УДК 681.3

С.Ф. Тюрин[1], В.С. Харченко[2]

[1] *Пермский государственный технический университет, Пермь, Россия*
[2] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков*

АВТОМАТНО-БАЗИСНЫЙ ПОДХОД К СОЗДАНИЮ ЕСТЕСТВЕННО НАДЕЖНЫХ И БЕЗОПАСНЫХ СИСТЕМ

Предлагается подход к созданию естественно надежных и безопасных систем, толерантных к отказам (различным негативным воздействиям). Сформулированы основные принципы автоматно-базисного подхода. Подход основан на применении избыточного базиса, позволяющего сохранить все или часть функций систем при отказах. Система представляется автоматной моделью, причём восстановление логического преобразователя осуществляется путём использования предлагаемых функционально-полных толерантных базисов. Приведены примеры реализации функционально-полных толерантных базисов на вентильном уровне.

Ключевые слова: *избыточный базис, автоматная модель, функционально-полный толерантный базис, отказ, воздействие.*

Введение

Создание надёжных и безопасных систем является одной из ключевых проблем современной науки и инженерной практики. При этом речь идет о системах в широком диапазоне: от относительно несложных технических устройств до организационно-технических систем и инфраструктур ("системах систем") разной природы и разного назначения.

Исторически сложилось так, что наиболее продуктивные идеи и решения появились в области дискретных (цифровых) систем, хотя они носили и более общий характер. Ключевыми здесь были, по нашему мнению, работы J. Von Neumann [1], который сформулировал парадигму "надежных организмов из ненадежных компонент", A. Avižienis, который предложил принципы отказоустойчивости и N-версионного программирования [2], а затем (совместно с J.-C. Laprie, B. Randell, C. Landwehr) сформировал методологию гарантоспособных вычислений [3, 4].

Эволюция методов и технологий в сфере цифровых (и компьютерных) систем проанализирована в [5]. За последние десятилетия здесь наблюдалась нарастающая динамика роста терминов и парадигм, предложенных для создания надежных систем [6, 7]: устойчивых (fault-tolerant) и "эластичных" (fault-resilient) к отказам; "естественно надёжных" (naturally reliable), "естественно гарантоспособных" (naturally dependable); отказобезопасных (fault-safe) и "естественно безопасных" (naturally safe); высокой готовности (high availability) и живучести (high syrvivability); самовосстанавливающихся (self-recovery) и "самоизлечивающихся" (self-healing) и др.

Для более сложных систем и инфраструктур, кроме того, получили развитие идеи, связанные с устойчивостью к катастрофам (disaster tolerance) и восстанавливаемостью при катастрофах (disaster recovery). Инфраструктурный контекст становится все более актуальным в связи с масштабностью инцидентов и аварий, происходящих вследствие естественных отказов, отказов и нарушений физической или информационной природы, которые носят непредумышленный или целенаправленный характер.

Большинство из известных методов обеспечения надежности основывается на применении различных видов избыточности, причем чаще всего эта избыточность применяется на канальном (системном) уровне, т.е. реализуется общее резервирование для системы в целом или ее наиболее важных подсистем. В то же время хорошо известно, что раздельное резервирование более эффективно.

Что касается безопасности (здесь и далее речь идет о функциональной безопасности (safety)), то в рамках данной работы будем руководствоваться простым постулатом: пока система надежна (работоспособна), она безопасна. Другими словами, здесь не рассматриваются методы, специфические для обеспечения безопасности (независимая верификация, диверсность и др. [8]).

Цель статьи – разработка похода, основанного на обеспечении надежности на базисном уровне, т.е. уровне элементов системы. Статья структурирована следующим образом.

1. Сущность автоматно-базисного подхода

Предлагаемый подход основывается на следующих принципах.

1. Концептуальным принципом является базисный подход к обеспечению надежности. Другими словами, обеспечение надежности осуществляется на уровне базисных компонент. Такими базисами являются логический базис для цифровых автоматов, автоматный или иной базис – для сложных систем.

