УДК 681.3
doi:10.15217/issn1684-8853.2016.2.26

МЕТОДЫ И СРЕДСТВА АНАЛИЗА НАДЕЖНОСТИ СТРУКТУРНЫХ БЛОКОВ С РЕЗЕРВИРОВАНИЕМ И ПЕРИОДИЧЕСКИМ ВОССТАНОВЛЕНИЕМ ИНФОРМАЦИИ НА РАЗЛИЧНЫХ ЭТАПАХ ПРОЕКТИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

И. В. Егоров[a], *аспирант*
В. Ф. Мелехин[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, РФ*

Постановка проблемы: *проектирование отказоустойчивых вычислительных систем, работающих в условиях повышенной радиации, требует оценки влияния сбоев, заключающихся в искажении информации при попадании заряженной частицы. Средства анализа надежности таких систем должны учитывать возникновение таких сбоев, а также моделировать влияние средств периодического восстановления искаженной информации, применяемых для повышения характеристик надежности.* ***Цель:*** *определение границ применимости методов анализа надежности, основанных на использовании аналитических и имитационных моделей, для оценки надежности систем с периодическим восстановлением; сравнение результатов анализа показателей надежности восстанавливаемой системы, полученных с помощью аналитической и имитационной моделей.* ***Результаты:*** *с помощью аналитической и имитационной моделей произведен расчет и анализ времени наработки восстанавливаемой системы до отказа. Выявлено, что наличие детерминированных процессов восстановления ограничивает применимость традиционных методов оценки надежности, таких как построение марковской модели и логико-вероятностные методы. Определена необходимость учета влияния программного обеспечения при проектировании систем с периодическим восстановлением.* ***Практическая значимость:*** *благодаря проведенным исследованиям определены области применения моделей надежности разного вида на различных этапах проектирования отказоустойчивых восстанавливаемых вычислительных систем.*

Ключевые слова *— имитационное моделирование, надежность восстанавливаемых систем, радиационно-стойкая вычислительная система, марковская модель, структурное резервирование, информационная избыточность.*

Введение

Из работ, посвященных исследованию влияния радиации на полупроводниковые структуры [1–3], известно, что попадание заряженных частиц наиболее часто приводит к появлению ложных импульсов на выходах логических элементов и сохранению искаженной информации в триггерах, иными словами, к возникновению «мягких» (информационных) отказов. При этом аппаратура продолжает находиться в работоспособном состоянии, а это значит, что за счет имеющейся временной избыточности и специальной организации вычислительного процесса можно обеспечить периодическое восстановление поврежденной информации и возвратить уровень работоспособности устройства к начальному состоянию.

Статистические исследования [4] показывают, что полное разрушение структуры полупроводника, которое влечет окончательный выход элементов вычислительной системы (ВС) из строя, происходит в сотни раз реже «мягких» отказов. Это меняет взгляд на организацию проектирования отказоустойчивых систем, поскольку распространенные в традиционных подходах методы структурного резервирования, используемые при борьбе с невосстанавливаемыми отказами, должны быть дополнены средствами периодического восстановления поврежденной информации, что существенно повысит надежность системы. Такой подход приводит к новым архитектурным решениям.

В работах [5, 6] предложен подход к проектированию ВС, основанный на представлении системы в виде сети функциональных блоков (конечного автомата с памятью или модуля памяти), внутри которых реализуются средства защиты от «мягких» отказов путем периодического восстановления информации с помощью структурного резервирования для конечных автоматов и использования корректирующих кодов с исправлением ошибок для блоков памяти.

Организация восстановления влечет за собой новые требования к анализу надежности и к моделям надежности. Аналитические модели, основанные на вероятностной оценке возникновения отказов, применимы для случаев, когда среднее время между двумя «мягкими» отказами значительно меньше периода восстановления информации. При недостаточной временной избыточности в системе эти ограничения могут не выполняться. В такой ситуации требуются модели надежности, учитывающие регулярные процессы

восстановления и влияние логики программного обеспечения на процессы в системе. Этим обосновано применение метода оценки, базирующегося на программной имитации процессов, протекающих в системе (таких как возникновение отказов, восстановление информации, действие вычислительного процесса и т. д.), т. е. имитационных моделей.

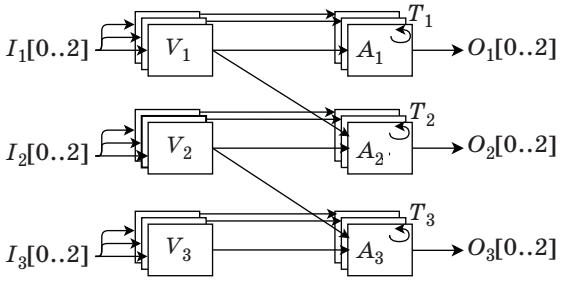
В настоящей работе предлагается реализация имитационной модели надежности, позволяющей учитывать влияние процессов восстановления на работоспособность системы. С помощью данной имитационной модели производится оценка системы со структурной избыточностью и восстановлением.

Объект исследования

Для иллюстрации использования аналитических и имитационной моделей оценим структурную надежность фрагмента структуры (рис. 1).

