

Методи оцінки та забезпечення необхідного рівня технічної безпеки роботи спеціалізованих багатопроцесорних систем управління

Методы оценки и обеспечения необходимого уровня технической безопасности работы специализированных многопроцессорных систем управления

Methods of evaluation and guarantee of technical security's required level for specialized multiprocessor control systems' functioning

- 1. Номер державної реєстрації теми - 0115U000323,**
- 2. Науковий керівник - д.т.н., проф. Романкевич О.М., Романкевич Алексей Михайлович, Romankevych Oleksiy**

3. Суть розробки, основні результати.

(укр.) Метою роботи є розробка методів та засобів визначення ймовірності переходу реконфігурованої багатопроцесорної системи (БС) управління складним об'єктом у небезпечний стан та підвищення вірогідності результатів роботи системи. Під час експлуатації помірі виходу з ладу процесорів БС може перейти у небезпечний стан (стан, коли не може бути реалізована хоч би одна з функцій управління, без якої об'єкт управління переходить у небезпечний стан). Запропоновано методи розрахунку ймовірності виникнення такої ситуації у двох напрямках: коли множина векторів небезпечних станів системи відома та коли – ні. Методи базуються на виконанні статистичних експериментів з моделями поведінки БС у потоку відмов. Виведено відповідні формули, дано їх теоретичне обґрунтування. Запропоновано метод організації взаємо тестування процесорів у БС для 3- та 4-відмовостійких n-процесорних БС. Верше у світовій практиці число тестуючи процесорів менше числа відмов, що допускається. Метод базується на новому конструктивно-регулярному діагностичному графі та подальшому аналізі результатів. Показано, що загальна кількість взаємоперевірок не перевищує величини $2n+2$, що декілька разів менше відомих методів. Для виконання статистичних експериментів необхідно мати джерело векторів стану БС. Запропонована конкретна схема генератора псевдовипадкових двійкових векторів, що відповідає всім необхідним вимогам, зокрема генератор повинен бути швидкодіючим, рівноваговим та керованим.

Для аналізу наслідків збоїв запропоновані моделі ймовірностей значень сигналів на виходах цифрових пристроїв. Властивістю запропонованої моделі є можливість комплексного врахування як спотворень на входах пристрою, так і збоїв у самому пристрою. Моделі враховують структуру цифрових пристроїв та фізичну природу спотворень даних. На основі моделей запропоновано методи зменшення обсягу обчислень достовірності функціонування комп'ютерних пристроїв та методи оптимізації пристроїв з метою підвищення достовірності їх функціонування.

(рос.)

Целью работы является разработка методов и средств определения вероятности перехода реконфигурируемой многопроцессорной системы (МС) управления сложным объектом в опасное состояние и повышение достоверности результатов работы системы. В процессе эксплуатации по мере выхода из строя процессоров МС может перейти в опасное состояние (состояние, когда не может быть реализована хотя бы одна из функций управления, без которой объект управления переходит в опасное состояние). Предложены методы расчета вероятности появления такой ситуации в двух направлениях: когда множество векторов опасных состояний системы управления известно и когда - нет. Методы основаны на выполнении статистических экспериментов с моделями поведения МС в потоке отказов. Выведены соответствующие формулы, дано их теоретическое обоснование. Предложен метод организации взаимного тестирования процессоров в МС для 3- и 4-отказоустойчивых

n-процессорных МС Впервые в мировой практике число тестирующих процессоров менее числа допустимых отказов. Метод основан на новом конструктивно-регулярном диагностическом графе и последующем анализе результатов. Показано, что общее число взаимопроверок не превышает величины $2n+2$, что в несколько раз меньше известных методов. Для выполнения статистических экспериментов необходим источник векторов состояния МС. Предложена конкретная схема генератора псевдослучайных двоичных векторов, отвечающая всем необходимым требованиям, в частности, генератор должен быть быстродействующим, равновесным и управляемым.