2. Система строится с использованием компонент, обеспечивающих устойчивость (толерантность)

к заданному набору и типам отказов или воздействиям, если известна модель воздействий, которая позволяет получить модель отказов с требуемой детализацией. Под воздействием понимается явление любой природы (умышленное или непреднамеренное, случайное или детерминированное) или масштаба (одиночный сбой или отказ, множественный отказ в одной системе, катастрофический или кластерный отказ для инфраструктуры).

3. Компоненты, из которых строится система, имеют минимальную избыточность, чтобы обеспечить требуемую устойчивость к отказам. При этом должен обеспечиваться уровень устойчивости не ниже, чем при резервировании системы в целом.

4. Отказы, возникающие в одном компоненте, не могут влиять на работоспособность других компонент (снижать их устойчивость к отказам).

2. Автоматная модель системы, толерантной к воздействиям

Допустим, имеется система с некоторым множеством функций:

$$\Phi = \{\phi_1, \phi_2, ...\phi_n\}. \quad (1)$$

Пусть задана модель Ψ воздействий в виде множества

$$\Psi = \{\psi_1, \psi_2, ...\psi_m\}. \quad (2)$$

Причём, в общем случае, воздействие – некоторая цепочка (или множество цепочек) из Ψ^*, где * – итерация Ψ. В результате воздействия система деградирует, в частности, лишается некоторых функций:

$$\Phi^{\times} = \{\phi_j^{\times i}\}, i = \overline{1,r}, j = \overline{1,k}, k \le n, \quad (3)$$

где r – число вариантов деградации j-й функции; k – число оставшихся функций, которые также могут деградировать.

Пусть требуется сохранить некоторое множество функций $\Phi^R \subset \Phi$ после воздействия. Тогда это можно описать композицией оставшихся функций или цепочками из $\Phi^{\times *}$, где * – соответствующая итерация. При этом могут быть дополнительно заданы временные T_o и стоимостные ограничения C_o.

Функции системы представляются автоматными моделями, описывающими преобразование входных данных в выходные. Автоматная модель представляет собой пятёрку [9]:

$$S=<X,Y,Z,\varphi,\psi>, \quad (4)$$

в которой $X=\{x_1,x_2,...,x_i\}$ – конечное входное множество (входной алфавит); $Y=\{y_1,y_2,...,y_j\}$ – конечное множество внутренних состояний автомата (алфавит состояний); $Z=\{z_1,z_2,...,z_k\}$ – конечное выходное множество (выходной алфавит); φ – функция переходов (из состояния в другие состояния); ψ – функция выходов; функция переходов представляет собой отображение вида φ: $X \times X \mapsto Y$; функция выходов представляет собой отображение вида ψ: $X \times Y \to Z$.

Таким образом, вместо абстрактных функций системы рассматривается множество автоматов $A = \{a_1, a_2, ...a_n\}$, деградирующих в результате воздействий Ψ^*:

$$A^{\times} = \{a_j^{\times i}\}, i = \overline{1,r}, j = \overline{1,k}, k \le n, \quad (5)$$

Причём, ставится условие обеспечения восстановления части автоматов $A^R \subset A$ после воздействия с заданными ограничениями T_o, C_o. В этом случае необходима суперпозиция автоматов, т.е. множество автоматов будет толерантным в случае, если после воздействий возможно указанное восстановление. Речь идёт не о простом структурном резервировании, а о резервировании свойства базисности, т.е. о сохранении базиса, позволяющего восстановление.

Однако, проблема функциональной полноты последовательностного автомата в общем случае алгоритмически неразрешима [10]. Тем не менее, любой автомат может быть представлен декомпозицией логического преобразователя и элементов памяти, а проблема функциональной полноты логического преобразователя разрешима в соответствии с теоремой Поста [11]. Логический преобразователь – не что иное, как частный случай автомата – комбинационный автомат:

$$KS=<X,Z,\psi>. \quad (6)$$

Восстановление памяти автомата обеспечивается известными методами структурного резервирования и помехоустойчивого кодирования. Применительно к сложным системам она решается путем создания резервных хранилищ и коммуникаций. Таким образом, для KS необходима не только функциональная полнота, но и её сохранение после воздействий [12].