Представленная структура является частным случаем обобщенной структуры (см. рис. 2), используемой при проектировании отказоустойчивых ВС, основанном на разбиении системы на независимые блоки с периодическим восстановлением работоспособного состояния блока [7]. Такое построение структуры обосновано для невосстанавливаемых систем и соответствует «доменной» организации, допускающей масштабирование уровня резервирования. Структура обеспечивает блокирование распространения отказов за пределы блока как для невосстанавливаемых, так и для «мягких» отказов.

Выбор этой структуры обусловлен также тем, что именно для нее в работе [8] получена аналитическая модель расчета показателей надежности с учетом периодического восстановления «мягких» отказов. С этой аналитической моделью будем сравнивать расчеты на имитационной модели. Вопрос о целесообразности модификации структуры применительно к случаю превалирования мягких отказов требует отдельного рассмотрения.



■ ***Рис. 1.*** Исследуемый фрагмент структуры: I_1, I_2, I_3 — входные данные; V_1, V_2, V_3 — группы троированных мажоритаров; A_1, A_2, A_3 — группы троированных блоков типа «конечный автомат с памятью» с периодическим восстановлением (каждая тройка блоков имеет свой собственный период восстановления T_1, T_2, T_3); O_1, O_2, O_3 — выходы троированных блоков

Если в каком-либо блоке произошел один отказ за период восстановления, он никак не скажется на функционировании других, связанных с его выходами, блоков благодаря мажоритарам, расположенным на их входах.

Система считается работоспособной, если на каждом из выходов O_1, O_2, O_3 выставлены корректные данные. Это условие выполняется, если на выходе каждого блока присутствует не более одного искаженного сигнала из трех.

На примере из рис. 1 продемонстрируем расчет интенсивности потока отказов на выходах O_1, O_2, O_3 в зависимости от интенсивности восстановления информации в блоках $A_N = \lambda_{rn}$ при заданных значениях:

— интенсивность собственных отказов каждого экземпляра в тройке блоков $A_N = \lambda_n$;

— интенсивность собственных отказов каждого мажоритара в тройке $V_N = \delta_n$.

Подходы к аналитическому расчету

Аналитическая оценка данной системы может быть произведена одним из следующих методов:

— комбинаторной оценкой возникновения различных комбинаций отказов в блоках и получением аналитической формулы для расчета общей вероятности отказа системы [8];

— построением марковской модели и ее решением [9];

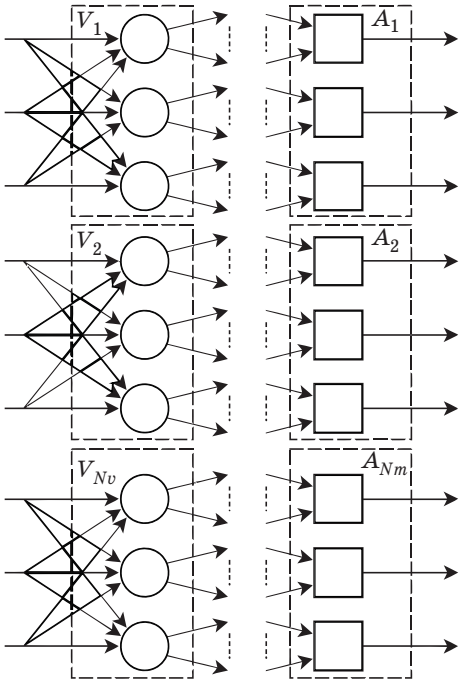
— построением логической функции работоспособного состояния и ее решением логико-вероятностными методами [10, 11].

Комбинаторная оценка

В работе [8] выводится обобщенная формула, оценивающая надежность отказоустойчивой структуры (рис. 2), состоящей из троированных мажоритаров V_i на входе и подключенных к ним троированных периодически восстанавливаемых блоков A_k. Данная структура является обобщением исследуемой (см. рис. 1) с соответствующими наименованиями элементов.

Зависимость интенсивности потока отказов на выходе блока от параметров восстановления определяется по формуле

$$\lambda_s = 3\sum_{j\in 1:N_m}\lambda_j^2 t_{Rj} + 3\sum_{j\in 1:N_v}\delta_j^2 K_j t_{R\_\max(j)} + 6\sum_{j,k\in 1:N_v}\delta_j\delta_k K_{jk} t_{R\_\max(j,k)} + 6\sum_{\substack{i\in 1:N_v \\ j\in \mathrm{out}(i)}}\delta_i\lambda_j t_{Rj}. \quad (1)$$



■ ***Рис. 2***. Обобщенная структура соединений отказоустойчивых блоков

В формуле (1) использованы следующие обозначения:

λ_s — интенсивность отказов на выходах структуры (см. рис. 2);

N_m — количество троированных блоков;

N_v — количество троированных мажоритаров;

K — коэффициент кратности периодов обновления в блоках ($1 \le K \le 2$). При кратных периодах обновления $K = 1$;

out:$V \to 2^M$ — функция, определяющая множество троек узлов, подключенных к выходам заданной тройки мажоритаров;

λ_j — интенсивность собственных отказов экземпляров блока j;

