УДК 681.3(075.8)

Ю.А. БЕЛЫЙ

Научно-производственное предприятие «Радий», Украина

МОДЕЛИ ОТКАЗОВ И ОЦЕНКА НАДЕЖНОСТИ МУЛЬТИДИВЕРСНЫХ СИСТЕМ

Для мультидиверсных систем, полученных с использованием нескольких видов версионной избыточности, разработаны модели надежности с учетом интенсивностей проявления различных отказов программно-аппаратных версий.

мультидиверсные системы, модели отказов, модели надежности

Постановка задачи

Многоверсионные системы управления, применяемые в атомной энергетике и в аэрокосмической отрасли, позволяют реализовать принцип «защиты в глубину» [1] и таким образом снизить вероятность отказов по общей причине [2].

В работе [3] проанализированы типы многоверсионности, применимые для систем управления критическими объектами.

Дальнейшим развитием концепции «защиты в глубину» является принцип мультидиверсности, заключающийся в одновременном применении нескольких видов версионной избыточности [4, 5]. Мультидиверсной называют такую двухверсионную систему W [5], в которой версии v_1, v_2 получены с использованием нескольких видов версионной избыточности, таких, что устранение одного из этих видов избыточности не делает версии тождественными (рис. 1).

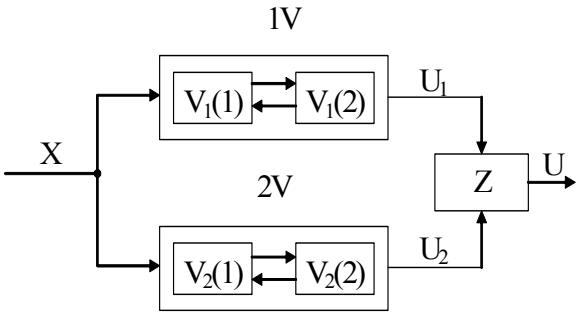

Рис. 1. Структура мультидиверсной системы с двумя видами версионной избыточности

Оценка надежности мультидиверсных систем базируется на анализе возможных видов дефектов и отказов [6] (рис. 2). Исходя из такого анализа, могут быть построены структурные схемы надежности (ССН), а затем получены модели безотказности для невосстанавливаемых систем или модели готовности для восстанавливаемых систем. Такая задача решалась для многоверсионных систем [4], однако для мультидиверсных систем модели отказов имеют свою специфику.

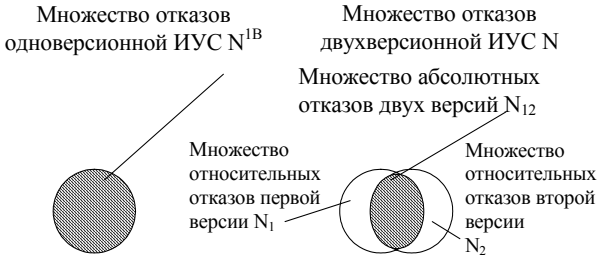

Рис. 2. Модель отказов двухверсионной ИУС

Целью статьи является разработка моделей отказов мультидиверсных систем и методики использования для исследования их надежности.

1. Связь дефектов и отказов. Обоснование допущений

Получим теоретико-множественные модели отказов и структурные схемы надежности (ССН) двухверсионных систем с различными видами версионной избыточности, включая программную и аппаратную диверсность [3]. Для этого необходимо

учесть различную природу отказов технических средств (ТС) и программного обеспечения (ПО). Отказы ПО обусловлены дефектами проектирования, при этом относительное количество абсолютных отказов ПО двух версий может изменяться от 0% (полностью идентичные версии) до 100% (абсолютно диверсные решения).

Отказы ТС вызываются, в первую очередь, физическим дефектами. Кроме того, отказы ТС также могут быть обусловлены дефектами проектирования (например, выбор неадекватной элементной базы или ошибки в схемах цифровых устройств).

При разработке теоретико-множественных и вероятностных моделей принято ряд допущений.

1. Об идеальности решающего устройства (РУ) (с учетом его простоты для систем рассматриваемого класса). Это допущение легко снимается, при необходимости получения консервативных оценок, путем домножения результата на вероятность безотказной работы РУ, включая вероятность отсутствия абсолютных дефектов. Кроме того, если учесть возможность существования различимых абсолютных дефектов, это упрощает работу средств контроля.