3. Сохранение базиса логического преобразователя при воздействии

В [13 – 16] разработана концепция избыточного логического базиса как альтернатива структурному резервированию. Он представляет собой функционально-полный толерантный базис (ФПТБ), сохраняющий при воздействии не саму исходную функцию, а функциональную полноту при заданной модели негативных воздействий (отказов).

Один из вариантов функционально-полного толерантного базиса для модели константных однократных модификаций переменных имеет вид:

$$\bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4 \quad \text{или} \quad \overline{(x_1 \vee x_2)(x_3 \vee x_4)}. \quad (7)$$

Все модификации этой функции $f_{4383} = \bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4$: $\bar{x}_2 \vee \bar{x}_3\bar{x}_4$, $\bar{x}_1 \vee \bar{x}_3\bar{x}_4$, $\bar{x}_1\bar{x}_2 \vee \bar{x}_4$, $\bar{x}_3\bar{x}_4$, $\bar{x}_1\bar{x}_2$ представляют собой функции, обладающие функциональной полнотой в смысле теоремы Поста [16]. Реализация ФПТБ на вентильном уровне в виде элемента на базе КМОП транзисторов с p и n каналами [17] приведена на рис. 1.

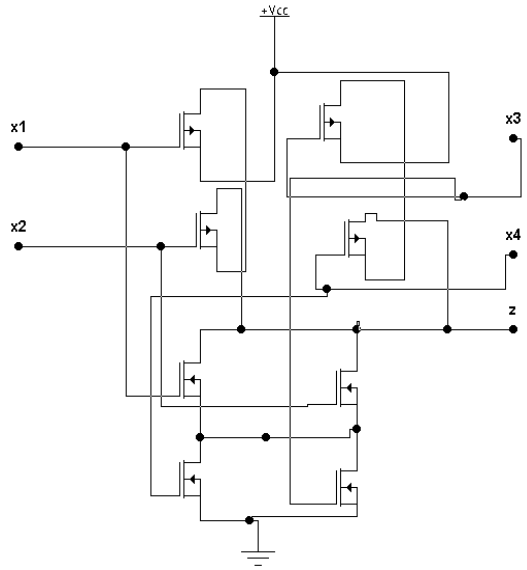

Рис. 1. ФПТБ в виде транзисторной структуры на базе КМОП-транзисторов с p и n каналами

Второй вариант ФПТ элемента, реализующий функцию $(\bar{x}_1 \vee \bar{x}_2)(\bar{x}_3 \vee \bar{x}_4)$ имеет вид, приведенный на рис. 2.

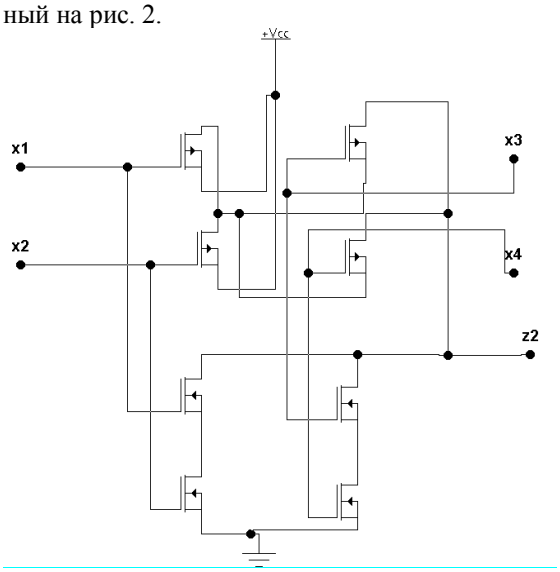

Рис. 2. Второй вариант ФПТБ в виде транзисторной структуры на базе КМОП-транзисторов с p и n каналами

В предлагаемых вариантах имеется избыточность логического базиса, однако структурной избыточности фактически нет. По количеству транзисторов такие элементарные комбинационные автоматы эквивалентны автоматам 4И-НЕ. Причём, цепочка транзисторов от шины +Vcc до общей шины содержит 4 транзистора, а у элемента 4И-НЕ – 5 транзисторов, что даёт непреднамеренный выигрыш в быстродействии!

