

СТРУКТУРНЫЙ СИНТЕЗ И АНАЛИЗ ОТКАЗОУСТОЙЧИВЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

*Институт проблем математических машин и систем НАН Украины, Киев, Украина

**АЕС «Киевоблэнерго», Киев, Украина

Анотація. Розглянуті питання структурного синтезу та аналізу відмовостійких систем на прикладі квазімісткової структури з самоперевіренням. Приведені результати моделювання структури засобами пакетів програм RELIABmod та Matlab Simulink+Stateflow.

Ключові слова: квазімісткова структура, відмовостійкість, реконфігурація, моделювання.

Аннотация. Рассмотрены вопросы структурного синтеза и анализа отказоустойчивых компьютерных систем на примере самопроверяемой квазимостиковой структуры. Приведены результаты моделирования структуры средствами пакетов программ RELIABmod и Matlab Simulink+Stateflow.

Ключевые слова: квазимостиковая структура, отказоустойчивость, реконфигурация, моделирование.

Abstract. In this paper there were discussed the problems of structural synthesis and analysis of fault-tolerant computer systems: a case of self-checking quasibridging structure. The results of structure modeling by means of RELIABmod and Matlab Simulink+Stateflow software packages were given.

Keywords: quasibridging structure, fault tolerance, reconfiguration, modeling.

1. Введение

Анализ и классификация отказоустойчивых структур, проведенные в [1], показали, что основным недостатком всех дублированных структур со слабыми, умеренными и сильными связями является их невысокая эксплуатационная готовность. Это связано с тем, что любой отказ в одном из каналов переводит систему либо в нерабочее защитное состояние, либо в работу по одному исправному каналу (в зависимости от логической функции восстанавливающего органа (ВО), являющегося выходной схемой системы).

Рассмотрим самопроверяемую дублированную структуру (рис. 1), состоящую из двух вычислительных каналов (условно ЭВМ), снабженных самопроверяемой схемой внутреннего контроля (ССВК), задачей которой является обнаружение неисправностей заданного класса в вычислительном канале и собственных неисправностей. Самопроверяемые

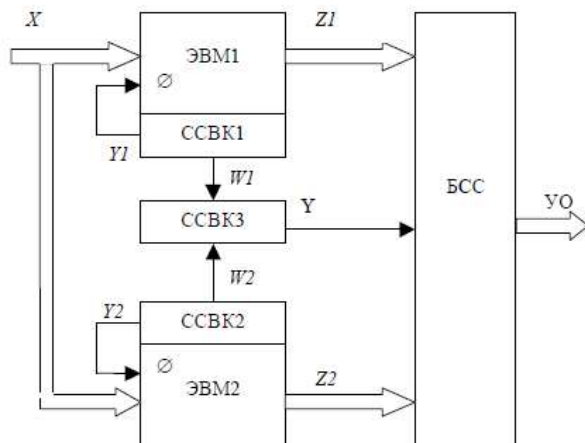


Рис. 1. Самопроверяемая дублированная структура

схемы внутреннего контроля каждого канала при обнаружении ошибки вырабатывают сигнал Y1 или Y2, который отключает соответствующий вычислительный канал.

Выходные сигналы Z1 и Z2 сравниваются безопасной схемой сравнения (БСС). При совпадении сигналов формируется управляющее воздействие на управляемый объект (УО). Сигналы контроля W1 и W2, формируемые с помощью ССВК1 и ССВК2, сравниваются в ССВК3. При обнаружении ошибки ССВК3 вырабатывает сигнал Y, который переводит БСС в защитное состояние.

Минимальная кратность необнару-

живаемых отказов равна 4 – по два отказа в каждом канале, которые не обнаруживаются ССВК1 и ССВК2 и одинаковым образом искажают выходные сигналы Z1 и Z2. Самоконтроль каналов может быть аппаратный и программный. Возможно использование независимых (диверситетных) программ в каждом вычислительном канале.

Основным достоинством данной структуры являются высокая глубина контроля вычислительных каналов и возможность диагностики отказавшего канала, а также высокая безопасность структуры в целом. В качестве недостатков следует отметить сложность синтеза ССВК1,2 для вычислительного канала (ЭВМ) в целом и, как уже отмечалось выше, невысокая эксплуатационная готовность, так как любой отказ канала или ССВК переводит систему в нерабочее защитное состояние.