Для анализа последствий сбоев предложены модели вероятностей значений сигналов на выходах цифровых устройств. Свойством предложенной модели является возможность комплексного учета как искажений на входах устройства, так и сбоев в самом устройстве. Модели учитывают структуру цифровых устройств и физическую природу искажений данных. На основе моделей предложены методы уменьшения объема вычислений достоверности функционирования компьютерных устройств и методы оптимизации устройств с целью повышения достоверности их функционирования.

(англ.)

Purpose of the work is design of methods and means for determination of transition's probability of reconfigurable multiprocessor system (MS) aimed to control the complex objects. This transition can lead to dangerous state. Also as result of the work is enhance of system functioning results' veracity. During exploitation due to the processors' failures MS can went into dangerous state (that is state when is only one (any) of control functions can not be realized and without of those the control object went into dangerous state). The methods to design the probabilities of existence of such in two directions, when the set of control system's dangerous state vectors is known and when it is not. Methods are based on implementation of statistic experiments with behavior of MS under failure flow. Relevant formulas are obtained and theoretic justification is given. The method of organization of processors' mutual testing in MS for 3- and 4-fault-tolerant n-processor MS is proposed. Firstly in world practice the number of testing processors is lesser then the number of allowed faults. The method is based on new constructive-regular diagnostic graph and next analysis of results. It is shown that whole the number of mutual tests is no more than $2n+2$ and is lesser then of ones for known methods. For implementation of statistic experiments a source of state MS' vectors is needed. A specific circuit of pseudorandom binary vectors' generator is proposed. The circuit corresponds to all needed requirements in particularly it must be high speeded, equal weighted and controllable.

To analyze consequences of failures the probabilities models of signals values on the outputs are proposed. A property of the model proposed is the possibility to comprehensively take into account both the distortions on the device' inputs and the failures within the device. The models take the digital devices structure into account and the physical essence of the data distortion. Based on the models the methods for reduction of calculations volume of the functioning of computer devices validity and the methods for devices optimization in order to increase its functioning validity.

4. Наявність охоронних документів на об'єкти права інтелектуальної власності.

1. Гроль В.В., Коваль І.О., Фаллагі Алі Сармаст. Комп'ютерна програма «Програма для отримання множини векторів стану систем, що відрізняють графологічну модель від базової»// Свідоцтво про реєстрацію авторського права на твір № 59823 від 27.05.2015р.
2. Потапова К.Р., Трошина М.І., Морозов К.В., Корнейчик Б.А. Комп'ютерна програма «Програма підтримки експериментів з графо-логічними моделями відмово стійких багатопроцесорних систем» // Свідоцтво про реєстрацію авторського права на твір

№ 59822 від 27.05.2015р.

3. Романкевич В.О., Яшунін В.О., Вербицький Є., Олійник В.В. Комп'ютерна програма «Програма для знаходження 0-ланцюжків під час самодіагностування у багатопроцесорних системах» // Рішення про реєстрацію договору, який стосується права автора на твір №2895 від 01.03.2016р
4. Потапова К.Р., Яшунін В.О., Кічігін Н.К., Олійник В.В. Комп'ютерна програма «Програма для визначення станів процесорів багатопроцесорної системи під час моделювання процесу самодіагностування» // Рішення про реєстрацію договору, який стосується права автора на твір №2894 від 01.03.2016р
5. Шаповал І.І., Тесленко О.К. Модифікація жадібного алгоритму пошуку кліки в графі Хемінга. Свідоцтво про реєстрацію авторського права на твір №61201 від 25.05.2015р.
6. Невмержицький П.А., Тесленко О.К. "Алгоритм шифрування, який ґрунтується на суперпозиції підстановок із найпростіших регулярних ОККМ" Свідоцтво про реєстрацію авторського права на твір. № 66618 Дата реєстрації 13.07.2016
7. Патент на корисну модель № 100006 G06F 7/00. Багаторозрядний суматор зі змінним модулем з груповим переносом / Клятченко Я.М.; Роговенко А.І.; Тарасенко В.П.; Тесленко О.К.; Шепотіннік О.Ю.; НТУУ КПІ; заявл. 21.03.2014; опубл. 10.07.2015, бюл. №13.Власник НТУУ «КПІ»

5. Порівняння зі світовими аналогами.