δ_j — интенсивность отказов мажоритара j. Стоит отметить, что эта величина отражает только отказы мажоритаров, оказавшие непосредственное влияние на подключенный к ним блок, т. е. повлекшие изменение состояния памяти блока. При рассмотрении «мягких» отказов необходимо учитывать, что не каждое попадание заряженной частицы в область мажоритара влечет за собой сбой в работе подключенного автомата. Наведенные импульсы, не сохранившиеся в течение всего времени удержания запоминающего элемента, не вызовут запоминания искаженного бита. Также при оценке влияния мажоритаров необходимо учитывать особенности их структуры — как минимум тот факт, что вероятность попадания частицы прямо пропорциональна площади, занимаемой элементом на кристалле, которая для мажоритаров относительно мала. Вышеперечисленные причины уменьшают вероятность отказа системы из-за сбоев в мажоритарах и уменьшают их структурную значимость с точки зрения надежности;

t_{Rj} — период восстановления блока j;

$t_{R\_\max(j,\ k)}$ — максимальный из периодов восстановления блоков j и k.

При получении формулы (1) принимались следующие допущения:

— в элементе в течение периода восстановления возникает не более двух отказов (предположение о наличии достаточного резерва времени для обеспечения нужной интенсивности регулярного восстановления);

— отсутствуют невосстанавливаемые отказы.

Один из основных выводов, полученных из формулы (1): интенсивность отказов на выходе троированных блоков находится в прямой линейной зависимости от периода восстановления блоков.

Марковская модель

При проведении комбинаторной оценки приходится ограничивать количество рассматриваемых событий, возникающих за период восстановления, чтобы сократить количество анализируемых комбинаций и упростить тем самым итоговое выражение. Этого ограничения можно избежать, если выделить все возможные состояния системы (полностью работоспособное и состояния с частичной деградацией в результате отказов экземпляров блоков и мажоритаров) и представить систему в виде марковской модели. В этом случае можно получить точный результат путем решения системы алгебраических уравнений Чепмена — Колмогорова [9].

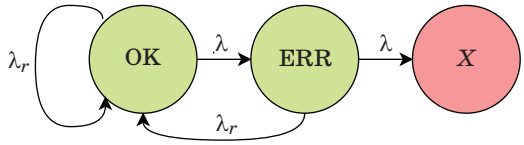
Однако марковская модель накладывает ограничения следующего рода:

— величины интервалов времени между отказами и периодов между восстановлениями подчиняются экспоненциальному закону распределения случайной величины;

— рост сложности системы ведет к резкому увеличению числа состояний, что приводит к усложнению системы уравнений и ее решения.

Первое ограничение значительно затрудняет анализ систем с детерминированным восстановлением. К примеру, рассмотрим поведение некоторого элемента системы, устойчивого к появлению однократного сбоя за детерминированный период восстановления $T_{\text{восст}} = 1/\lambda_r$. Поток отказов пуассоновский с интенсивностью λ.

Для построения марковской модели такой системы необходимо принять допущение об экспоненциальном законе распределения интервалов между событиями как потока восстановления, так и потока отказов. Модель будет иметь вид, представленный на рис. 3.



■ ***Рис. 3.*** Модель состояний элемента, устойчивого к однократному сбою

Пусть $\lambda_r = 1{,}0$, $\lambda = 0{,}2$. Тогда оценка среднего времени T до перехода в неработоспособное состояние X из полностью работоспособного состояния OK и состояния с частичной деградацией ERR (error) на основании марковской модели дает результат $T = 33{,}78$ (некорректная оценка).

При использовании комбинаторного метода (корректной оценки) необходимо оценить вероятность возникновения двух и более отказов за период восстановления 1,0. Так как поток отказов пуассоновский, эта вероятность приближенно равна $P_o = \sum_{n=2}^{\infty} P(n) = \sum_{n=2}^{\infty} \frac{\lambda^n e^{-\lambda}}{n!} \approx 0{,}018$. Данная величина определяет среднее количество периодов восстановления, прошедших до возникновения первого сбоя, и позволяет оценить среднее время наработки до отказа $T = \frac{T_{\text{восст}}}{P_o} = \frac{1{,}0}{0{,}018} = 55{,}56$.

Расхождение в результатах оценки среднего времени наработки двумя методами иллюстрирует некорректность допущения об экспоненциальном законе распределения периода восстановления, использованного при построении марковской модели (при переходе из состояния в состояние марковская модель «забывает» предысторию перехода и, следовательно, информацию о том, сколько времени осталось до наступления следующего момента восстановления).

Логико-вероятностные методы

Рассмотрение использования логико-вероятностных методов [10, 11] выходит за рамки данной статьи. Лишь отметим, что применение этих методов по сравнению с марковскими моделями зачастую избавляет от трудоемкого построения модели состояний системы, но сохраняет ограничения на закон распределения интенсивностей отказов и восстановлений, характерные для применения марковской модели, а также добавляет требование независимости событий отказов, возникающих в элементах системы.

Применение имитационной модели

Цель применения имитационной модели — получение характеристик надежности для систем, не укладывающихся в ограничения традиционных аналитических моделей.

Для этого на ЭВМ производится моделирование последовательности возникших в системе событий и ее реакций на них (эксперимент). Эксперимент заканчивается при наступлении определенного условия (например, при переходе системы в неработоспособное состояние или по истечении времени моделирования).

В качестве имитационных моделей надежности в различных работах предлагаются либо модели общего назначения (к примеру, сети Петри), либо специализированные, ориентированные на оценку надежности специфических систем [12].