2. Структурный синтез самопроверяемой квазимостиковой структуры

С целью повышения эксплуатационной готовности в [2] был предложен новый класс самопроверяемой дублированной структуры с реконфигурацией, позже получившей название квазимостиковой. Повышение безотказности и эксплуатационной готовности такой структуры достигается ее декомпозицией, при которой каждый вычислительный канал (ЭВМ) разбивается на n микроконтроллеров (далее по тексту – элементов структуры Э), которые с помощью схем реконфигурации (СР) образуют n дублированных узлов.

Если ЭВМ разбивается на условно равнонадежные Э (например, ЭВМ1.1 и ЭВМ1.2, ЭВМ2.1 и ЭВМ2.2), то средняя наработка до отказа такого Э может быть ориентировочно оценена по формуле [3] $T_{\text{Э}} = \sqrt{n} \cdot T_{\text{ЭВМ}}$. Схема декомпонированной структуры, состоящей из двух узлов, приведена на рис. 2.

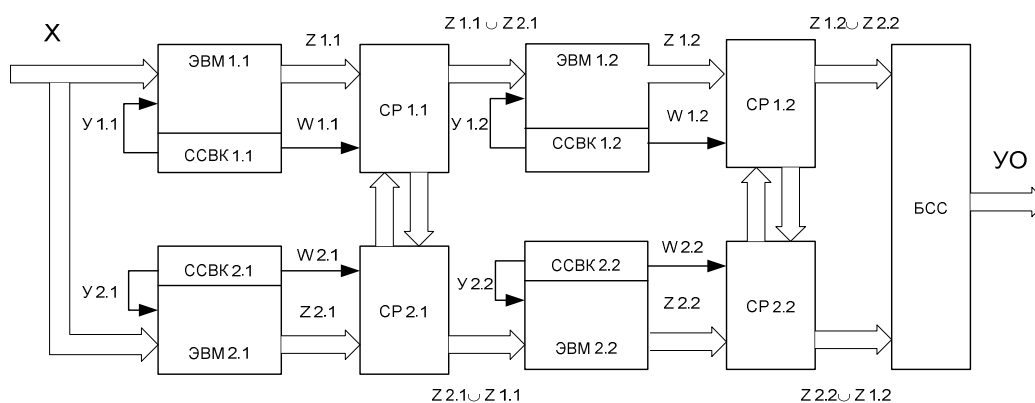


Рис. 2. Самопроверяемая квазимостиковая структура

Визуально она напоминает мостиковую структуру ССН-4, в которой, вместо центрального типового элемента структуры, установлены две СР (по одной в каждый канал), которые обеспечивают перекрестные связи между каналами с целью реконфигурации структуры в случае выхода из строя соответствующего Э канала. Такая структура и получила название “квазимостиковой”.

3. Анализ логической функции структуры

Запишем логическую функцию дублированной структуры, изображенной на рис. 1.

$$F_{\text{д}} = z_1 \cdot z_2. \quad (1)$$

Проводя аналогию двух структур (рис. 1, 2), можно записать:

$$z_1 = z_{1.1} \cdot z_{1.2} \text{ и } z_2 = z_{2.1} \cdot z_{2.2}. \quad (2)$$

Откуда

$$F_D = z_1 \cdot z_2 = z_{1.1} \cdot z_{1.2} \cdot z_{2.1} \cdot z_{2.2}. \quad (3)$$

Запишем логические функции узлов для квазимостиковой структуры, изображенной на рис. 2.

$$\begin{aligned} f_{1.1} &= z_{1.1} \cup z_{2.1}; f_{1.2} = z_{1.2} \cup z_{2.2}, \\ f_{2.1} &= z_{2.1} \cup z_{1.1}; f_{2.2} = z_{2.2} \cup z_{1.2}. \end{aligned} \quad (4)$$

Запишем логическую функцию квазимостиковой структуры через логические функции узлов:

$$F_{KM} = (f_{1.1} \cdot f_{1.2}) \cdot (f_{2.1} \cdot f_{2.2}) = [(z_{1.1} \cup z_{2.1})(z_{1.2} \cup z_{2.2})] \cdot [(z_{2.1} \cup z_{1.1})(z_{2.2} \cup z_{1.2})]. \quad (5)$$

С учетом (2) и принимая во внимание (3), получим

$$\begin{aligned} F_{KM} &= z_1 \cup z_2 \cup z_1 \cdot z_2 \cup z_1 \cdot z_{1.2} \cdot z_{2.1} \cup z_1 \cdot z_{1.1} \cdot z_{2.2} \cup z_2 \cdot z_{1.1} \cdot z_{2.2} \cup \\ &\cup z_2 \cdot z_{1.2} \cdot z_{2.1} \cup z_{1.1} \cdot z_{2.2} \cup z_{1.2} \cdot z_{2.1}. \end{aligned} \quad (6)$$

Рассматривая (6), нетрудно видеть, что квазимостиковая структура характеризуется более высоким уровнем отказоустойчивости и, как следствие, эксплуатационной готовности, так как имеет значительно большее количество работоспособных состояний, чем простая дублированная структура. Наличие работоспособных состояний на импликантах $z_1 \cup z_2$ свидетельствует о том, что квазимостиковая структура, изображенная на рис. 2, способна к автоматической реконфигурации в одноканальную структуру без дополнительного вмешательства и изменения функции ВО.