В качестве дополнительного преимущества для такого избыточного базиса, сочетающего функции И-НЕ, ИЛИ-НЕ имеется существенный выигрыш в сложности при реализации достаточно широкого класса логических функций.

Представление в ФПТБ имеет вид:

$$f = \bigvee_{i=1}^{r} \&_{j=1}^{S_i} x_i \rightarrow \bar{f}_{1.1}\bar{f}_{1.2} \vee \bar{f}_{2.1}\bar{f}_{2.2}, \qquad (8)$$

где r – число конъюнкций в ДНФ, S_i – число переменных в i-й конъюнкции.

В свою очередь, подфункции $f_{1.1}$, $f_{1.2}$, $f_{2.1}$, $f_{2.2}$ исходной функции могут быть представлены в виде

$$f_{ij} = \bar{f}_{ij.1.1}\bar{f}_{ij.1.2} \vee \bar{f}_{ij.2.1}\bar{f}_{ij.2.2}, \qquad (9)$$

и так далее, пока подфункции на определенном шаге не будут реализовываться одним элементом.

Такое представление должно быть оптимальным по показателю количества операций вида $\bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4$.

В качестве примера реализуем логическую функцию «сумма по модулю два» двух переменных

$$m2 = \bar{x}_2 x_1 \vee x_2 \bar{x}_1 = \bar{x}_2 \overline{=} x_1 \vee \overline{=} x_2 \bar{x}_1. \qquad (10)$$

Необходимо 3 элемента с базисом $\bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4$, при наличии парафазных входов – 1 элемент. Реализация в базисе $\overline{x_1 x_2 x_3 x_4}$ потребует 5 элементов, а при наличии парафазных входов – 3 элемента:

$$\overline{\overline{=}\,\overline{x_2 x_1 x_2 x_1}}. \qquad (11)$$

Реализуем логическую функцию «сумма по модулю два» трёх переменных

$$\begin{aligned} m3 &= \bar{x}_3\bar{x}_2 x_1 \vee \bar{x}_3 x_2 \bar{x}_1 \vee x_3 \bar{x}_2 \bar{x}_1 \vee x_3 x_2 x_1 = \\ &= \bar{x}_3(\bar{x}_2 x_1 \vee x_2 \bar{x}_1) \vee x_3(\bar{x}_2 \bar{x}_1 \vee x_2 x_1). \end{aligned} \qquad (12)$$

После преобразований по закону двойной инверсии выражений в скобках, получим:

$$m3 = \bar{x}_3 \overline{(\bar{x}_2 x_1 \vee x_2 \bar{x}_1)} \vee x_3 \overline{(\bar{x}_2 \bar{x}_1 \vee x_2 x_1)}. \qquad (13)$$

Итак, при наличии парафазных входов необходимо всего 3 элемента с базисом $\bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4$, иначе – 6 элементов (добавляются 3 инвертора по числу переменных). Можно показать, что реализация в базисе $\overline{x_1 x_2 x_3 x_4}$ потребует 5 элементов при наличии парафазных входов, иначе 8 элементов.

Разработан метод, алгоритмы и программа автоматизированного синтеза в предлагаемом и остаточных базисах.

Однако после воздействий функции этих ФПТ элементов изменяются, хотя и сохраняется функциональная полнота. Это усложняет процесс восстановления, поскольку необходимо установить, какие функции сохранились, после чего произвести реконфигурацию в соответствии с максимально возможным общим базисом. Если это невозможно, необходимо выбрать максимальное подмножество элементов, обладающих общим базисом.