Имитационная модель, предложенная в данной работе, имеет сходства с марковской:

— для ее построения задаются состояния системы, определяемые последовательностью возникших в системе сбоев (состояния частичной деградации);

— между состояниями задаются переходы, главные причины которых — возникновение отказов и событий восстановления. Вес перехода задает интенсивность возникновения данного события.

С другой стороны, имитационная модель расширяет возможности марковских моделей:

1. Интервалы времени между переходами не обязательно подчинены экспоненциальному закону распределения случайной величины. В общем случае имеется возможность выбора закона распределения и параметров функции распределения для данного закона. В частности, может быть задан детерминированный интервал времени, через который осуществляется переход, что полезно для моделирования процессов восстановления.

2. Многие события, возникающие в системе, не зависят от ее текущего состояния. Например, восстановление происходит через фиксированные моменты времени, в каком бы состоянии система не находилась. Такие явления можно задать с помощью генератора глобальных событий (Global Events Generator). Также в модели определяется реакция системы на эти события, которая в общем случае зависит от текущего состояния.

3. Марковская модель требует определения всех возможных состояний системы и переходов между ними. Для системы из рис. 1 требовалось бы выделить отдельное состояние для каждой возможной комбинации отказавших элементов — мажоритаров и блоков. Модель в этом случае содержала бы 22 состояния. При возрастании сложности системы количество ее состояний возрастало бы еще значительнее. Для устранения упомянутого ограничения предлагается представить имитационную модель в виде сети независимых графов состояний, взаимосвязь между которыми обеспечивается путем передачи сигналов (именованных событий) от одного графа

к другому. Такого рода событие порождается графом при возникновении в нем перехода из состояния в состояние. Данное событие может стать причиной перехода между состояниями в других графах. Такой подход позволяет перейти от моделирования сложной системы к моделированию нескольких простых со значительно меньшим количеством состояний.

4. Следствием из п. 3 является то, что работоспособность сети графов задается в виде логической функции (Health Function), зависящей от текущего состояния заданного подмножества графов (непосредственно определяющего работоспособность системы), входящих в состав сети.

Результатом расчета модели является:

— вероятностная функция работоспособности;

— среднее время наработки до отказа;

— оценка погрешности рассчитанных характеристик.

Пример расчета

При расчете системы (см. рис. 1) используются следующие допущения и относительные значения:

— поток отказов в блоках и мажоритарах является пуассоновским;

— отсутствуют невосстанавливаемые отказы в элементах;

— интенсивности отказов всех экземпляров блоков A_1, A_2, A_3 равны $\lambda = \lambda_1 = \lambda_2 = \lambda_3 = 1{,}0$;

— интенсивности отказов всех экземпляров мажоритаров V_1, V_2, V_3 равны $\delta = \delta_1 = \delta_2 = \delta_3 = 0{,}01$;

— период восстановления блоков A_1, A_2, A_3 детерминирован и равен $t_r = 1/\lambda_r$.

Аналитическая оценка комбинаторным методом.

Для аналитической оценки применим формулу (1), которая для данной структуры имеет вид

$$\lambda_s = 3\left(\lambda_1^2 t_r + \lambda_2^2 t_r + \lambda_3^2 t_r\right) + 3\left(\delta_1^2 t_r + \delta_2^2 t_r + \delta_3^2 t_r\right) + 6\left(\delta_1\delta_2 t_r + \delta_2\delta_3 t_r\right) + 6\left(\delta_1\lambda_1 t_r + \delta_1\lambda_2 t_r + \delta_2\lambda_2 t_r + \delta_2\lambda_3 t_r + \delta_3\lambda_3 t_r\right) = 3t_r\left(3\lambda^2 + 7\delta^2 + 10\lambda\delta\right). \quad (2)$$

Формула (2) определяет интенсивность потока отказов исследуемой структуры.

Оценка имитационным моделированием.

Имитационная модель для структуры, представленной на рис. 1, может быть реализована сетью из следующих графов с независимыми состояниями:

V_1, V_2, V_3 — примитивные графы, моделирующие события отказов в соответствующих мажоритарах;

$A_1[1]$, $A_1[2]$, $A_1[3]$ — графы состояний экземпляров троированного блока A_1;

$A_2[1]$, $A_2[2]$, $A_2[3]$ — аналогично для блока A_2;

$A_3[1]$, $A_3[2]$, $A_3[3]$ — аналогично для блока A_3;