4. Анализ надежности структуры методом статистического моделирования

Для анализа надежности квазимостиковой структуры был использован специально разработанный пакет программ статистического моделирования надежности сложных систем – RELIABmod v.2.0 [4]. В качестве теоретической модели надежности всех компонентов структуры использовалось диффузионное немонотонное распределение (DN-распределение) наработки до отказа [3].

Примечания:

1. «Суммарная надежность» ССВК1.1 (ССВК2.1) и ССВК1.2 (ССВК2.2) приблизительно равна надежности ССВК1 (ССВК2).

2. Схемы реконфигурации СР1.1 (СР1.2) и СР2.1(СР2.2) реализуются на мультиплексоре, имеют малое количество логических элементов, легко резервируются и в первом приближении считаются абсолютно надежными.

В процессе исследований установлено, что уже при количестве узлов $n > 4$ средняя наработка до отказа самопроверяемой квазимостиковой структуры (рис. 2) превышает аналогичный показатель для структуры, изображенной на рис. 1. Использование декомпозиции структуры вычислительного канала на ряд микроконтроллеров (Э) и образование из них так называемых узлов приводит также к значительному увеличению и вероятности безотказной работы. Интересным является и тот факт, что с увеличением количества узлов коэффициент вариации наработки до отказа структуры существенно уменьшается, что, наряду с ростом средней наработки до отказа, также является причиной роста вероятности безотказной работы.

5. Анализ функционирования структуры методом имитационного моделирования

Работа квазимостиковой структуры моделировалась средствами пакета имитационного моделирования Matlab Simulink+Stateflow с целью проверки ее соответствия выражению (5). Для построения модели структуры использовались логические блоки OR/AND (рис. 3). Моделирование отказа Э структуры осуществлялось с помощью сигнала Pulse Generator, который активировал функцию нормального распределения $\text{exprnd}(1)$. Данный подход позволил генерировать случайные значения вероятности отказа соответствующих Э структур от 0 до 1 и формировать сигнал работоспособности (1) или отказа (0) на выходах $z_{1.1}, z_{1.2}, z_{2.1}, z_{2.2}$.

