УДК 681.3

АНАЛИЗ НАДЕЖНОСТИ ФУНКЦИОНАЛЬНЫХ УЗЛОВ ЦИФРОВЫХ СБИС СО СТРУКТУРНЫМ РЕЗЕРВИРОВАНИЕМ И ПЕРИОДИЧЕСКИМ ВОССТАНОВЛЕНИЕМ РАБОТОСПОСОБНОГО СОСТОЯНИЯ

С. Л. Максименко,
старший преподаватель
В. Ф. Мелехин,
доктор техн. наук, профессор
Санкт-Петербургский государственный политехнический университет

Проводится анализ влияния радиационных воздействий на цифровые устройства со структурным резервированием на уровне функциональных узлов интегральных схем в составе информационно-управляющих систем. Предлагается математическая модель, позволяющая оценить надежность узла, представленного на уровне регистровых передач, с учетом цикличности вычислительных процессов и периодического восстановления информации при сбоях в элементах. Показано, что при организации цикличности работы узлов с периодическим восстановлением информации достигается существенное улучшение показателей надежности.

Ключевые слова *— информационно-управляющие системы, радиационные эффекты, интегральные схемы, сбои, отказы, восстановление, надежность, модель, структура, троирование, мажоритар.*

Введение

В работе [1] проведен анализ радиационных эффектов в полупроводниковых структурах и их влияния на информационные процессы в цифровых устройствах. Обоснована актуальность повышения радиационной стойкости за счет соответствующей функциональной организации устройств и организации периодических процессов восстановления информации в случаях сбоев.

Сбои (восстанавливаемые отказы) вызываются попаданием одиночных частиц высоких энергий (Single Event Effects — SEE). Попадание частицы в триггер может вызвать информационный отказ триггера (Single Event Upset — SEU), т. е. искажение хранящейся информации. Информационный отказ является устранимым (soft error), поскольку может быть исправлен записью правильной информации в пораженный элемент. Попадание отдельной частицы в логический вентиль комбинационной схемы может привести к появлению сбоя в виде «иголки» на его выходе (этот эффект носит название Single Event Transient — SET). Распространяясь по цепочке элементов, такой импульс может привести к нежелательной смене состояния триггеров.

Основными методами борьбы с информационными отказами являются структурное резервирование (троирование и мажорирование), введение информационной избыточности (помехоустойчивое кодирование), использование временной избыточности (повторное выполнение операций). Информационная и временная избыточность преимущественно используются в запоминающих устройствах и системах передачи данных. Троирование и мажорирование применяют для устройств преобразования информации, которые можно представить композицией операционных и управляющих автоматов.

В данной работе рассматриваются задачи повышения надежности устройств преобразования информации.

Важным вопросом при проектировании системы является выбор уровня резервирования. Резервирование на уровне отдельных комбинаторных и запоминающих элементов [1] имеет ряд недостатков: ограничение по энергии частиц, невозможность фиксировать факт отказа (например, для выявления неустранимых отказов или получения информации о приближении к пороговой дозе), наибольшее влияние на быстродействие си-

стемы (необходимость использовать элементы с внутренней избыточностью на критических цепях). Резервирование на уровне готовых сложных функциональных узлов (IP-ядер) имеет другой недостаток: восстановление информации в таком узле обычно требует остановки вычислений. Возможность временной остановки работы отдельных узлов должна быть поддержана архитектурой устройства. Для реализации обоих вариантов, как правило, необходима еще и глубокая переработка схемы узла, сводящаяся к внедрению в нее цепей, реализующих восстановление.

Чем ниже уровень резервирования узлов, тем проще становится восстановление узла при информационном отказе. С другой стороны, при понижении уровня резервирования увеличивается количество контролируемых узлов, суммарная сложность средств контроля и восстановления возрастает. Повышается также сложность системы учета частоты отказов.