2. Об отсутствии одновременных отказов ТС двух версий (каналов). Данное допущение не является принципиальным, поскольку вполне соответствует нормальным условиям функционирования и результатам анализа статистики отказов при реальной эксплуатации. Снятие этого допущения, с одной стороны, в рамках поставленной задачи неоправданно усложнит математические модели, с другой, – может быть компенсировано, в случае необходимости учета экстремальных воздействий, переходом от использования понятия «интенсивность отказов элементов» канала (системы) к использованию понятия «интенсивность событий, связанных с кратными отказами».

3. Об отсутствии эффекта компенсации отказов вследствие различных дефектов ТС и ПО. Это допущение позволяет получить консервативную оценку показателей надежности исходя из того, что, как показано в [4] программная диверсность может привести к возможности парирования физических дефектов ТС в двухканальной системе без встроенного контроля каналов.

Может быть сделано аналогичное симметричное предположение о возможности парирования проектных дефектов ПО в двухверсионной системе без контроля версий при использовании разнообразия ТС, что усилит степень консервативности оценки. Степень занижения показателей надежности вследствие такого консерватизма требует дополнительного анализа, выходящего за рамки данного исследования.

2. Множества отказов и структурные схемы надежности

С учетом вышеизложенного для двухверсионной системы имеем следующие множества отказов, которые будем учитывать при разработке оценочных моделей:

$N_{12}^{ТС}$ – абсолютных отказов ТС двух версий, вызванные дефектами проектирования;

$N_{12}^{ПО}$ – абсолютных отказов ПО двух версий, вызванные дефектами проектирования;

$N_1^{ПО}$ – относительных отказов ПО первой версий, вызванные дефектами проектирования;

$N_2^{ПО}$ – относительных отказов ПО второй версий, вызванные дефектами проектирования;

$N_1^{ТС}$ – относительных отказов ТС первой версий, вызванные дефектами проектирования;

$N_2^{ТС}$ – относительных отказов ТС второй версий, вызванные дефектами проектирования;

$N_{ТС1}$ – относительных отказов ТС первой версий, вызванные физическими дефектами;

$N_{ТС2}$ – относительных отказов ТС второй версий, вызванные физическими дефектами.

Каждому отказу $n_d \in N$ соответствует тройка:

1) $x(n_d) \in X$ – соответствующий входной сигнал;

2) $y(n_d) \in Y$ – соответствующий выходной сигнал;

3) d (n_d) ∈ D(N) – соответствующий дефект, являющийся причиной отказа.

В работе исследуются следующие виды систем:

– одноверсионная система;

– двухверсионная система с версионной избыточностью ПО;

– двухверсионная система с версионной избыточностью ТС;

– мультидиверсная система с версионной избыточностью ПО и ТС.

Теоретико-множественные модели отказов указанных систем приведены на рис. 3, а их ССН – на рис. 4.

