Скольльзящее резервирование толерантных элементов

Сергей Ф. Тюрин, Пермский национальный исследовательский политехнический университет, Пермь, Россия,
e-mail: tyurinsergfeo@yandex.ru

Сергей Ф. Тюрин

Резюме. Одним из основных путей повышения надёжности является резервирование. В частности, используется структурное резервирование. В таком случае может обеспечиваться отказоустойчивость элементов, устройств и систем. Отказоустойчивость может обеспечивать парирование как сбоев, так и отказов. Исследуется повышение надёжности путём так называемого скольльзящего резервирования, обеспечивающего работоспособность систем из n элементов с резервом из m элементов, которые могут заменить любой основной элемент. Предлагается усовершенствование скольльзящего резервирования путём восстановления элементов из нескольких отказавших элементов, но сохранивших некоторую функциональность (базис). Например, базис логической (булевой) функции в смысле теоремы Поста обеспечивается в случае, если эта функция является не сохраняющей константу нуля, не сохраняющей константу единицы, не самодвойственной, не линейной, не монотонной. Ранее автором предложены так называемые функционально-полные толерантные логические функции (ФПТФ), не только обладающие функциональной полнотой, но и сохраняющие её при заданной модели отказов. Тогда даже неисправный элемент остаётся функционально полным, но с меньшими возможностями, например, становится элементом 2ИЛИ-НЕ, хотя сама ФПТФ может быть реализована элементом 2И-2ИЛИ-НЕ. В этом случае для восстановления исходной функции необходимо несколько элементов 2ИЛИ-НЕ. Однако проблемой является диагностика этих элементов и их реконфигурация в случае отказов. Такой подход может быть интерпретирован восстановлением логики программируемых логических интегральных схем (ПЛИС), которая реализована на так называемых LUT (Look Up Table), представляющих собой запоминающие устройства на основе мультиплексоров 16-1. Причём схема представляет собой дерево передающих транзисторов. При их отказах возможно использование работоспособной половины LUT. Из таких «половинных» LUT можно путём реконфигурации на основе штатных средств ПЛИС, содержащих матрицы локальных и глобальных связей, восстановить LUT, функции которых эквиваленты исходным. Это равносильно увеличению количества резервных элементов. Скольльзящее резервирование с восстановлением элементов из нескольких отказавших, но сохранивших базис, может быть использовано в областях критического применения систем, когда ремонт либо замена элементов невозможны. В статье предлагается формула, учитывающая такое восстановление, анализируются особенности такого резервирования и оценивается выигрыш в надёжности.

Ключевые слова: надёжность, резервирование, скольльзящее резервирование, восстановление, отказы, отказоустойчивость, интенсивность отказов.

Формат цитирования: Тюрин С.Ф. Скольльзящее резервирование толерантных элементов // Надёжность. 2017. Т. 17, №1. С. 17-21. DOI: 10.21683/1729-2646-2017-17-1-17-21

Введение

Надёжность систем может быть обеспечена путём резервирования, часто используется резервирование замещением, при котором функции основного элемента передаются резервному только после отказа основного элемента [1]. При мажоритарном резервировании отказ или сбой маскируется. Однако это требует большой избыточности. Меньшей структурной избыточностью характеризуется адаптивная отказоустойчивость [2, 3 и др.], включающая процедуры контроля, реконфигурации и автоматического замещения отказавших модулей имеющимися избыточными. В случае скольльзящего резервирования группа основных элементов резервируется одним или несколькими резервными элементами, каждый из которых может заменить любой из отказавших элементов данной группы [1]. Скольльзящее резервирование при n основных элементах и m резерв-

ных обеспечивает работоспособность в случае, если работоспособно подмножество R элементов мощностью $|R| \geq n$. Без учёта сложности и времени диагностирования и восстановления для экспоненциальной модели отказов вероятность безотказной работы системы со скольльзящим резервированием описывается выражением:

$$P_{\text{СССР}}(n, m, t) = \sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} \cdot [1 - e^{-\lambda \cdot t}]^{n+m-i}. \quad (1)$$

В формуле (1) $P_{\text{СССР}}$ – вероятность безотказной работы системы со скольльзящим резервированием (СССР), t – время, ч. Графики изменения (1) в системе компьютерной математики «MathCad» представлены на рисунке 1.