Процессы в узлах информационно-управляющей системы носят циклический характер. Каждый цикл работы узла связан с получением новой информации для обработки и выдачей результатов. Результаты работы на предыдущем цикле, как правило, не важны. В противном случае устройство, хранящее предыдущие результаты, можно рассматривать как отдельный узел со своей цикличностью. Таким образом, на каждом цикле происходит восстановление информации в узле без необходимости его останова. Обычно чем ниже уровень иерархии узла, тем короче цикл его работы (поскольку проще выполняемая операция) и тем чаще происходит восстановление информации.

Отказ одного из запоминающих элементов узла не обязательно сразу приводит к выдаче узлом неправильного результата. Отказ может проявиться через некоторое время. Чем выше длительность цикла работы узла, тем дольше узел может проработать до обнаружения отказа. За это время может возникнуть отказ в другом экземпляре узла, что приведет к аварии системы в целом.

Правильный выбор уровня резервирования требует учета цикличности процессов в системе. Для этого необходимо построить математическую модель, позволяющую связать эффекты радиационного воздействия на отдельные вентили с параметрами надежности системы при заданном уровне резервирования и известных параметрах цикличности.

Для СБИС со сложным поведением (например, для микропроцессоров) характерны латентность проявления отказов, невозможность по их проявлению определить первоисточник отказа (например, оценить влияния SET на общее количество отказов), что делает крайне сложным получение оценки устойчивости СБИС в физическом эксперименте.

В целях получения экспериментальных данных по устойчивости отдельных элементов разрабатывают специальные интегральные схемы, обладающие высокой наблюдаемостью, такие как сдвигающий регистр с дополнительными цепочками инверторов [2].

Перенос результатов физических экспериментов над отдельными элементами на СБИС со структурным резервированием требует применения соответствующей математической модели СБИС. Современная СБИС обработки информации — это сложная система, которую можно представить в виде сети функциональных узлов. В данной работе рассматривается модель функционального узла. Расширение модели узла до уровня системы требует дополнительного рассмотрения.

Построение параметризируемой модели узла

Обоснование способа абстрактного представления узла, не связанного с его функциональностью

Основной целью построения модели является анализ надежности узла при выбранном варианте резервирования и восстановления для заданной библиотеки элементов. Поэтому можно исключить рассмотрение процессов внутри элемента, считая, что интенсивность отказов элементов известна (например, из физических экспериментов над элементами).

В соответствии с разделением эффектов SET и SEU [1] будем рассматривать узел как сеть регистров, связанных комбинаторными преобразователями. Триггеры, составляющие регистры, подвержены отказам типа SEU. Комбинаторные элементы подвержены сбоям типа SET, которые, распространяясь, могут привести к формированию неверных сигналов на «информационных» входах триггеров в момент записи или к появлению «ложных» импульсов в цепях управления (асинхронных установок и тактирования).

Критерий исправности узла определяем следующим образом: узел исправен, если формирует выходные сигналы, соответствующие спецификации.

Из-за своей малой длительности импульсы, порожденные SET, не могут непосредственно привести к сбоям на внешних выводах устройства (высокоскоростные интерфейсы типа LVDS, SSTL и т. п. рассматривать не будем). Поэтому к отказу может привести только ситуация, когда некоторые запоминающие элементы хранят неверные значения.

Сам по себе информационный отказ элемента не является отказом устройства. Отказ произой-

дет, только если неверное значение распространится до выхода устройства.

Информационный отказ не приведет к отказу устройства, если значение пораженного элемента памяти не влияет на формирование выходов и на вычисление новых значений других элементов памяти. Это возможно, например, когда к некоторому адресуемому регистру не обращаются либо когда информационный отказ не влияет на функцию перехода автомата. Понятно, что данная ситуация не может продолжаться бесконечно долго, иначе данный элемент памяти просто не используется в устройстве.

В общем случае чтобы определить, влияет ли значение элемента памяти на другие элементы, необходимо проанализировать все логические функции, их связывающие. Будем рассматривать худший случай, считая, что любой узел — это автомат с памятью, и сбой в элементе памяти — это изменение состояния автомата, что неизбежно приводит к отказу всего узла.

Приняв это предположение, мы избавляемся от необходимости рассматривать отдельные комбинаторные преобразователи внутри узла. Можно рассматривать все комбинаторные преобразователи как один блок, являющийся источником потока сбоев, некоторая известная доля которых будет запомнена в триггерах и приведет к отказу узла.