4. Сохранение функций логического преобразователя при воздействии

Сохранение исходных логических функций возможно методом так называемой учетверённой логики:

$$f = f_1 f_2 \vee f_3 f_4,$$
$$f_1 = f_2 = f_3 = f_4 = f.$$

При изменении любой одной из четырёх функций функция системы не изменяется:

$$f = 1 f_2 \vee f_3 f_4 = f \vee ff = f,$$
$$f_1 = 1.$$
$$f = 0 f_2 \vee f_3 f_4 = 0 \vee ff = f,$$
$$f_1 = 0.$$
$$f = \bar{f}_1 f_2 \vee f_3 f_4 = f\bar{f} \vee ff = 0 \vee ff = f,$$
$$f_1 = \bar{f}_1.$$

В этом случае необходима четырёхкратная избыточность, однако достаточно просто осуществляется объединение этих четырёх функций – используется дизъюнкция. Для сохранения исходных функций возможно также использование трёхкратной избыточности, но при этом применяется более сложная мажоритарная функция:

$$f = f_1 f_2 \vee f_1 f_3 \vee f_2 f_3,$$
$$f_1 = f_2 = f_3 = f.$$

Например,

$$f = 1 f_2 \vee 1 f_3 \vee f_2 f_3 = f \vee f \vee ff = f,$$
$$f_1 = 1$$
$$f = 0 f_2 \vee 0 f_3 \vee f_2 f_3 = 0 \vee 0 \vee ff = f,$$
$$f_1 = 0$$
$$f = \bar{f}_1 f_2 \vee \bar{f}_1 f_3 \vee f_2 f_3 = 0 \vee 0 \vee ff = f,$$
$$f_1 = \bar{f}_1$$

Пусть имеется функция 2ИЛИ-НЕ:

$$f = \bar{x}_1 \bar{x}_2 = \overline{x_1 \vee x_2}.$$

Выполним троирование этого базиса базисными элементами:

$$\overline{\overline{f_1 f_2 \vee f_2 f_3 \vee f_1 f_3}},$$
$$\overline{\overline{f_1 f_2} \vee \overline{f_2 f_3} \vee \overline{f_1 f_3}},$$
$$\overline{\overline{\bar{f}_1 \vee \bar{f}_2 \vee \bar{f}_2 \vee \bar{f}_3}} \vee \overline{\bar{f}_1 \vee \bar{f}_3}.$$

В виде транзисторной КМОП структуры требуется 7 элементов 2ИЛИ-НЕ (а это 28 транзисторов) + инверсии, если их нет, это ещё 3 элемента или 12 транзисторов. Всего 40+12=52 транзистора. Таким образом, мажоритирование базиса по сравнению со сложностью одного базисного элемента приводит к более чем семикратной избыточности. К тому же временная задержка равна 5 задержкам одного 2ИЛИ-НЕ.

Пусть имеется функция 2И-НЕ: $f = \bar{x}_2 \vee \bar{x}_2 = \overline{x_1 x_2}$. Выполним троирование этого базиса базисными элементами:

$$\overline{\overline{f_1 f_2 \vee f_2 f_3 \vee f_1 f_3}},\ \overline{\overline{f_1 f_2 f_2 f_3 f_1 f_2}},\ \overline{\overline{f_1 f_2 f_2 f_3 f_1 f_2}}.$$

В виде транзисторной КМОП структуры требуется 6 элементов 2ИЛИ-НЕ (24 транзистора). Всего 24 + 12 = 36 транзисторов. Таким образом, мажоритирование этого базиса по сравнению со сложностью одного базисного элемента приводит к шестикратной избыточности. К тому же временная задержка равна 4 задержкам одного 2И-НЕ.