Результати відповідають світовому рівню, а метод організації взаємо тестування у БС не має аналогів у світовій інженерній практиці. Крім того, метод тестування 3- та 4-відмовостійких БС з оцінкою $2n+2$ перевірок при незалежному паралельному тестуванні за ефективністю перевищують світовий рівень. Запропоновані методи обчислень достовірності функціонування комп'ютерних пристроїв не мають аналогів у світовій практиці комп'ютерної інженерії.

6. Економічна привабливість для просування на ринок

Розроблені методи, алгоритми, моделі та програми дозволяють знизити собівартість проектування та розробки багатопроцесорних систем управління, зокрема, за рахунок:

- скорочення часу тестування щонайменше у двічі;
- зменшення витрат на багатoversійну розробку процесорних пристроїв на 20 – 30 %;
- суттєве зменшення (на декілька порядків) обсягів обчислень достовірності функціонування процесорних пристроїв, зокрема суматорів на 32 та 64 розряди.

7. Потенційні користувачі (галузі, міністерства, підприємства, організації). Методи, моделі, алгоритми можуть бути застосовані в інститутах, проектних установах та підприємствах, що займаються розробкою багатопроцесорних систем управління складними і надскладними об'єктами.

8. Стан готовності розробки.

По запропонованим методам розроблено алгоритми та відлагоджено програми. Достовірність отриманих результатів підтверджена

- шляхом експериментів на розроблених прототипах програмних комплексів
- шляхом моделювання на загально прийнятих мовах програмування;
- шляхом моделювання на САПР ПЛІС WebPACK ISE та шляхом фізичної реалізації на ПЛІС.

9. Існуючі результати впровадження.