Выходные комбинаторные преобразователи не могут повлиять на отказ своего узла. Однако они могут привести к отказу других узлов, подключенных к нему по входу. Если учесть, что в системе со структурным резервированием различные узлы связаны между собой только через мажоритары (узлы, блокирующие распространение отказа), то для запоминания сбоя, порожденного в выходных преобразователях, должно наступить одно из двух событий:

— одновременно происходят два сбоя на одном выходе в разных экземплярах узла;

— сбой происходит одновременно с отказом другого экземпляра узла.

Первое событие является крайне маловероятным, второе — более вероятно. Кроме того, если сбой будет пропущен мажоритаром, он приведет к отказу всех экземпляров узла-приемника, т. е. к отказу системы. (Если мажоритар троирован, его экземпляры, скорее всего, среагируют одинаково.) Таким образом, сбой проявится так же, как если бы отказал второй узел в тройке.

Из изложенного следует, что выходные формирователи влияют на исправность системы так же, как внутренние, но только когда один из экземпляров узла отказал. Если считать, что доля времени, когда один из узлов отказал, мала, то учитывать сбои в выходных преобразователях не требуется. Это справедливо для узлов с периодическим восстановлением их исправного состояния. Если же рассматривать поведение системы при невосстановимых отказах, такой учет требуется.

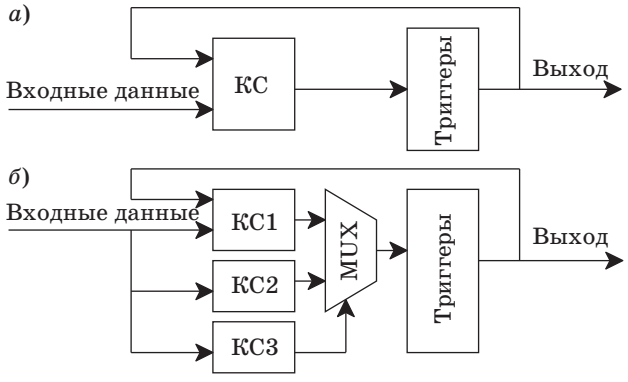
При разбиении схемы на узлы для последующего резервирования лучше размещать комбинаторные преобразователи на выходе узла.

Структурная модель узла

Будем рассматривать узел как автомат с памятью, состоящий из комбинационной схемы *КС* и триггеров (рис. 1, *а*). На входы КС поступают входные данные и выходные сигналы триггеров. Автомат работает в двух режимах: в рабочем режиме, когда автомат перерабатывает входные последовательности (данные) в выходные; в режиме сброса или предустановки, когда КС воспринимает только внешние входные сигналы и ее выходы не зависят от выходов триггеров. Не обязательно среди входов узла есть сигнал, напрямую определяющий загрузку входных данных в регистры. Режим загрузки может активироваться при некоторых комбинациях входных данных, при этом в регистры могут заноситься не сами входные данные, а результаты вычисления некоторой функции над ними.

Для анализа работы узла во всех режимах рассмотрим рис. 1, *б*. На нем комбинационные преобразователи в составе узла представлены в виде трех комбинационных схем: *КС*1 реализует преобразование информации в рабочем режиме, *КС*2 — преобразование входной информации при загрузке, а *КС*3 — активацию режима загрузки. Выходной комбинационный преобразователь, реализующий функцию выхода автомата, на рис. 1 не приведен по причинам, изложенным выше.

Узел, реализующий конвейерную обработку данных, не может быть непосредственно описан схемой, представленной на рис. 1, поскольку загрузка данных выполняется только на первой



■ ***Рис. 1.*** Структурная модель узла: *а* — как автомата с памятью; *б* — с периодической загрузкой информации

ступени. Если данные поступают на вход первой ступени, каждый такт и есть k ступеней, вся информация, относящаяся к одному входному набору данных, остается в конвейере k тактов, но в каждой ступени она хранится только один такт. Поэтому для оценки надежности при информационном отказе конвейеризованный узел может быть представлен узлом со схемой, рассмотренной на рис. 1, *а*, у которого загрузка выполняется каждый такт.

