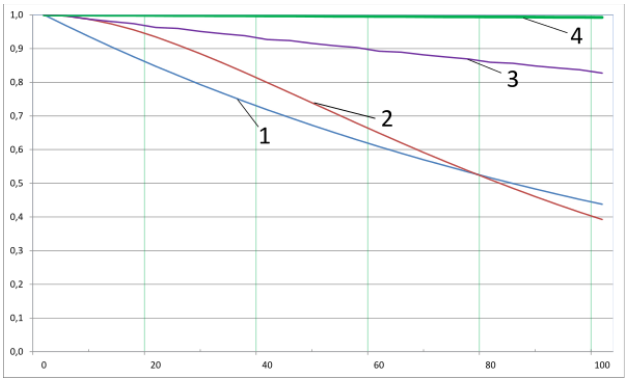

Рис. 5. Функции работоспособности анализируемых структур

Итоговая вероятность успешного решения задачи для предложенной структуры 4 равна 0,99. Аналогичная величина, рассчитанная для структуры 3 (показавшей в [8] лучшие характеристики надежности), равна 0,84 что наглядно демонстрирует преимущество предложенной структуры при работе в условиях мягких отказов. Это превосходство обеспечивается меньшим по сравнению со структурой 3 периодом восстановления – оно происходит на каждом такте, а не только по окончании цикла работы алгоритма.

Заключение

Определены расширения функциональности традиционной структуры автомата Мура, позволяющие повысить надежность устройства в случае функционирования при потоке мягких отказов.

Разработана структура автомата Мура с троированием памяти, мажорированием выходных сигналов памяти и восстановлением информации в каждом такте. Данная структура обладает повышенной защитой от ложных импульсов, возникающих как причине попадания частиц высокой энергии в области комбинационных схем, так памяти состояний автомата. Также она оснащена средствами регистрации количества мягких отказов, произошедших в ходе работы автомата.

Оценки надежности разработанной структурой демонстрируют превосходство разработанной структуры над другими известными отказоустойчивыми структурами автомата Мура с точки зрения устойчивости к возникновению мягких отказов.

Литература

[1] Егоров И.В., Мелехин В.Ф. Анализ проблемы повышения радиационной стойкости информационно-управляющих систем на этапе функционально-логического проектирования // Информационно-управляющие системы. 2016. № 1(80). С. 26–31.

[2] Edmonds D.L., Barnes C.E., Scheick L.Z. An introduction to space radiation effects on microelectronics. Pasadena, USA: NASA, Jet propulsion laboratory, California institute of technology, 2000.

[3] Schwank J.R., Shaneyfelt M.R., Dodd P.E. Radiation hardness assurance testing of microelectronic devices and integrated circuits: Test guideline for proton and heavy ion single-event effects // IEEE Transactions on Nuclear Science. 2013. Vol. 60, № 3. P. 2101–2118.

[4] Amusan O.A. et al. Single event upsets in deep-submicrometer technologies due to charge sharing // IEEE Transactions on Device and Materials Reliability. 2008. Vol. 8, № 3. P. 582–589.

[5] Koons H.C. et. al The impact of the space environment on space systems // 6th Spacecraft Charging Technology. 1998. P. 7–11.

[6] Максименко С.Л., Мелехин В.Ф., Филиппов А.С. Анализ проблемы построения радиационно-стойких информационно-управляющих систем // Информационно-управляющие системы. 2012. № 2(57). С. 18–25.

[7] Oliveira R., Jagirdar A., Chakraborty T.J. A TMR Scheme for SEU Mitigation in Scan Flip-Flops. IEEE, 2007. P. 905–910.

[8] Егоров И.В., Мелехин В.Ф. Анализ показателей надежности и сложности реализации различных вариантов структур автомата с памятью при потоке мягких отказов // Информационно-управляющие системы. 2017. № 3(88). С. 34–46.

[9] Глухих М.И. Разработка методов синтеза информационно-управляющих систем специального назначения со структурным резервирование: дис. ... канд. техн. наук. СПб, 2006.

[10] Abraham J.A., Siewiorek D.P. An algorithm for the accurate reliability evaluation of triple modular redundancy networks // IEEE Transactions on Computers. 1974. Vol. C–23(7). P. 682–692.

[11] Максименко С.Л., Мелехин В.Ф. Анализ надежности функциональных узлов цифровых СБИС со структурным резервированием и периодическим восстановлением работоспособного состояния // Информационно-Управляющие Системы. 2013. № 2(63). С. 18–23.

[12] Егоров И.В., Мелехин В.Ф. Анализ процессов в конечном автомате при воздействии радиации. Оценка вероятности искажения информации // Информационно-управляющие системы. 2016. № 3 (82). С. 24–33.

[13] Kaeslin H. Digital integrated circuit design. from vlsi architectures to cmos fabrication / H. Kaeslin, Cambridge University Press, 2008. 879 p.

[14] Пат. 174640 RU, МПК G06F 11/07 (2006.01). Отказоустойчивый цифровой преобразователь информации для управления дискретными процессами / И. В. Егоров (RU), В. Ф. Мелехин (RU). – № 174640/25–08; заявл. 14.06.2017; опубл. 24.10.2017, Бюл. № 30. – 7 с.