5. Разработка модифицированного ФПТБ

Предлагается для сохранения базисной функции ИЛИ-НЕ $\bar{x}_1 \bar{x}_2$ выражение:

$$\bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \vee \bar{x}_5 \bar{x}_6 \bar{x}_7 \bar{x}_8.$$

Легко видеть, что в случае

$$\bar{x}_{1.1} \bar{x}_{2.1} \bar{x}_{1.2} \bar{x}_{2.2} \vee \bar{x}_{1.3} \bar{x}_{2.3} \bar{x}_{1.4} \bar{x}_{2.4}$$

функция ИЛИ-НЕ $\bar{x}_1 \bar{x}_2$ сохранится при любой однократной константной модификации.

Например, при $x_{1.1} = 1$ «обнулится» левая конъюнкция и остаётся $\bar{x}_{1.3} \bar{x}_{2.3} \bar{x}_{1.4} \bar{x}_{2.4}$, что, очевидно, соответствует $\bar{x}_1 \bar{x}_2$, поскольку переменные $x_{1.3} = x_{1.4} = x_1$; $x_{2.3} = x_{2.4} = x_2$.

При $x_{1.1} = 0$

$$\bar{x}_{2.1} \bar{x}_{1.2} \bar{x}_{2.2} \vee \bar{x}_{1.3} \bar{x}_{2.3} \bar{x}_{1.4} \bar{x}_{2.4},$$

что, очевидно, соответствует $\bar{x}_1 \bar{x}_2$, поскольку переменные $x_{1.2} = x_{1.3} = x_{1.4} = x_1$; $x_{2.1} = x_{2.2} = x_{2.3} = x_{2.4} = x_2$. Толерантность сохраняется и при инверсии переменной, например, $x_{1.1}$: $\bar{\bar{x}}_{1.1} \bar{x}_{2.1} \bar{x}_{1.2} \bar{x}_{2.2} \vee \bar{x}_{1.3} \bar{x}_{2.3} \bar{x}_{1.4} \bar{x}_{2.4}$, при этом аналогично $x_{1.1} = 1$ «обнулится» левая конъюнкция. Следовательно, обеспечивается парирование сбоев. Толерантность обеспечивается и при замыкании соседних линий связи, а также при некоторых кратных отказах. Причём, каждый вход и выход учетверяются (рис. 3).

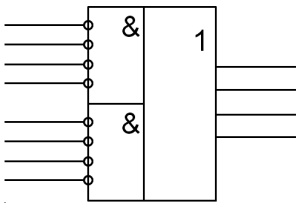

Рис. 3. Условное графическое обозначение элемента с толерантной базисной функцией

Для реализации такой схемы на КМОП-транзисторах необходимо 16 транзисторов (рис. 4).

Разработанный избыточный базис может быть использован как сложный (восьми переменных): $f = \bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \vee \bar{x}_5 \bar{x}_6 \bar{x}_7 \bar{x}_8$.

Например, может быть реализован частично резервированный ФПТ базис

$$\bar{x}_1 \bar{x}_2 \vee \bar{x}_3 \bar{x}_4$$

в виде $f = \bar{x}_1 \bar{x}_2 \bar{x}_1 \bar{x}_2 \vee \bar{x}_3 \bar{x}_4 \bar{x}_3 \bar{x}_4$.

Для сохранения базисной функции 2И-НЕ $\bar{x}_1 \vee \bar{x}_2$ при модели однократных константных отказов может быть предложено выражение:

$$(\bar{x}_1 \vee \bar{x}_2 \vee \bar{x}_3 \vee \bar{x}_4)(\bar{x}_5 \vee \bar{x}_6 \vee \bar{x}_7 \vee \bar{x}_8),$$

т.е. $(\bar{x}_{1.1} \vee \bar{x}_{2.1} \vee \bar{x}_{1.2} \vee \bar{x}_{2.2})(\bar{x}_{1.3} \vee \bar{x}_{2.3} \vee \bar{x}_{1.4} \vee \bar{x}_{2.4})$.