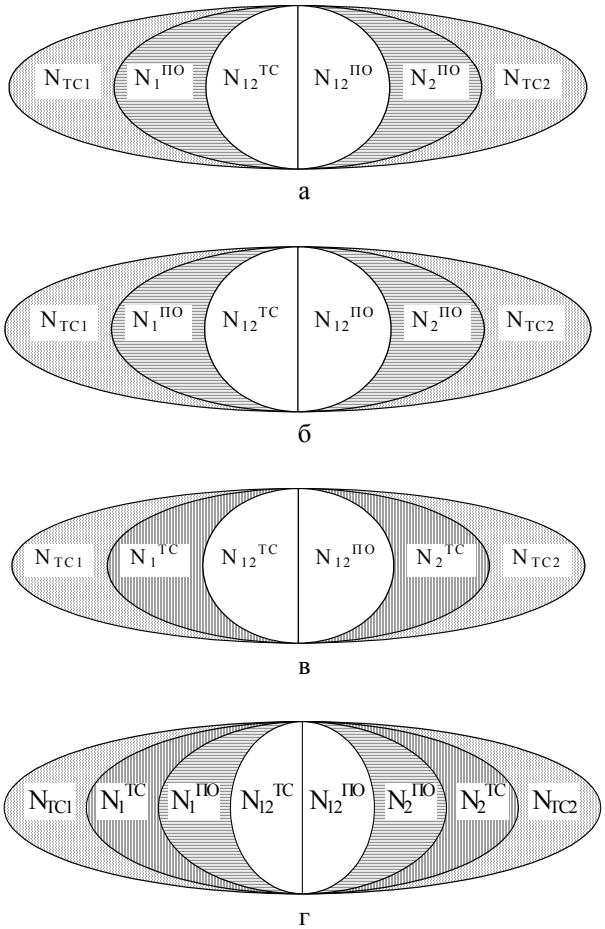

Рис. 3. Теоретико-множественные модели отказов одно- и двухверсионных систем:
а – двухканальная одноверсионная система;
б – двухверсионная система с версионной избыточностью ПО;
в – двухверсионная система с версионной избыточностью ТС;
г – двухверсионная система с версионной избыточностью ПО и ТС

В одноверсионной системе все отказы из-за дефектов проектирования являются абсолютными, парируются лишь отказы, вызванные физическими дефектами.

В двухверсионных системах с версионной избыточностью либо ПО (ТС) могут быть парированы отказы, вызванные дефектами проектирования ПО (ТС). Однако, все отказы, вызванные дефектами проектирования ТС (ПО), в таких системах являются абсолютными.

В мультидиверсной системе могут быть парированы отказы, вызванные и дефектами проектирования ТС, и дефектами проектирования ПО. Таким образом, число абсолютных отказов, вызванных дефектами проектирования, может быть сведено к минимуму.

3. Модели надежности

При разработке моделей надежности приняты допущения об экспоненциальном законе распределения времени до отказа и идеальных по достоверности и безотказности средствах контроля.

Кроме того, предполагается, что версии ТС и ПО имеют равные интенсивности отказов, т.е. $\lambda_1^{ПО} = \lambda_2^{ПО} = \lambda^{ПО}$; $\lambda_1^{ТС} = \lambda_2^{ТС} = \lambda^{ТС}$; $\lambda_{TC1} = \lambda_{TC2} = \lambda_{TC}$.

Введем коэффициент абсолютных отказов определяющий соотношение между интенсивностями отказов двухверсионной и одноверсионной системы (рис. 2) [6]:

$$K_{12} = \frac{\lambda_{12}}{\lambda^{1B}} = \frac{\lambda_{12}}{\lambda_{12} + \lambda_1} = \frac{\lambda_{12}}{\lambda_{12} + \lambda_2}. \qquad (1)$$

Для дублированной одноверсионной ИУС (рис. 4, а) формула для ВБР имеет вид [5]:

$$P = P_{12}^{ТС} \cdot P_{12}^{ПО} \cdot \left[1 - \left(1 - P_{ТС}\right)^2\right] = \\ = e^{-\lambda^{1B\,ТС} \cdot t} \cdot e^{-\lambda^{1B\,ПО} \cdot t} \cdot \left[1 - \left(1 - e^{-\lambda_{ТС} \cdot t}\right)^2\right], \qquad (2)$$

где $\lambda^{1B\,ТС}$ – интенсивность отказов одной версии ТС из-за дефектов проектирования; $\lambda^{1B\,ПО}$ – интенсивность отказов одной версии ПО из-за дефектов проектирования; $\lambda_{ТС}$ – интенсивность отказов одного канала ТС, вызванных физическими дефектами.