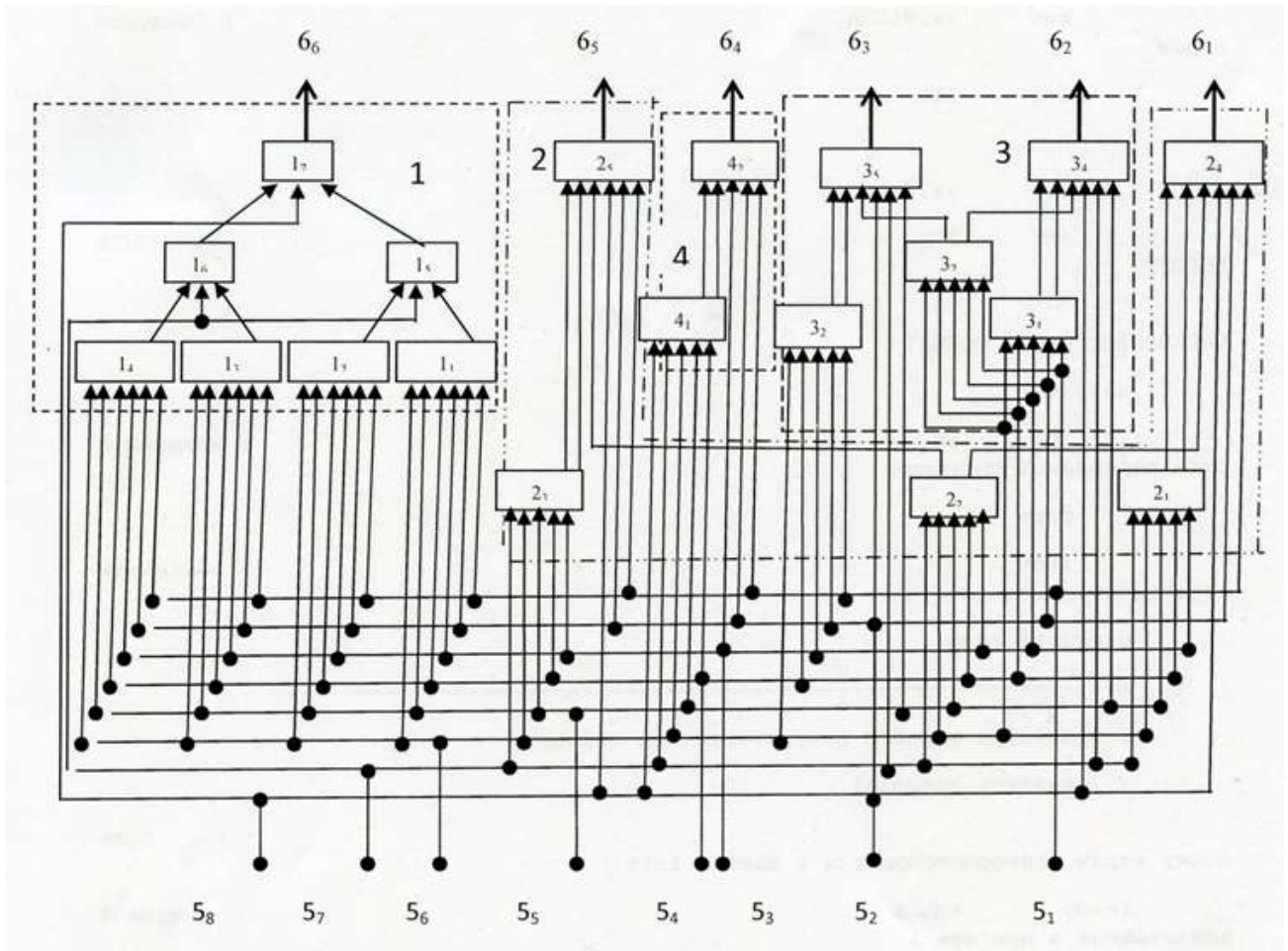
Результати роботи, зокрема ті, що стосуються організації процесу взаємотестування процесорів, використовуються у наукових дослідженнях інституту проблем математичних машин та систем НАНУ. Попередні експерименти підтверджують певну ефективність алгоритму в плані зменшення часу тестування.

Теоретичні основи побудови та застосування нових методів діагностування та організації процедур тестування у багатопроцесорних системах управління використовуються у дисципліні “Тестування, надійність, контроль та діагностика комп’ютерних систем” (нові засоби забезпечення надійності систем) спеціальностей “Спеціалізовані комп’ютерні системи”, “Системне програмування” та “Комп’ютерні системи та компоненти”. Одержані результати також використовуються в дисципліні «Дослідження і проектування СКС» (розділ «Проектування СКС на ПЛІС»), в лабораторній роботі «Проектування моделі цифрової частини передавача та приймача GPS»).

10. Назва організації, телефон, E-mail

КПІ ім. Ігоря Сікорського, факультет прикладної математики, кафедра системного програмування і спеціалізованих комп’ютерних систем, 044-236-3202, romankev@scs.ntu-kpi.kiev.ua

11. Фото розробки.



12. Перелік публікацій за матеріалами досліджень за період виконання (вагомі):
(монографії, підручники, посібники, наукові статті, дисертації, інші публікації).
Монографії:

- О. Корченко, І. Терейковський, А. Білощицький. Методологія розроблення нейромережових засобів інформаційної безпеки Інтернет-орієнтованих інформаційних систем. К. ТОВ «Наш Формат». 2016, 249 с
- Бояринова Ю.Є., Калиновский Я.А., Сукало А.С. Гиперкомплексные числовые системы четвертой размерности.- Киев, ИПРИ НАНУ Х.: Express-kniga 126с