Дальнейшим развитием подхода может быть сохранение более сложного и более эффективного ФПТ базиса $\bar{x}_1\bar{x}_2 \vee \bar{x}_3\bar{x}_4$ – для этого необходима функция

$$(\bar{x}_{1.1}\bar{x}_{2.1}\bar{x}_{1.2}\bar{x}_{2.2} \vee \bar{x}_{1.3}\bar{x}_{2.3}\bar{x}_{1.4}\bar{x}_{2.4}) \vee$$
$$\vee(\bar{x}_{3.1}\bar{x}_{4.1}\bar{x}_{3.2}\bar{x}_{4.2} \vee \bar{x}_{3.3}\bar{x}_{4.3}\bar{x}_{3.4}\bar{x}_{4.4}).$$

Реализация такого элемента требует 32 КМОП-транзистора.

Заключение

В данной работе предложен базисный подход к разработке надежных систем, в соответствии с которым обеспечение надежности осуществляется на уровне базисных компонент. Такие системы могут быть названы естественно надежными, а следовательно (при определенных условиях), и естественно безопасными, поскольку результаты воздействий и отказов парируются на самом нижнем уровне – уровне компонент. Для цифровых систем – это уровень логического базиса. Рассмотренные в статье функционально-полные толерантные базисы обеспечивают естественную в указанном смысле надежность таких систем.

В общем случае автоматно-базисный подход может быть применен для создания естественно надежных и безопасных инфраструктур. При этом возникает проблема выбора базиса и обеспечения его устойчивости к воздействиям заданного типа. Ее решение требует проведения дальнейших теоретических исследований и разработок.

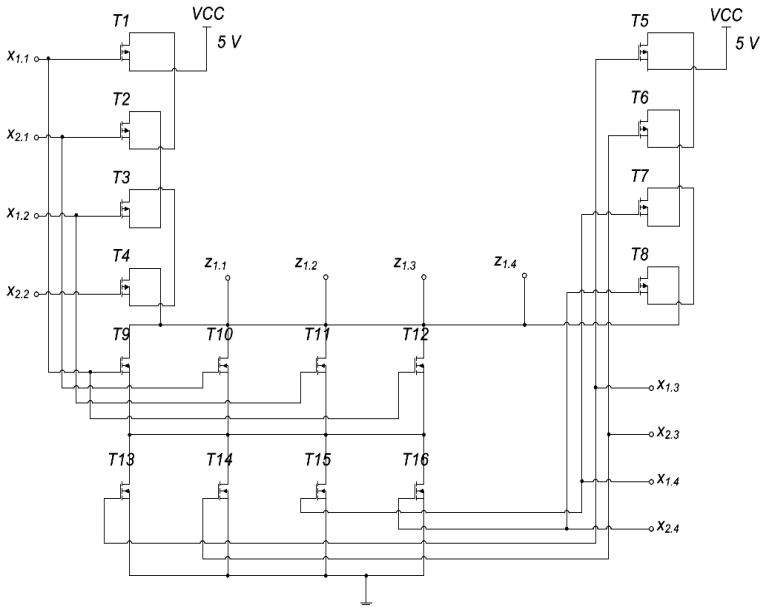

Рис. 4. Реализация базисного элемента ФПТ+ на КМОП-транзисторах

Список литературы

1. Von Neumann J. Probabilistic Logic and the Synthesis of Reliable Organisms from Unreliable Components. Automata Studies / J. Von Neumann; C. Shannon, J. McCarthy (eds). Princeton University Press, 1956. – P. 43-98.

2. Avižienis A. Fault-Tolerance: The survival attribute of digital system / A. Avižienis // Proc. of the IEEE. – 1978. – Vol. 66, № 10. – P. 1109-1125.

3. Avizienis A. Dependable Computing: From Concepts to Application / A. Avizienis, J.-C. Laprie // IEEE Trans. on Computers. – 1986. – №74 (5). – P. 629-638.

4. Avižienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

5. Харченко В.С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції / В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2009. – №7. – С. 46-59.

6. TR 026764, ReSIST: Resilience for Survivability in IST. Deliverable D12. Resilience-Building Technologies: State of Knowledge, September 2006. – 345 p.

7. Харченко В.С. Научно-методические результаты в области развития гарантоспособных систем / В.С. Харченко //Радіоелектронні і комп'ютерні системи. – 2009. – №4. – С. 24-33.

8. Айзенберг Я.Е. Сопоставление принципов обеспечения безопасности систем управления ракето-носителями и атомными электростанциями / Я.Е. Айзенберг, М.А. Ястребенецкий // Космічна наука та технологія. – 2002. – № 1. – С. 55-60.

9. Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика: уч. пособ. для вузов / В.А. Горбатов. – М.: Наука, 2000. – 540 с.

10. Кузнецов О.П. Дискретная математика для инженера / О.П. Кузнецов. – 3-е изд., перераб. и доп – СПб.: Лань, 2004. – 395 с.

11. Марченков С.С. Замкнутые классы булевых функций / С.С. Марченков. – М.: Физматлит, 2000. – С. 18.

12. Иыуду К. Надежность, контроль и диагностика вычислительных машин и систем / К. Иыуду. – М.: Высшая школа, 1989. – 219 с.

13. Тюрин С.Ф. Функционально-полные толерантные булевы функции / С.Ф. Тюрин // Наука и технология в России. – 1998. – № 4. – С. 7-10.

14. Тюрин С.Ф. Синтез адаптируемой к отказам цифровой аппаратуры с резервированием базисных функций / С.Ф. Тюрин // Приборостроение. – 1999. – № 1. – С. 36-39.

15. Тюрин С.Ф. Адаптация к отказам одновыходных схем на генераторах функций с функционально-полными толерантными элементами / С.Ф. Тюрин // Приборостроение. – 1999. – № 7. – С. 32-34.

16. Тюрин С.Ф. Проблема сохранения функциональной полноты булевых функций при «отказах» аргументов / С.Ф. Тюрин // Автоматика и телемеханика. – 1999. – № 9. – С. 176-186.

17. Пат. 2146840 Российская Федерация. Программируемое логическое устройство / Тюрин С.Ф., Несмелов В.А., Харитонов В.А. и др. Опубл. БИ № 8. 2000 г.

Поступила в редколлегию 7.12.2010

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

АВТОМАТНО-БАЗІСНИЙ ПІДХІД ДО СТВОРЕННЯ ПРИРОДНЬО НАДІЙНИХ І БЕЗПЕЧНИХ СИСТЕМ

С.Ф. Тюрін, В.С. Харченко

Пропонується підхід до створення природньо надійних і безпечних систем, толерантних до відмов (різних негативних впливів). Сформульовано основні принципи автоматно-базисного підходу. Він фундується на використанні надлишкового базису, який дозволяє виконувати всі або частину функцій при відмовах. Система описується автоматною моделлю, а відновлення логічного перетворювача реалізується шляхом використання запропонованих функційно-повних толерантних базисів (ФПТБ). Наведено приклади ФПТБ на вентильному рівні.

Ключові слова: *надлишковий базис, автоматна модель, функційно-повний толерантний базис, відмова, вплив.*

AUTOMATON-BASIS APPROACH TO DEVELOPMENT OF NATURALLY DEPENDABLE AND SAFE SYSTEMS

S.F. Tyurin, V.S. Kharchenko

An approach to development of naturally dependable and safe systems which are tolerant to failures (different types of intrusions) is suggested. Basic principles of automaton-basis approach are formulated. It is based on use of redundant basis allowing to carry out all or part of functions on failures. A system is described by automaton model and recovery of logical transformer is performed using by application of proposed function-full tolerant basis (FFTB). Examples of FFTBs on the gated level are analyzed.

Keywords: *redundant basis, automaton model, function-full tolerant basis, failure, intrusion.*