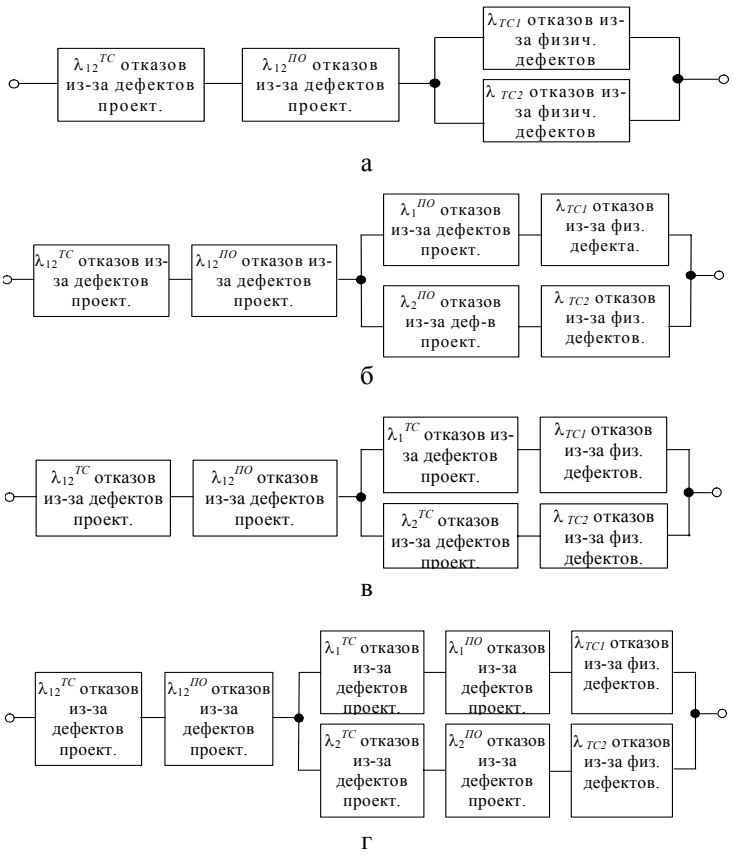

Рис. 4. Структурные схемы надежности одно- и двухверсионных систем:
а – двухканальная одноверсионная система; б – двухверсионная система с версионной избыточностью ПО; в – двухверсионная система с версионной избыточностью ТС; г – двухверсионная система с версионной избыточностью ПО и ТС

Для двухверсионной ИУС с версионной избыточностью ПО (рис. 4, б) ВБР определяется выражением:

$$P=P_{12}^{TC}\cdot P_{12}^{ПО}\cdot\left[1-\left(1-P^{ПО}\cdot P_{TC}\right)^2\right]= =e^{-\lambda^{1B\,TC}\cdot t}\cdot e^{-K_{12}^{ПО}\cdot\lambda^{1B\,ПО}\cdot t}\times \times\left[1-\left(1-e^{-(1-K_{12}^{ПО})\cdot\lambda^{1B\,ПО}\cdot t}\cdot e^{-\lambda_{TC}\cdot t}\right)^2\right], \quad (3)$$

где $K_{12}^{ПО}$ – коэффициент абсолютных отказов для ПО.

Для двухверсионной ИУС с версионной избыточностью ТС (рис. 4, в) ВБР вычисляется по формуле:

$$P=P_{12}^{TC}\cdot P_{12}^{ПО}\cdot\left[1-\left(1-P^{TC}\cdot P_{TC}\right)^2\right]= =e^{-K_{12}^{TC}\cdot\lambda^{1B\,TC}\cdot t}\cdot e^{-\lambda^{1B\,ПО}\cdot t}\times \times\left[1-\left(1-e^{-(1-K_{12}^{TC})\cdot\lambda^{1B\,TC}\cdot t}\cdot e^{-\lambda_{TC}\cdot t}\right)^2\right], \quad (4)$$

где K_{12}^{TC} – коэффициент абсолютных отказов для ТС.

Для мультиверсионной системы с версионной избыточностью ТС и ПО (рис. 4, г) ВБР определяется выражением:

$$P=P_{12}^{TC}\cdot P_{12}^{ПО}\cdot\left[1-\left(1-P^{TC}\cdot P^{ПО}\cdot P_{TC}\right)^2\right]= =e^{-K_{12}^{TC}\cdot\lambda^{1B\,TC}\cdot t}\cdot e^{-K_{12}^{ПО}\cdot\lambda^{1B\,ПО}\cdot t}\times \times\left[1-\left(1-e^{-(1-K_{12}^{TC})\cdot\lambda^{1B\,TC}\cdot t}\cdot e^{-(1-K_{12}^{ПО})\cdot\lambda^{1B\,ПО}\cdot t}\cdot e^{-\lambda_{TC}\cdot t}\right)^2\right]. \quad (5)$$

На основании анализа данных об отказах элементной базы и ПО [5, 6] для моделирования были выбраны следующие базовые значения интенсивностей отказов: $\lambda^{1B\,TC} = 10^{-5}$ 1/час; $\lambda^{1B\,ПО} = 10^{-5}$ 1/час; $\lambda_{TC} = 10^{-5}$ 1/час. Результаты моделирования зависимости ВБР от времени представлены на рис. 5, где 2VSW – график для двухверсионной системы с версионной избыточностью ПО; 2VHW – график для двухверсионной системы с версионной избыточностью ТС; 2V – график для МДВС системы с версионной избыточностью ТС и ПО.