В каждом триггере поток информационных отказов — пуассоновский [1] с интенсивностью λ_T [3]. Будем считать, что искаженное значение состояния хотя бы одного триггера приводит к неверному состоянию триггеров на следующем такте, и этот отказ не устраняется до момента записи нового значения с входов узла (а при записи он устраняется, если в момент записи не возникнет сбой в КС).

Комбинационная схема порождает сбои, которые могут быть запомнены триггерами. Запоминание конкретного сбоя имеет случайный характер, причем вероятность запоминания зависит как от параметров импульса сбоя, так и от свойств и условий работы триггера. Принимая, что ложные импульсы от эффекта SET могут распространяться по цепочкам логических элементов на существенное расстояние, можно считать, что для фиксированных условий количество сбоев на выходе КС пропорционально занимаемой ею площади на кристалле, т. е. количеству логических элементов.

Для конкретной элементной базы и условий работы узла путем моделирования [4] либо экспериментально [2, 5] можно определить, какая доля сбоев запоминается. В дальнейшем можно учитывать только такие «запоминаемые» сбои, считая, что интенсивность сбоев на выходе КС связана с количеством ее элементов некоторым коэффициентом, фиксированным для конкретной задачи анализа: $\lambda_{КС} = kN_{л.э}$.

Поскольку отказ в любом триггере или «запоминаемый» сбой в любом логическом элементе в нашей модели приводят к информационному отказу узла, вероятность его безотказной работы на одном цикле выполнения операции можно оценить как $P(t) = e^{-(N_T\lambda_T + kN_{л.э})t}$.

Причиной отказа узла могут быть неверные данные, поступившие со входа. Мажоритар, подверженный импульсам SET, может стать причиной информационных отказов в подключенных к нему узлах, если сбой в мажоритаре будет далее запомнен. Как и с КС внутри узла, вероятность запоминания сбоя зависит от многих факторов. Будем считать, что мы можем оценить эту вероятность, и будем учитывать только те сбои на выходе мажоритаров, которые будут запомнены узлами, т. е. введем поправочный коэффициент. Тогда интенсивность потока «запоминаемых» сбоев на выходе мажоритара можно оценить величиной, пропорциональной количеству логических элементов в мажоритаре, как $\lambda_{маж} = kN_{л.э\_маж}$.

Количество элементов в мажоритаре пропорционально его разрядности и зависит от типа мажоритара (побитный или пословный, с формированием признака ошибки или без).

Как сказано выше, восстановление информации в узле происходит за счет загрузки в него правильной информации. Для того чтобы на вход узла поступала правильная информация, отказы в узлах-источниках должны отсутствовать или быть блокированными. Если блокирующий узел (мажоритар) отсутствует, то узел-источник и узел-приемник можно рассматривать как один узел с конвейерной структурой (с соответствующим периодом обновления информации). Поэтому будем считать, что узлы в устройстве соединены только через мажоритары.

Далее будем рассматривать системы, для которых интенсивности возникновения отказов в узлах и мажоритарах известны (т. е. они войдут в формулы для расчета надежности как параметры).

Оценка надежности отдельного узла с троированным мажоритаром

Рассмотрим систему (рис. 2), которая состоит из троированного узла M (module) и троированного мажоритара V (voter). Пусть интенсивность потока отказов узла составляет λ_m, а интенсивность потока отказа мажоритара — λ_v.

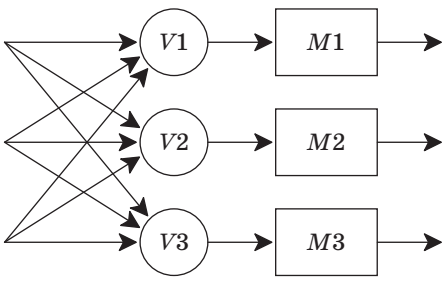
Зададим схему событий, позволяющую оценивать исправность работы системы. Будем считать, что:

— система исправна, если хотя бы два из трех экземпляров узла M выдают правильное значение;

— узел выдает правильное значение тогда и только тогда, когда он сам исправен и на его вход поступают правильные данные;

— мажоритар выдает правильное значение тогда и только тогда, когда он сам исправен и хотя бы на два его входа поступают правильные данные.