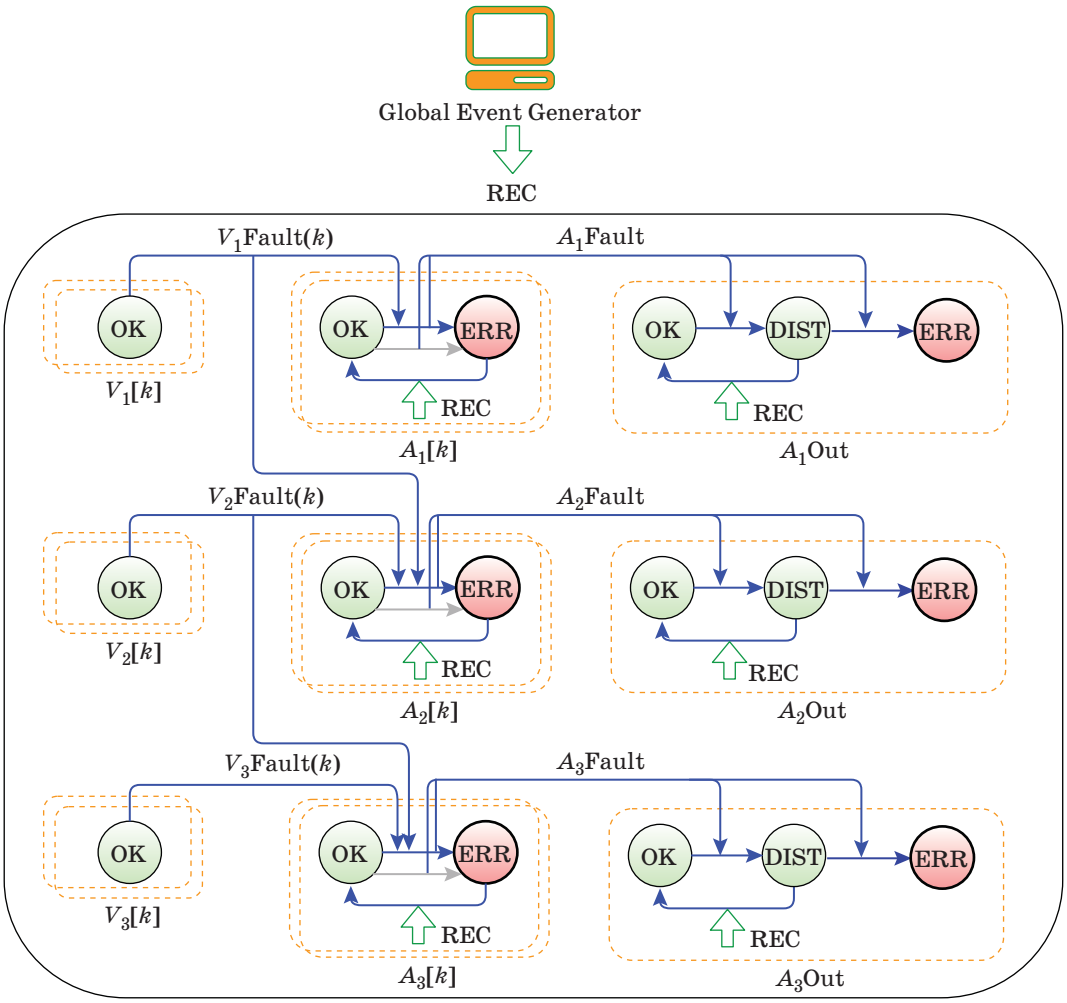
$A_1\mathrm{Out}$, $A_2\mathrm{Out}$, $A_3\mathrm{Out}$ — графы, моделирующие состояние выходных линий блоков O_1, O_2, O_3.

Графическая интерпретация имитационной модели представлена на рис. 4.

Пунктирными линиями на рис. 4 обозначены независимые графы, входящие в состав сети (двойными пунктирными — тройки однотипных графов). Состояния, выделенные тонким контуром, являются работоспособными, жирным — неработоспособными. Если над переходом между состояниями нет названия, он обозначает внутреннее событие в графе. Если переход именованный, он обозначает внешнее событие, передаваемое между графами (стрелка, входящая во внутренний переход, символизирует порождение внутреннего перехода внешним событием). Стрелки, исходящие из перехода, иллюстрируют генерацию внешнего события при возникновении данного перехода. Если стрелка выходит из состояния, значит внутреннего перехода в исходном графе при возникновении события нет. Утолщенные стрелки обозначают воздействие глобального события, порождаемого генератором Global Event Generator независимо от переходов в каком-либо графе (в данном случае — событие восстановления REC (recovery) с постоянным периодом).

Система находится в работоспособном состоянии, если все троированные модули A_1, A_2, A_3 исправны, т. е. на их выходах выставлены корректные сигналы. Другими словами, логическая функция работоспособности системы $\mathrm{HealthFunction} = A_1\mathrm{Out}\ \&\ A_2\mathrm{Out}\ \&\ A_3\mathrm{Out}$.

Рассмотрим принцип функционирования модели на примере блока A_1. Примитивные графы $V_1[1]$, $V_1[2]$, $V_1[3]$ моделируют работу подключенных к модулю мажоритаров, которые являются источниками отказов $\mathrm{V}_1\mathrm{Fault}[k]$, где $k = 1..3$. Как видно из рис. 4, данные отказы влияют на соответствующий граф $A_1[k]$, что переводит его в неработоспособное состояние ERR. Этот переход в свою очередь порождает событие A_1Fault. При этом в графе A_1Out, моделирующем состояние выходной линии тройки модулей A_1, происходит переход в состояние DIST (distortion), свидетельствующее о том, что одна из выходных линий блока A_1 искажена. Отметим, что после этого граф $A_1[k]$, в котором произошел отказ, продолжает хранить неработоспособное состояние ERR и не может быть источником отказов для $\mathrm{A}_1\mathrm{Out}$. Возникновение события восстановления REC, воздействующего на все блоки, переводит в состояние OK как $A_1[k]$, так и A_1Out. Отказ A_1Out произойдет в том случае, если событие A_1Fault возникнет дважды за период восстановления, другими словами, если два различных экземпляра блока A_1 перейдут в неработоспособное состояние