Переключающее устройство (ПУ) при отказе элемента подключает оставшиеся резервные (выполняется так называемая реконфигурация), с учётом интенсивности $\lambda_{\text{пу}}$ отказов ПУ и с учётом допущения об идеальности контроля основных и избыточных элементов получим:

Рисунок 1 – Зависимость P_{CCCp} от числа резервных элементов m , основных n , времени t (ч) при $\lambda = 10^{-5}$ (1/ч) без учета интенсивности отказов переключающего устройства

Рисунок 2 – Зависимость P_{CCCp} от числа резервных элементов m , основных n , времени t (ч) при $\lambda = 10^{-5}$ (1/ч) с учетом интенсивности отказов переключающего устройства $\lambda_{ny} = 10^{-7}$ (1/ч)

$$P_{CCCp}(n, m, t) = \sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i\lambda \cdot t} \cdot [1 - e^{-\lambda \cdot t}]^{n+m-i} \cdot e^{-\lambda_{ny} \cdot t}. \quad (2)$$

График зависимости P_{CCCp} (2) от времени t (ч), числа резервных элементов для $n=10$ при $\lambda = 10^{-5}$ (1/ч), $\lambda_{ny} = 10^{-7}$ (1/ч) представлен на рисунке 2.

Постановка задачи

Не будем рассматривать восстановление путём замены или ремонта отказавших элементов. Предложим использование возможностей отказавших элементов, то есть своего рода «внутреннее» резервирование [4]. В этом случае отказавшие элементы из системы со скользящим резервированием остаются в резерве, если они сохраняют хоть какую-то функциональность (базис) и могут быть использованы, но для реализации исходного элемента их потребуется больше одного. Такая постановка хорошо согласуется с современными программируемыми логическими интегральными схемами (ПЛИС) типа FPGA (field-programmable gate array), содержащими большое число логических элементов (LUT – Look Up Table) [5], при одиночных отказах которых иногда есть возможность использования LUT на меньшее число

переменных [6–7]. Как правило, в ПЛИС используются не все логические элементы (по некоторым оценкам 70%, а то и меньше). Поэтому оставшиеся элементы могут составить резерв для скользящего резервирования. Реконфигурация после соответствующей диагностики может быть выполнена дистанционно (например, для космического аппарата – по командам из центра управления полётом). Однако при исчерпании резерва ячеек LUT, ПЛИС оказывается неработоспособной. Для систем критического назначения, в которых отсутствует возможность замены ПЛИС, это недопустимо.

Теоретическая часть

Восстановление отказавших основных (резервных) элементов эквивалентно их увеличению при допущении, что они восстанавливаются по мере наступления отказов. Но для восстановления одного элемента надо несколько отказавших. Предпосылки предлагаемого подхода к восстановлению элементов из неисправных – современные тенденции введения блоков встроенной диагностики в ПЛИС и системы на кристаллах, встроенного сервисного обслуживания с генераторами тестовых воздействий в соответствии со стандартом IEEE 1500 [8].

Рисунок 3 – Зависимость P_{CCP} с частичным восстановлением от времени t (ч), числа резервных элементов m , основных n , при $\lambda = 10^{-5}$ (1/ч) при $r=3$ и без учета интенсивности отказов переключающего устройства

Рисунок 4 – Зависимость P_{CCP} с частичным восстановлением от числа резервных элементов m , основных n , времени t (ч) при $\lambda = 10^{-5}$ (1/ч) при $r=3$ с учетом интенсивности отказов переключающего устройства $\lambda_{\text{ны}} = 10^{-7}$ (1/ч)

Эти блоки могут быть также резервированы, например, в соответствии с технологией, применяемой фирмой Xilinx в ПЛИС Virtex [9], что и позволяет применить допущения об идеальности контроля основных и избыточных элементов.

Рассмотрим LUT на две переменные, который описывается выражением:

$$z = \bar{a}\bar{x}_2\bar{x}_1 \vee b\bar{x}_2x_1 \vee cx_2\bar{x}_1 \vee dx_2x_1. \quad (3)$$

При отказе в одной половине такого LUT он может быть представлен, например, выражением:

$$z_1 = \bar{a}\bar{x}_1 \vee bx_1. \quad (4)$$

Если имеется три таких «половинных» элемента с функциями z_1, z_2, z_3 , то из них путём соответствующего подключения переменных (реконфигурации) можно восстановить выражение (3):

$$z = z_3 = (\bar{a}\bar{x}_1 \vee bx_1 = z_1)\bar{x}_2 \vee (c\bar{x}_1 \vee dx_1 = z_2)x_2. \quad (5)$$