Навчальні посібники

- Теоретичні основи комп'ютерних напівпровідникових електронних компонентів: навчальний посібник./ [Азаров О.Д., Гарнага В.А., Сапсай Т.Г., Тарасенко В.П.] – Вінниця: ВНТУ, 2015.-135с.
- Дослідження і проектування СКС [Електронний ресурс] : завдання для виконання лабораторних робіт для студентів спеціальності 8.05010203 «Спеціалізовані комп'ютерні системи» / НТУУ «КПІ»; уклад. Я. М. Клятченко, О. К. Тесленко. - Електронні текстові дані (1 файл: 2,27 Мбайт). - Київ : НТУУ «КПІ», 2015. - 47 с. - Назва з екрана. - Доступ : <http://ela.kpi.ua/handle/123456789/13792>
- Ю.М.Зорін, В.П.Тарасенко. Методи та алгоритми обчислень. Навчальний посібник. Видавництво «Корнійчук», Київ, 2016, с.168.

Докторські дисертації:

Романкевич Віталій Олексійович. Методи і засоби оцінки технічних характеристик гарантоздатності відмовостійких багатопроцесорних систем управління складними об'єктами. Дата прийняття Вченою радою до захисту – 13.11.2017

Терейковський Ігор Анатолійович. Назва дисертації - Нейромережеві моделі, методи і засоби оцінювання параметрів безпеки інтернет-орієнтованих інформаційних систем. Дата захисту – 28(29).05.2015

Кандидатська дисертація:

Цибаєв Євгеній Ігорович. Методи і засоби прогнозування часу виконання програм в спеціалізованих комп'ютерних системах. Дата захисту – 08.06.2015

Статті

1. Romankevich A. M., Romankevich V. A. Diagnosis of multiprocessor systems under failure of more than half processors // Automation and Remote Control. – 2017. – Vol. 78, Issue 9. – P. 1614 – 1618. (Видання реферується наукометричною базою **SCOPUS**)
2. Romankevich V. A. Self-testing of multiprocessor systems with regular diagnostic connections // Automation and Remote Control. – 2017. – Vol. 78, Issue 2. – P. 289 – 299. (Видання реферується наукометричною базою **SCOPUS**)
3. Rabah AlShboul, Vitaliy A. Romankevich. Structural Means Generating Pseudorandom Sequences Of Fixed Weight Binary Patterns // IJCSNS International Journal of Computer Science and Network Security. – 2017. – Vol. 17, No.10. – P. 62 – 66. (Видання реферується наукометричною базою **Web of Science**)
4. Tarassenko V., Romankevych V., Feseniuk A. Statistical Experiments Error Minimization for Fault-tolerant Multiprocessor System Reliability Estimation // Journal of Qafqaz university- Mathematics and computer science.- Volume 4, Number 2.- 2016.- pp.140-146
5. Rabah AlShboul, Vitaliy A. Romankevich. GL-model, presenting Emergence of Dangerous State in Multiprocessor Management System // The World of Computer Science and Information Technology. – 2017. – Vol. 7, № 2. – P. 7–9.
6. Дробязко І.П., Клятченко Я.М., Тарасенко-Клятченко О.В., Тарасенко В.П., Тесленко О.К. Методика аналізу та оцінки явища самокорекції у загальному випадку нерозподільних декомпозицій булевих функцій // Международная научная конференция имени Т.А.Таран "Интеллектуальный анализ информации" (ИАИ-2015) Сборник трудов. - К.: Просвіта, 2015. – С.62-68 <http://pma.fpm.kpi.ua/uk/node/822>

7. Дробязко І.П., Клятченко Я.М., Тарасенко-Клятченко О.В., Сапсай Т.Г. Тарасенко В.П., Тесленко О.К. Аналіз властивості автокорекції для комбінаційних суматорів. «Интеллектуальный анализ информации (ИАИ-2016)» им. Т.А.Таран. Сборник трудов. - К.: Просвіта, 2016. – С.56-60 <http://pma.fpm.kpi.ua/uk/node/822>

13. Ключові слова

Багатопроцесорні системи, самодіагностування, відмовостійкість, оцінювання безпеки, показники достовірності функціонування.