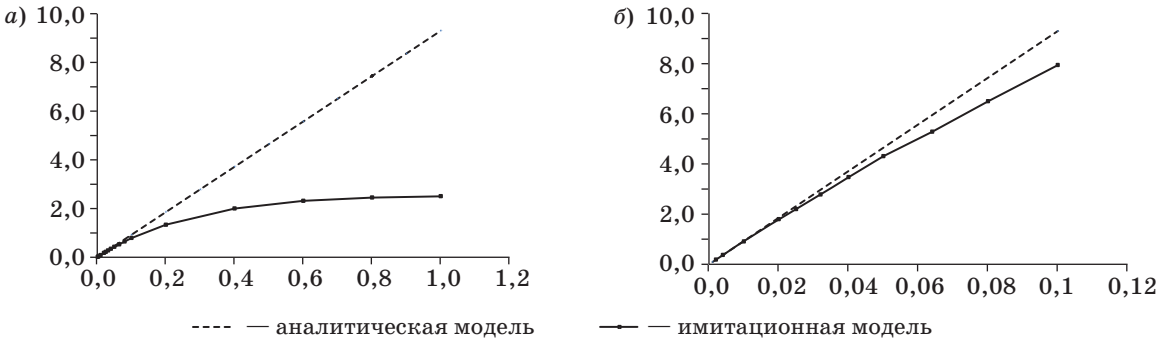
■ ***Рис. 4.*** Графическая интерпретация имитационной модели исследуемой системы

■ Описание графов состояний сети, моделирующей анализируемую структуру

Граф	Состояния	Переходы
$V_n[k]$ $n = 1..3$ — номер тройки мажоритаров $k = 1..3$ — номер экземпляра в тройке мажоритаров	OK (работоспособное) — графы имеют всего одно состояние, так как непосредственно не влияют на работоспособность системы, а лишь являются источниками внешних сбоев для связанных модулей	OK –> OK Закон распределения: экспоненциальный Интенсивность: $\delta = 0{,}01$ Возникает при отказе мажоритара Генерируется событие V_nFault(k), свидетельствующее о сбое в соответствующем экземпляре мажоритара k
$A_n[k]$ $n = 1..3$ — номер блока $k = 1..3$ — номер экземпляра в блоке	OK (работоспособное) — соответствующий экземпляр блока исправен ERR (неработоспособное) — соответствующий экземпляр модуля неисправен вследствие возникновения восстанавливаемого отказа	OK –> ERR Закон распределения: экспоненциальный Интенсивность: $\lambda = 1{,}0$ Возникает при внутреннем отказе экземпляра блока Генерируется событие A_nFault, свидетельствующее об отказе соответствующего экземпляра блока k
		OK –> ERR Возникает при генерации V_nFault(k) в одном из подключенных к модулю мажоритаров Генерируется событие A_nFault
		ERR –> OK Возникает при генерации глобального события REC

■ *Окончание табл.*

Граф	Состояния	Переходы
A_nOut n = 1..3 — номер блока	OK (работоспособное) — троированный блок исправен DIST (работоспособное) — один из экземпляров блока неисправен ERR (неработоспособное) — два или более экземпляра блока n неисправны, что приводит к возникновению невосстанавливаемого отказа и выходу системы из строя	OK –> DIST Возникает при наступлении события A_nFault
		DIST –> OK Возникает при генерации глобального события REC
		DIST –> ERR Возникает при наступлении события A_nFault



■ ***Рис. 5.*** Зависимость интенсивности потока отказов системы от периода восстановления блоков A_1, A_2, A_3: *а* — общий результат; *б* — начальный участок

в течение периода восстановления. Модель событий для блоков A_2 и A_3 строится аналогичным образом.

Более подробно связи между событиями и состояниями в графах описаны в таблице.

При расчете для каждого фиксированного значения t_r в диапазоне от 0,0 до 1,0 производится заданное число экспериментов (50 000), каждый из которых продолжается до перехода системы в неработоспособное состояние. Во время каждого эксперимента моделируются возникновение случайных и детерминированных событий и реакции системы, заключающиеся в переходах графов между состояниями, и производится измерение времени наработки до отказа. Итоговые результаты получаются путем статистической оценки произведенного набора экспериментов.

Полученные результаты.

Расчет исследуемой структуры (рис. 5, *а*) проведен с помощью комбинаторной оценки и рассчитанной имитационной модели. Начальный участок данных кривых показан на рис. 5, *б*.

Ось абсцисс: период восстановления блоков A_1, A_2, A_3 ($T_{\text{восст}} = 1/\lambda_r$).

Ось ординат: интенсивность потока отказов на выходах O_1, O_2, O_3. Относительная единица измерения 1,0 обозначает интенсивность сбоя в любом из троированных элементов A_1, A_2, A_3. Интенсивность сбоев в любом из троированных мажоритаров равна 0,01.

Заключение

Полученные результаты позволяют сделать следующие выводы.