В общем случае для различных абстрактных базисов будет иметь место, например, выражение:

$$v = \left\lfloor \frac{m}{r} \right\rfloor, \quad (6)$$

где r – максимальное требуемое количество отказавших элементов для восстановления исходной функции, $\lfloor \cdot \rfloor$ – ближайшее меньшее целое натуральное число (ceil). Например, $m=5; r=4; v=1$. То есть, дополнительно можно парировать шестой отказ. Остаток будет:

$$w = m - r \left\lfloor \frac{m}{r} \right\rfloor. \quad (7)$$

В нашем случае $w=1$.

$$1 \leq w \leq r - 1. \quad (8)$$

Остатки могут пригодиться в дальнейшем при последующих отказах элементов из количества n .

Если не считать остатки, то количество $v_1 = \left\lfloor \frac{m}{r} \right\rfloor$ используется для парирования v_1 дополнительных к m отказов. Например, $m=18; r=4; v=4$. Значит, после отказа четырёх элементов, можно из них восстановить ещё один элемент, то есть, ещё дополнительных отказов будет парировано:

$$v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor. \quad (9)$$

В принципе «вложенность» дробей может быть большая, но парируется дополнительных отказов не более n . Считаем, что повторно отказавшие элементы не восстанавливаются (хотя в ряде случаев это возможно, например, переход из трёхэлементного базиса в двухэлементный). Получаем ряд:

$$m; v_1 = \left\lfloor \frac{m}{r} \right\rfloor; v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor; v_3 = \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor}{r} \right\rfloor \dots \quad (10)$$

Это не что иное, как геометрическая прогрессия, но с выделением целой части.

$$\sum_i v_i = \theta \leq n. \quad (11)$$

Эта сумма показывает дополнительное число парируемых отказов без учёта «остатков». Если учитывать «остатки», то:

$$v_2 = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor + m - r \left\lfloor \frac{m}{r} \right\rfloor}{r} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor;$$

$$v_3 = \left\lfloor \frac{\left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor + \left\lfloor \frac{m}{r} \right\rfloor (1-r) + m - r \left\lfloor \frac{\left\lfloor \frac{m}{r} \right\rfloor (1-r) + m}{r} \right\rfloor}{r} \right\rfloor. \quad (12)$$

Экспериментальная часть

В первом приближении (для восстановления из m отказавших элементов системы) получаем для v_1 :

$$P_{CCCP}(t) = \sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} \cdot (1 - e^{-\lambda t})^{n+m-i} \cdot e^{-\lambda_{np} \cdot t} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j) \lambda t} (1 - e^{-\lambda t})^{m+j} e^{-\lambda_{np} \cdot t}. \quad (13)$$

Соответствующие (13) графики без учёта и с учётом интенсивности отказов переключающего устройства изображены на рисунках 3 и 4.

В случае дополнительных затрат на восстановление оказавших λ_b получаем:

$$P_{CCCP}(t) = \sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} \cdot (1 - e^{-\lambda t})^{n+m-i} \cdot e^{-\lambda_{np} \cdot t} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j) \lambda t} (1 - e^{-\lambda t})^{m+j} e^{-(\lambda_{np} + \lambda_b) t}. \quad (14)$$

Графики изменения (14) изображены на рисунке 5. Получим значение выигрыша δP :

$$\delta P = \left[\sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} \cdot (1 - e^{-\lambda t})^{n+m-i} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j) \lambda t} (1 - e^{-\lambda t})^{m+j} \right] e^{-(\lambda_{np} + \lambda_b) t} - \left[\sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \lambda t} (1 - e^{-\lambda t})^{n+m-i} \right] e^{-\lambda_{np} t}. \quad (15)$$

Результаты расчетов формулы (15) в СКМ «MathCad» представлены на рисунке 6.

Из соотношения (15) определим при заданной λ_b условия выигрыша. Преобразуем (15) для определения λ_b :

$$\delta P_{mp} + \left[\sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} (1 - e^{-\lambda t})^{n+m-i} \right] e^{-\lambda_{np} t} = \left[\sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} \cdot (1 - e^{-\lambda t})^{n+m-i} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j) \lambda \cdot t} (1 - e^{-\lambda t})^{m+j} \right] e^{-(\lambda_{np} + \lambda_b) t}. \quad (16)$$