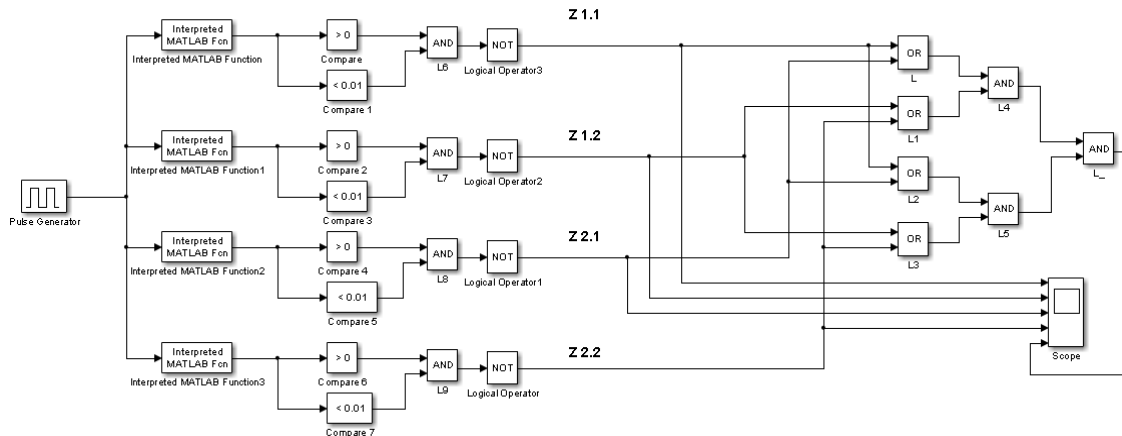


Рис. 3. Имитационная модель квазимостиковой структуры

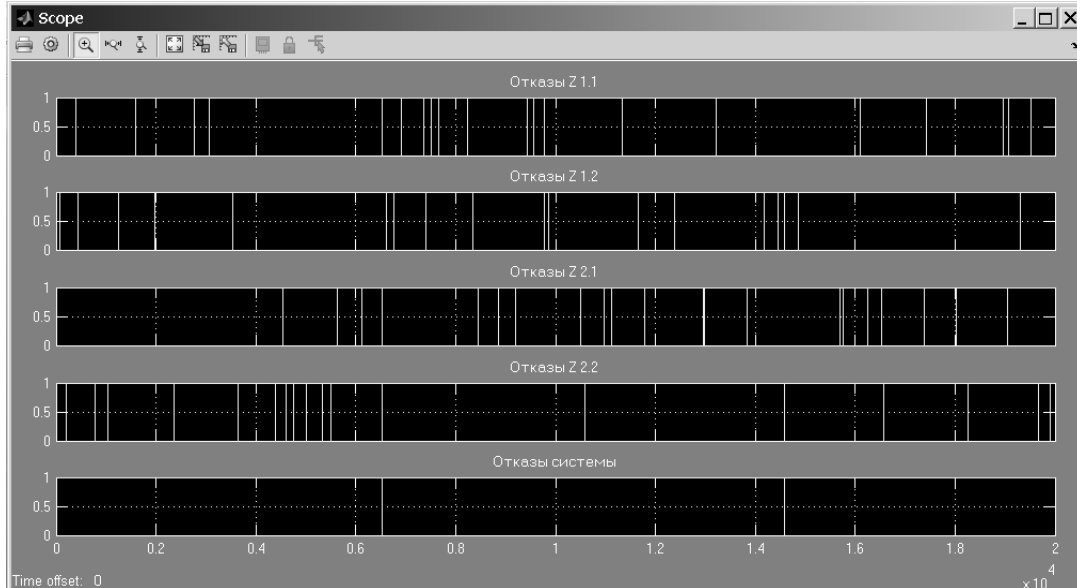


Рис. 4. Диаграмма состояний квазимостиковой структуры

Результаты моделирования сравнивались с таблицей истинности (табл. 1), построенной по выражению

$$F_{KM} = [(z_{1.1} \cup z_{2.1})(z_{1.2} \cup z_{2.2})] \cdot [(z_{2.1} \cup z_{1.1})(z_{2.2} \cup z_{1.2})].$$

Таблица 1. Таблица истинности

	$z_{1.1}$	$z_{1.2}$	$z_{2.1}$	$z_{2.2}$	УО
1	1	1	1	1	1
2	0	1	1	1	1
3	1	0	1	1	1
4	1	1	0	1	1
5	1	1	1	0	1
6	1	0	0	1	1
7	0	1	1	0	1
8	1	0	1	0	0
9	0	1	0	1	0
10	0	0	1	1	1
11	1	1	0	0	1
12	1	0	0	0	0
13	0	1	0	0	0
14	0	0	1	0	0
15	0	0	0	1	0
16	0	0	0	0	0

моконтроля и реконфигурации.

СПИСОК ЛИТЕРАТУРЫ

1. РТМ 32 ЦШ 1115842.01 – 94. Безопасность железнодорожной автоматики и телемеханики. Методы и принципы обеспечения безопасности микроэлектронных СЖАТ. – СПб.: ПГУПС, 1994. – 2 с.
2. Федухин А.В. К вопросу об аппаратной реализации избыточных структур: резервированная двухканальная система с реконфигурацией / А.В. Федухин, Ар.А. Муха // Математичні машини і системи. – 2010. – № 4. – С. 156 – 159.
3. Стрельников В.П. Оценка и прогнозирование надежности электронных элементов и систем / В.П. Стрельников, А.В. Федухин. – К.: Логос, 2002. – 486 с.
4. Федухин А.В. Моделирование надежности систем / А.В. Федухин, В.П. Пасько // Методы менеджмента качества. – 2012. – № 3. – С. 50 – 55.

Стаття надійшла до редакції 25.04.2013

Средствами пакета Matlab Simulink+Stateflow были подтверждены работоспособность и ожидаемая отказоустойчивость квазимостиковой структуры. Показано, что отказ структуры наступает только в случае одновременного отказа Э, принадлежащих одному узлу (отказы кратности 2, строки 8,9 и отказы кратности 3, строки 12-16). Вероятность кратного отказа при наличии системы восстановления работоспособности Э практически очень мала.

6. Выводы

Использование на практике самопроверяемой квазимостиковой структуры для проектирования гарантоспособных систем критического использования открывает новые возможности в направлении повышения их эксплуатационной надежности при незначительном увеличении аппаратных затрат на реализацию функции са-