1. Аналитическая формула дает достаточно точную оценку надежности анализируемой структуры для малых периодов восстановления. Из рис. 5, *б* видно, что при периоде восстановления меньше 0,1 (в десять раз меньшем приблизительного периода между сбоями в каждом блоке) обе характеристики имеют линейную зависимость с одинаковым коэффициентом наклона.

2. Если обеспечение достаточно малого периода восстановления блоков невозможно из-за недостаточного резерва времени, зависимость интенсивности отказов от периода восстановления выходит на нелинейный участок, что приводит к необходимости применять имитационную модель для корректного расчета.

3. Расчет с помощью имитационной модели позволяет оценить эффективность применения механизмов повышения отказоустойчивости:

— если бы в системе не было реализовано ни восстановление, ни структурное резервирование, то отказ в любом из модулей A_1, A_2, A_3 приводил бы к выходу из строя всей системы. С учетом того, что периоды между отказами являются случайной величиной, подчиненной экспоненциальному закону распределения, а интенсивность возникновения отказов в каждом блоке равна 1,0,

среднее время наработки до отказа может быть оценено как $T_{\text{исх}} = \frac{1}{\lambda_1 + \lambda_2 + \lambda_3} = \frac{1}{3 \cdot 1{,}0} = 0{,}333$;

— если применяется троирование блоков и мажоритаров (что соответствует результатам расчета имитационной модели на больших периодах восстановления), то при интенсивности отказов каждого мажоритара, равной 0,01, интенсивность отказов системы стремится приблизительно к 2,5, а время средней наработки до отказа — к $T_{\text{рез}} = \frac{1}{2{,}5} = 0{,}4$ (эти величины соответствуют результату расчета марковской модели при отсутствии переходов по событию восстановления). Таким образом, по сравнению с нерезервированной системой время наработки до отказа было увеличено на $\frac{T_{\text{рез}} - T_{\text{исх}}}{T_{\text{исх}}} = \frac{0{,}4 - 0{,}333}{0{,}333} \cdot 100\% \approx 20\%$;

— обеспечение регулярного восстановления искаженных данных с периодом 0,05 (в 20 раз чаще возникновения сбоев в модулях) приводит к увеличению периода наработки до отказа до $T_{\text{восст}} = 1/0{,}43 = 2{,}33$, т. е. приблизительно в 5 раз относительно резервированной, но не восстанавливаемой структуры, что доказывает эффективность применения восстановления для борьбы с «мягкими» отказами.

4. Большое влияние периода восстановления на надежность системы подтверждает необходимость учета программного обеспечения при проектировании системы, так как оно определяет допустимый резерв времени, отводимый на периодическое восстановление блоков. Так как имитационная модель пригодна для анализа при любых величинах периода восстановления, она помогает оценить, достаточен ли имеющийся резерв времени для обеспечения требуемых характеристик надежности.

5. Имитационная модель также необходима для сравнительного анализа возможных организаций восстанавливаемых блоков на этапе синтеза с учетом таких показателей, как сложность реализации и быстродействие.

6. После того как в процессе проектирования были определены параметры восстановления для каждого блока и с помощью имитационной модели вычислена интенсивность потока отказов на выходе блоков, надежность сети блоков может быть оценена с помощью традиционных аналитических моделей или логико-вероятностными методами.

Литература

1. **Edmonds L. D., Barnes C. E., Scheick L. Z.** An Introduction to Space Radiation Effects on Microelectronics // JPL Publication 00-06, 2000. http://snebulos.mit.edu/projects/reference/NASA-Generic/JPL-00-06.pdf (дата обращения: 05.12.2015).
2. **Gaillard R.** Single Event Effects Mechanisms and Classification // Frontiers in Electronic Testing. 2011. Vol. 41. P. 27–54.
3. **Amusan O. A.,** et al. Single Event Upsets in Deep-Submicrometer Technologies due to Charge Sharing/ O. A. Amusan, L. W. Massengill, M. P. Baze, A. L. Sternberg, A. F. Witulski, B. L. Bhuva, J. D. Black // IEEE Transactions on Device and Materials Reliability. 2008. Vol. 8. N 3. P. 582–589.
4. **James R. Schwank, Marty R. Shaneyfelt, Paul E. Dodd.** Radiation Hardness Assurance Testing of Microelectronic Devices and Integrated Circuits: Radiation Environments, Physical mechanisms, and Foundations for Hardness Assurance // IEEE Transactions on Nuclear Science. 2013. Vol. 60. N 3. P. 2074–2100.
5. **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.
6. **Максименко С. Л., Мамутова О. В., Филиппов А. С., Мелехин В. Ф.** Методология проектирования восстанавливаемых встраиваемых вычислительных систем // Университетский научный журнал. 2014. № 8. С. 144–153.
7. **Jacob A. Abraham, Daniel P. Siewiorek.** An Algorithm for the Accurate Reliability Evaluation of Triple Modular Redundancy Networks // IEEE Transactions on Computers. 1974. Vol. C-23. N 7. P. 682–692.
8. **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.
9. **Черкесов Г. Н.** Надежность аппаратно-программных комплексов. — СПб.: Питер, 2005. — 480 с.
10. **Черкесов Г. Н., Можаев А. С.** Логико-вероятностные методы расчета надежности структурно-сложных систем // Качество и надежность изделий. Вып. 3 (15). — М.: Знание, 1991. С. 3–65.
11. **Черкесов Г. Н., Степанов Ю. В.** Логико-вероятностный анализ надежности сложных систем на основе общего решения систем логических уравнений // Научно-технические ведомости СПбГТУ. 2003. № 2. С. 149–158.
12. **Мельников И. В.** Применение имитационной модели надежности при проектировании изделий ракетно-космической техники // Молодой ученый. 2011. № 9. С. 39–42.