Выполнив деление левой части выражения (16) на выражение правой части без члена, учитывающего λ_b , и проведя логарифмирование, получим λ_b :

$$-\frac{1}{t} \ln \frac{\left\{ \delta P_{mp} + \left[\sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \lambda t} (1 - e^{-\lambda t})^{n+m-i} \right] e^{-\lambda_{np} t} \right\}}{\left[\sum_{i=n}^{n+m} C_{n+m}^i \cdot e^{-i \cdot \lambda \cdot t} \cdot (1 - e^{-\lambda t})^{n+m-i} + \sum_{j=1}^{\left\lfloor \frac{m}{r} \right\rfloor} C_{n+m}^{m+j} \cdot e^{-(n-j) \lambda \cdot t} (1 - e^{-\lambda t})^{m+j} \right] e^{-\lambda_{np} t}} = \lambda_b. \quad (17)$$

Заключение

Предложенное скользящее резервирование с восстановлением элементов из тех отказавших элементов, которые сохранили базис, позволяет получить существенное увеличение надёжности, в ряде случаев вероятность безотказной работы при условии идеальной диагностики увеличивается на 15-20% от максимально возможного выигрыша. Подход может быть применён для систем, в которых техническое обслуживание невозможно, например, для космических аппаратов на орбите, в полёте или при их работе на других планетах. В дальнейшем целесообразно рассмотреть вопрос учёта времени восстановления, например, с использованием математического аппарата Марковских цепей, а также более подробно проанализировать вопросы контроля и диагностики. Вызывает интерес и учёт снижения быстродействия элементов, построенных из отказавших элементов.

Рисунок 5 – Зависимость P_{CCCP} с частичным восстановлением от числа резервных элементов m , основных n , времени t (ч), при $\lambda = 10^{-5}$ (1/ч) при различных r с учетом интенсивности отказов переключающего устройства $\lambda_{\text{пы}} = 10^{-7}$ и затрат на аппаратуру восстановления $\lambda_{\text{в}} = 10^{-8}$ (1/ч)

Рисунок 6 – Зависимость $\delta P(n, m, r, t)$ с частичным восстановлением от числа резервных элементов m , основных n , требуемым для восстановления одного элемента количеством отказавших r , времени t (ч) при $\lambda = 10^{-5}$ (1/ч) с учетом интенсивности отказов переключающего устройства $\lambda_{\text{пы}} = 10^{-7}$ (1/ч), $\lambda_{\text{в}} = 10^{-8}$ (1/ч)

Библиографический список

- ГОСТ 27.002-89. Надежность в технике Основные понятия. Термины и определения. – М.: Издательство стандартов, 1990. – 42 с.
- Надежные отказоустойчивые информационные системы. Методы синтеза/ И.Б. Шубинский. – 2016. – 544 с.
- Васильев Н.П., Шубинский И.Б. Аналитическая оценка вероятности успешной адаптации к отказам модульных вычислительных систем с многоуровневой активной защитой. Известия высших учебных заведений. Приборостроение. 1994. Т. 37. № 3-4. С. 47.
- Тюрин С.Ф. Проблема сохранения функциональной полноты булевых функций при «отказах» аргументов // Автоматика и телемеханика. 1999. № 9. С. 176-186.
- Строгонов А., Цыбин С. Программируемая коммутация ПЛИС: взгляд изнутри [Электронный ресурс]. – URL: http://www.kit-e.ru/articles/plis/2010_11_56.php (дата обращения: 16.10.2016).
- Tyurin S.F., Gromov O.A. A residual basis search algorithm of fault-tolerant programmable logic integrated circuits // Russian Electrical Engineering. – 2013. – 84 (11). – P. 647–651. DOI: 10.3103/S1068371213110163

7. Tyurin S.F., Grekov A.V. Functionally Complete Tolerant Elements // International Journal of Applied Engineering Research. -2015.- Volume 10, №14. pp. 34433-34442.

8. Парфентий А.Н., Хаханов В.И., Литвинова Е.И. Модели инфраструктуры сервисного обслуживания цифровых систем на кристаллах // АСУ и приборы автоматики. 2007. Вып. 138. С. 83 – 99.

9. Carl Carmichael. Triple Module Redundancy Design Techniques for Virtex FPGAs [Электронный ресурс]. https://www.xilinx.com/support/documentation/application_notes/xapp197.pdf (дата обращения: 07.12.2016).

Сведения об авторе

Сергей Ф. Тюрин – доктор технических наук, профессор, Заслуженный изобретатель Российской Федерации, профессор кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, Россия, e-mail: tyurinsergfeo@yandex.ru

Поступила 21.11.2016