Вероятность исправности узла в некоторый момент времени t составляет $P_m(t) = e^{-\lambda_m t}$.



■ ***Рис. 2.*** Троированный узел с троированным мажоритаром

Вероятность исправности мажоритара

$$P_v(t) = e^{-\lambda_v t}.$$

Нетрудно показать для приведенной схемы событий, что вероятность исправности системы

$$P(t) = 3P_s(t)^2 - 2P_s(t)^3,$$

где $P_s(t) = P_m(t) \cdot P_v(t)$. Выражая вероятность исправного состояния системы через $\lambda_s = \lambda_m + \lambda_v$, получим $P_s(t) = 3e^{-2\lambda_s t} - 2e^{-3\lambda_s t}$.

Рассмотрим теперь систему, у которой информация в узлах восстанавливается в начале каждого интервала длительностью t_R. Восстановление происходит за счет цикличности работы узла.

Очевидно, что восстановление произойдет только в том случае, если в момент восстановления на узел поступает правильная информация с соответствующего мажоритара. Физическая природа отказов мажоритара (проявляющихся как «иголки» на его выходе) позволяет следующим образом учитывать их при анализе: отказ мажоритара, возникший во время восстановления, мы заменяем отказом, возникшим «сразу после» восстановления, что по влиянию на работу системы эквивалентно.

Оценим вероятность исправности системы в момент $T = Nt_R$. Поскольку возникновение отказа на некотором цикле восстановления не зависит от отказов на предыдущем цикле, $P(T) = P(t_R)^N$.

Для рассматриваемых класса систем и природы отказов $\lambda_S t_R << 1$, при этом N очень велико, и вычислить $P(T)$ напрямую невозможно из-за ограничения точности представления чисел в ЭВМ.

Воспользовавшись тем, что $\lambda_S t_R << 1$, построим приближенную оценку $P(T)$:

$$P(T) = P(t_R)^N = e^{\ln(P(t_R))N};$$

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

При $|x| < H$ остаточный член $\gamma_n(x) < \frac{e^H}{(n+1)!} x^{n+1}$. Тогда

$$P_s(t_R) = 3e^{-2\lambda_s t_R} - 6e^{-3\lambda_s t_R} = 3 - 6\lambda_s t_R + 6(\lambda_s t_R)^2 -$$
$$- 2 + 6\lambda_s t_R - 9(\lambda_s t_R)^2 + O((\lambda_s t_R)^3) \approx 1 - 3(\lambda_s t_R)^2.$$

Если ограничиться степенью 2 в разложении, то погрешность оценки не превысит

$$3\frac{e^H}{6} \cdot 8(\lambda_s t_R)^3 + 2\frac{e^H}{6} \cdot 27(\lambda_s t_R)^3 = 13e^H(\lambda_s t_R)^3.$$

При $\lambda_s t_R < 0{,}001$ погрешность меньше $14(\lambda_s t_R)^3$.

Воспользуемся разложением функции ln в степенной ряд: $\ln(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} x^n}{n}$. Обозначив $\lambda_s t_R$ через x и учитывая, что q мало, оставим только первый член ряда: $\ln(1 + x) \approx x$. При этом погрешность составит менее $x^2/2$. Тогда

$$P(T) = e^{\ln(1-3(\lambda_s t_R)^2)N} \approx e^{-3\lambda_s^2 t_R^2 \cdot T/t_R} = e^{-3\lambda_s^2 t_R T} \quad (1)$$

и систему можно рассматривать как элемент с простейшим потоком отказов с интенсивностью $3\lambda_s^2 t_R$.

Выражение (1) показывает, что интенсивность потока отказов прямо пропорциональна периоду восстановления информации.