UDC 681.3
doi:10.15217/issn1684-8853.2016.2.26

Methods and Tools for Structural Block Reliability Analysis with Reservation and Periodic Information Recovery at Various Stages of Computing System Design

Egorov I. V.[a], Post-Graduate Student, iegorov@kspt.icc.spbstu.ru
Melekhin V. F.[a], Dr. Sc., Tech., Professor, melekhin@kspt.ftk.spbstu.ru
[a]Peter the Great St. Petersburg Polytechnic University, 29, Politekhnicheskaia St., 195251, Saint-Petersburg, Russian Federation

Introduction: When designing fault-tolerant computing systems which must work under radiation, you have to estimate the influence of information distortion caused by charged particles. Software tools developed to analyze the reliability of such systems should take into account these particle-caused failures and simulate the features of periodic recovery of the distorted information which are used to increase the reliability. **Purpose:** The goal of this study is to determine the bounds within which you can apply the reliability analysis methods based on using analytical and imitational models in order to evaluate the reliability of systems with periodic recovery. Another goal is to compare the results of analyzing the reliability characteristics obtained by the analytical and imitational models. **Results:** The analytical and imitating models helped to calculate and analyze the time for which a recoverable system works until a failure happens. It has been found out that determined recovery processes restrict the applicability of the traditional reliability estimation approaches such as Markov models or logical-probabilistic methods. The necessity to take into account the software influence when designing systems with periodic recovery has been substantiated. **Practical relevance:** The conducted research helped to specify the application areas for certain reliability models at various stages of designing fault-tolerant recoverable computing systems.

Keywords — Imitational Modeling, Reliability of Recoverable Systems, Radiation Resistant Computing System, Markov Model, Structural Reservation, Information Redundancy.

References

1. Edmonds L. D., Barnes C. E., Scheick L. Z. An Introduction to Space Radiation Effects on Microelectronics. JPL publication, 2000, no. 00-06. Available at: http://snebulos.mit.edu/projects/reference/NASA-Generic/JPL-00-06.pdf (accessed 05 December 2015).
2. Gaillard R. Single Event Effects Mechanisms and Classification. *Frontiers in Electronic Testing*, 2011, vol. 41, pp. 27–54.
3. Amusan O. A., Massengill L. W., Baze M. P., Sternberg A. L., Witulski A. F., Bhuva B. L., Black J. D. Single Event Upsets in Deep-Submicrometer Technologies due to Charge Sharing. *IEEE Transactions on Device and Materials Reliability*, 2008, vol. 8, no. 3, pp. 582–589.
4. James R. Schwank, Marty R. Shaneyfelt, Paul E. Dodd. Radiation Hardness Assurance Testing of Microelectronic Devices and Integrated Circuits: Radiation Environments, Physical mechanisms, and Foundations for Hardness Assurance. *IEEE Transactions on Nuclear Science*, 2013, vol. 60, no. 3, pp. 2074–2100.
5. Maximenko S. L., Melekhin V. F., Filippov A. S. Analysis of the Problem of Radiation-Tolerant Information and Control-Systems Implementation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2012, no. 2(57), pp. 18–25 (In Russian).
6. Maximenko S. L., Filippov A. S., Melekhin V. F., Mamoutova O. V. Design Methodology for Embedded Systems with Built-in Self-Recovery. *Universitetskii nauchnyi zhurnal*, 2014, no. 8, pp. 144–153 (In Russian).
7. Jacob A. Abraham, Daniel P. Siewiorek. An Algorithm for the Accurate Reliability Evaluation of Triple Modular Redundancy Networks. *IEEE Transactions on Computers*, 1974, vol. C-23, no. 7, pp. 682–692.
8. Maximenko S. L., Melekhin V. F. Analysis of Reliability of Functional Nodes of Digital VLSI Circuits with Structural Redundancy and Periodic Operational State Recovery. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 2(63), pp. 18–23 (In Russian).
9. Cherkesov G. N. *Nadezhnost' apparatno-programmnyh kompleksov* [Reliability of Hardware and Software Systems]. Saint-Petersburg, Piter Publ., 2005. 480 p. (In Russian).
10. Cherkesov G. N., Mozhaev A. S. Logical-and-Probabilistic Methods of Calculation of Reliability of Structural and Difficult Systems. *Kachestvo i nadezhnost' izdelii*, 1991, no. 3(15), pp. 3–65 (In Russian).
11. Cherkesov G. N., Stepanov Y. V. Logical-and-Probabilistic Analysis of Reliability of Difficult Systems on the Basis of the Common Decision of Systems of the Logical Equations. *Nauchno-tehnicheskie vedomosti SPbGTU*, 2003, no. 2, pp. 149–158 (In Russian).
12. Melnikov I. V. Application of Imitating Model of Reliability at Design of Products of the Missile and Space Equipment. *Molodoj uchenyj*, 2011, no. 9, pp. 39–42 (In Russian).