A Method for Organizing the Soft Error Tolerant Moore Finite State Machine

I.V. Egorov

Peter the Great St. Petersburg Polytechnic University, Saint-Petersburg, ig-ego@mail.ru

***Abstract* — up-to-date design rules used in computer engineering make hardware unreliable when working under radiation. A hit of a charged particle causes a "soft failure" - a situation, when hardware elements remain in usable condition but the information transmitted or stored in memory is corrupted. This problem appeared after the introduction of nanotechnology in production of integrated circuits. With old submicron technologies, soft failures occurred much less frequently, because false impulses caused by charged particles were invisible due to the inertia of the logic elements. Now we need to develop new circuitry solutions, which would increase the resistance of hardware (especially of the finite states machines) to soft failures. Known research revealed, that soft failures occur more often in memory units, than in combinational circuits, and can be eliminated by the periodic recovery of the memory state. In spite of this, the most of known reliable structures of finite state machines are based on structural redundancy, which is not enough efficient in case of soft failures, and don't use self-recovery for memory units. *Purpose*: suggest new technical solutions to increase the reliability of a Moore automaton working in case of periodic soft failures. *Results:* the developed structure of Moore automaton with triple redundancy of internal memory and output signals and with self-recovery on each synchronization clock period has increased resistance to the soft errors occurred both in combinational circuits and internal memory. This structure also contains the tools to register a count of soft failures occurred during exploitation, which allow to control the state of the automaton and detect the dangerous state, when soft failures occur too often. The reliability characteristic of the developed structure has been estimated. The reliability analysis has revealed the advantage of the developed structure against known fault-tolerant structures of the Moore automaton - in case of periodic soft failures it's operating time to failure is greater by an order of magnitude.**

***Keywords* — finite state machine, combinational circuit, reliability analysis, synchronization, soft failures, structural redundancy, recoverable systems, probability of non-failure.**

REFERENCES

[1] Egorov I.V., Melekhin V.F. Analiz problemy povyshenija radiacionnoj stojkosti informacionno-upravljajushhih sistem na jetape funkcional'no-logicheskogo proektirovanija (Analysis of Radiation Resistance Improvement Issue for Information and Control Systems at the Stage of Functional and Logical Design) // Informacionno-upravljajushhie sistemy. 2016. № 1(80). S. 26–31.

[2] Edmonds D.L., Barnes C.E., Scheick L.Z. An introduction to space radiation effects on microelectronics. Pasadena, USA: NASA, Jet propulsion laboratory, California institute of technology, 2000.

[3] Schwank J.R., Shaneyfelt M.R., Dodd P.E. Radiation hardness assurance testing of microelectronic devices and integrated circuits: Test guideline for proton and heavy ion single-event effects // IEEE Transactions on Nuclear Science. 2013. Vol. 60, № 3. P. 2101–2118.

[4] Amusan O.A. et al. Single event upsets in deep-submicrometer technologies due to charge sharing // IEEE Transactions on Device and Materials Reliability. 2008. Vol. 8, № 3. P. 582–589.

[5] Koons H.C. et. al The impact of the space environment on space systems // 6th Spacecraft Charging Technology. 1998. P. 7–11.

[6] Maksimenko S.L., Melehin V.F., Filippov A.S. Analiz problemy postroenija radiacionno-stojkih informacionno-upravljajushhih sistem (Analysis of the Problem of Radiation-Tolerant Information and Control-Systems Implementation) // Informacionno-upravljajushhie sistemy. 2012. № 2(57). S. 18–25.

[7] Oliveira R., Jagirdar A., Chakraborty T.J. A TMR Scheme for SEU Mitigation in Scan Flip-Flops. IEEE, 2007. P. 905–910.

[8] Egorov I.V., Melekhin V.F. Analiz pokazatelej nadezhnosti i slozhnosti realizacii razlichnyh variantov struktur avtomata s pamjat'ju pri potoke mjagkih otkazov (Analysis of Reliability and Complexity Characteristics for Various Structures of a Finite State Machine Working in Case of Soft-Failure Flow) // Informacionno-upravljajushhie sistemy. 2017. № 3(88). S. 34–46.

[9] Glukhih M.I. Razrabotka metodov sinteza informacionno-upravljajushhih sistem special'nogo naznachenija so strukturnym rezervirovanie: dis. ... kand. tehn. nauk. (Development of methods of synthesis of information and control systems of a special purpose with structural redundancy: PhD thesis) Saint-Petersburg, 2006.

[10] Abraham J.A., Siewiorek D.P. An algorithm for the accurate reliability evaluation of triple modular redundancy networks // IEEE Transactions on Computers. 1974. Vol. C–23(7). P. 682–692.

[11] Maksimenko S.L., Melehin V.F. Analiz nadezhnosti funkcional'nyh uzlov cifrovyh SBIS so strukturnym rezervirovaniem i periodicheskim vosstanovleniem rabotosposobnogo sostojanija (Analysis of Reliability of Functional Nodes of Digital VLSI Circuits with Structural Redundancy and Periodic Operational State Recovery) // Informacionno-Upravljajushhie Sistemy. 2013. № 2(63). S. 18–23.

[12] Egorov I.V., Melekhin V.F. Analiz processov v konechnom avtomate pri vozdejstvii radiacii. Ocenka verojatnosti iskazhenija informacii (Analysis of Processes in a Finite State Machine under Radiation. Probabilistic Assessment of Information Distortion) // Informacionno-upravljajushhie sistemy. 2016. № 3 (82). S. 24–33.

[13] Kaeslin H. Digital integrated circuit design. from vlsi architectures to cmos fabrication / H. Kaeslin, Cambridge University Press, 2008. 879 p.

[14] Pat. 174640 RU, MPK G06F 11/07 (2006.01). Otkazoustojchivyj cifrovoj preobrazovatel' informacii dlja upravlenija diskretnymi processami (The failure-safe information digitizer for management of discrete processes) / I. V. Egorov (RU), V. F. Melehin (RU). – № 174640/25–08; zajavl. 14.06.2017; opubl. 24.10.2017, Bjul. № 30. – 7 s.