На основании этого можно сделать вывод, что при определении уровня резервирования и декомпозиции системы на резервируемые узлы необходимо учитывать период восстановления информации в каждом узле и стремиться минимизировать этот период.

При $a, b > 0$ $(a + b)^2 > a^2 + b^2$. Если считать, что интенсивность потока отказов узла пропорциональна его размеру, и не учитывать влияние отказов в мажоритаре на надежность системы, то из выражения $P(T) = e^{-\left(3\lambda_e^2 t_R\right)T}$ следует, что максимальная надежность достигается при минимальном уровне резервирования.

Минимальный уровень — это отдельные триггеры: каждый триггер троируется, и на вход триггеров поступают данные, вычисленные по результатам мажорирования. Запись в триггеры должна производиться на каждом такте: если алгоритмом работы устройства запись новых данных на некотором такте не предусмотрена, в триггер записывается результат мажорирования старых значений в тройке триггеров (это дополнительный мультиплексор).

Описанный вариант резервирования требует максимального количества мажоритаров, максимально ухудшает быстродействие устройства за счет наличия мажоритаров и мультиплексоров на всех критических путях. Кроме того, из-за максимального количества мажоритаров наиболее сложной становится схема сбора данных об отказах.

Кроме того, известно [6, 7], что при снижении проектной нормы увеличивается вероятность одновременного поражения нескольких близлежащих триггеров, что снижает эффективность резервирования на уровне отдельных триггеров.

Необходимо выбирать оптимальный уровень резервирования с учетом периода восстановления и суммарной сложности мажоритаров.

Для принятия решений в процессе проектирования при рассмотрении различных вариантов резервирования узлов необходимо построить оценку надежности системы как сети из резервированных узлов с различными периодами восстановления.

Заключение

Предложен подход, позволяющий оценить надежность цифровых СБИС к информационным отказам, вызванным радиационными воздействиями, основанный на анализе цикличности функционирования узлов. В рамках данного подхода предлагается рассматривать устройство как сеть из групп резервированных узлов, соединенных через мажоритары. В каждом узле выделяются регистровая и комбинаторная составляющие. Обосновывается выбор параметров для оценки надежности этих составляющих. Для предложенной структурной модели получена оценка зависимости вероятности безотказной работы резервированного узла от периода восстановления информации. Полученная оценка показывает, что организация циклической работы резервированного узла в составе системы существенно повышает показатели надежности. Результат при учете параметров мажоритаров, связывающих узлы, может быть обобщен на устройство (систему) в целом. Многократное восстановление после информационных отказов за время наработки на невосстанавливаемый отказ устройства позволяет организовать ведение статистики информационных отказов и определить приближение к неустранимому отказу из-за накопления изменений в полупроводниковой структуре.

Литература

1. **Максименко С. Л., Мелехин В. Ф., Филиппов А. С.** Анализ проблемы построения радиационно-стойких информационно-управляющих систем // Информационно-управляющие системы. 2012. № 2. С. 18–25.
2. **Hass K. J., Ambles J. W.** Single Event Transients in Deep Submicron CMOS // 42nd Midwest Symp. on Circuits and Systems. 2000. Vol. 1. P. 122–125.
3. **Глухих М. И., Максименко С. Л., Мелехин В. Ф., Филиппов А. С.** Организация и проектирование высоконадежных вычислительных систем // Научно-технические ведомости СПбГПУ. 2011. № 6.1(138). С. 54–61.
4. **Rao R. R., Chopra K., Blaauw D. T., Sylvester D. M.** Computing the Soft Error Rate of a Combinational Logic Circuit Using Parameterized Descriptors // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 2006. Vol. 26. N. 3. P. 468–479.
5. **Benedetto J. M.** et al. Variation of Digital SET Pulse Widths and the Implications for Single Event Hardening of Advanced CMOS Processes // IEEE Transactions on Nuclear Science. 2005. Vol. 52. P. 2114–2119.
6. **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. N 3. P. 582–589.
7. **Haghi M., Draper J.** The 90 nm Double-DICE storage element to reduce Single-Event upsets // IEEE Intern. Midwest Symp. on Circuits and Systems. 2009. P. 463–466.