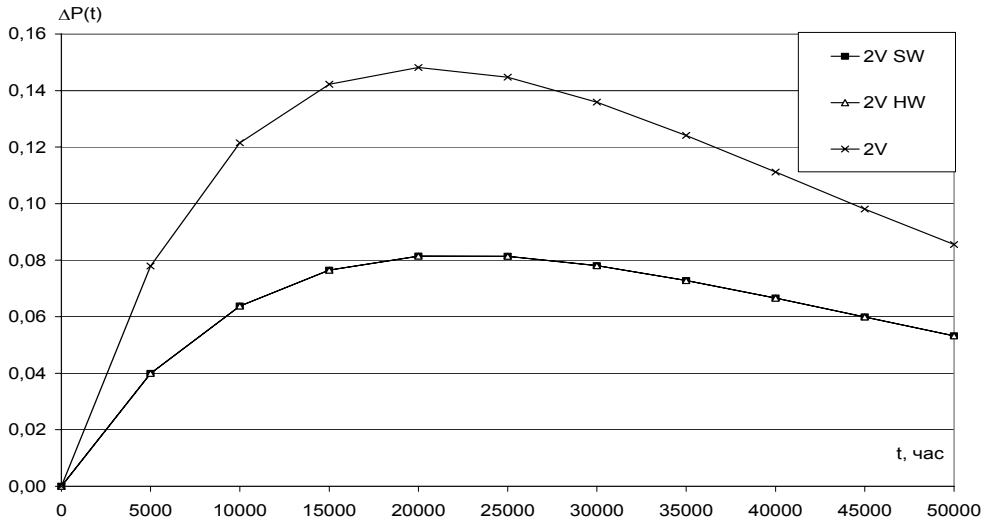

Рис. 5. Графики зависимости выигрыша в ВБР
по сравнению с одноверсионной системой от времени
при значениях коэффициентов абсолютных отказов $K_{12}^{ТС} = K_{12}^{ПО} = 0$

Выводы

В статье разработаны модели надежности мультидиверсных систем с учетом интенсивностей проявления различных отказов программно-аппаратных версий. Исследованы модели надежности для невосстанавливаемых систем. Максимальное значение выигрыша в вероятности безотказной работы для двухверсионных систем при выбранных значениях интенсивностей отказов и при отсутствии абсолютных отказов наступает через 20 000 часов (27 месяцев) и составляет 0,08 для ИУС с версионной избыточностью ПО и ТС, 0,15 – для ИУС с версионной избыточностью и ПО и ТС.

Модели надежности (готовности) для восстанавливаемых мультидиверсных систем могут быть получены в дальнейшем путем применения марковских моделей [4].

Литература

1. Либман Ж. О ядерной безопасности. – Институт по ядерной и радиационной безопасности (Франция), 1997. – 690 с.

2. Avizienis A., Laprie J., Randell B. Fundamental Concepts of Dependability. Research Report n 01145, LAAS-CNRS, 2001. – 25 p.

3. Preckshot G. Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems. NUREG/CR-6303. – Livermore, USA: Lawrence Livermore National Laboratory, 1994.– 35 p.

4. Харченко В.С. Теоретические основы дефектоустойчивых цифровых систем с версионной избыточностью. – Х: ХВУ, 1996. – 506 с.

5. Харченко В.С., Скляр В.В., Сиора А.А., Белый Ю.А. Модели безотказности и готовности встроенных мультидиверсных систем // Авиационно-космическая техника и технология. – 2008. – № 1. – С. 68-73.

6. Скляр В.В. Анализ метрик многоверсионности программного обеспечения // Электронное моделирование. – 2004. – Т. 26, № 4. – С. 95-104.

Поступила в редакцию 18.02.2008

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.