РОЗДІЛ 4 АВТОМАТИКА, КОМП'ЮТЕРНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.315

М. О. Дрозд[1], О. В. Дрозд[1], І. М. Ніколенко[2]
[1] Одеський національний політехнічний університет, пр. Шевченка, 1, м. Одеса, 65044
[2] Одеська національна академія харчових технологій, вул. Дворянська, 1/3, м. Одеса, 65082

МОДЕЛІ КОНТРОЛЕПРИДАТНОСТІ ЦИФРОВИХ КОМПОНЕНТІВ В СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Розглянуто проблему прихованих несправностей, за якою відмовостійке побудування цифрових компонентів не гарантує функціональної безпеки систем критичного застосування. Запропоновано структурну, функціональну та двохрежимну моделі контролепридатності для цифрових компонентів. За цими моделями визначаються різні шляхи для вирішення проблеми. Показана доцільність використання двохрежимної моделі, що відкриває шлях для методів вирівнювання контролепридатності нормального та аварійного режимів, а також виявлення та усунення потенційно небезпечних точок цифрових компонентів.
Ключові слова: *Комп'ютерні системи критичного застосування – Цифрові компоненти – Приховані несправності – Моделі контролепридатності – Потенційно небезпечні точки.*

М. А. Дрозд[1], А. В. Дрозд[1], И. Н. Николенко[2]
[1] Одесский национальный политехнический университет, пр. Шевченко, 1, г. Одесса, 65044
[2] Одесская национальная академия пищевых технологий, ул. Дворянская, 1/3, г. Одесса, 65082

МОДЕЛИ КОНТРОЛЕПРИГОДНОСТИ ЦИФРОВЫХ КОМПОНЕНТОВ В СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Рассмотрена проблема скрытых неисправностей, из-за которой отказоустойчивое построение цифровых компонентов не гарантирует функциональной безопасности систем критического применения. Предложены структурная, функциональная и двухрежимная модели контролепригодности для цифровых компонентов. По этим моделям определяются различные пути решения проблемы. Показана целесообразность использования двухрежимной модели, открывающая путь для методов выравнивания контролепригодности нормального и аварийного режимов, а также выявления и устранения потенциально опасных точек цифровых компонентов.
Ключевые слова: *Компьютерные системы критического применения – Цифровые компоненты – Скрытые неисправности – Модели контролепригодности – Потенциально опасные точки.*

I. ВСТУП

Переднім краєм розвитку комп'ютерних систем є їх застосування у критичних областях для управління об'єктами підвищеного ризику, що набувають поширення в енергетиці, на транспорті, в космічній та оборонній галузях [1]. Якісне зростання таких інформаційних управляючих систем (ІУС) критичного застосування полягає в диверсифікації робочого режиму, що поділяється на нормальний та аварійний. Причому ІУС проектуються заради виконання функцій в аварійному режимі, а основний час, як правило, працюють в нормальному режимі [2].

До ІУС критичного застосування пред'являються підвищені вимоги з функціональної безпеки як частини загальної безпеки об'єкта та системи керування, включаючи побудову відмовостійких цифрових компонентів (ЦК) [3].

Однак відмовостійкість не гарантує функціональної безпеки ЦК внаслідок проблеми прихованих несправностей, які можуть накопичуватись упродовж тривалого часу нормального режиму та проявлятися в аварійному, знижуючи рівень відмовостійкості та функціональної безпеки.

Традиційним вирішенням цієї проблеми є використання періодичного контролю з переходом у режим тестового діагностування, в якому виконується імітація аварійного стану ІУС. Однак практика застосування такого контролю не раз приводила до несанкціонованої імітації аварії внаслідок прояву несправностей [4].

Таким чином, проблема прихованих несправностей потребує пошуку кращих рішень порівняно до використання тестового режиму з імітацією аварійного стану ІУС. Для вирішення цієї проблеми доцільно розглянути контролепридатність

ЦК, з якою безпосередньо пов’язано накопичення прихованих несправностей цифрових схем.

II. КОНТРОЛЕПРИДАТНІСТЬ ЦК СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

У розвитку контролепридатності можна виділити три етапи, які можна характеризувати різними моделями її подання в ІУС: структурною, функціональною та двохрежимною моделлю.

Початковий етап розвитку контролепридатності пов'язаний з тестовим діагностуванням, де сформувалося її поняття як тестопридатності для оцінки складності синтезу тестів, спрямованих на виявлення несправностей у паузах робочого режиму. Тесторидатність оцінюється для точок цифрової схеми шляхом обчислення керованості, спостережуваності та їх добутку і підвищується тестопридатним проектуванням ЦК, використовуючи методи сканування та самотестування в режимі тестового діагностування [5, 6]. Для ІУС критичного застосування ці методи задіяні для тестування ЦК, включаючи імітацію аварійного стану.

Така контролепридатність представляється структурною моделлю, що повністю описується структурою цифрової схеми.

Наступний розвиток контролепридатність ЦК набуває в робочому діагностуванні. На другому етапі задача підвищення контролепридатності переноситься з режиму тестового діагностування в нормальний режим, де спрямована безпосередньо на виявлення прихованих несправностей ЦК. Контролепридатність описується функціональною моделлю, проявляючи себе залежною не тільки від структури цифрової схеми, а й від вхідних даних нормального режиму.

Існують об'єктивні та суб'єктивні причини виникнення прихованих несправностей ЦК, що використовуються в ІУС критичного застосування.

Об'єктивні причини визначаються особливостями систем критичного застосування, які створюють структурну надмірність цифрових схем, що властива відмовостійким рішенням та обмеженням на вхідні дані нормального режиму.

Суб'єктивні причини складаються з особливостей побудови ІУС, орієнтованих на досягнення високих, але не завжди обґрунтованих показників. До них належить висока стабільність амплітуди сигналів на виходах датчиків вимірюваних параметрів. Сигнали перетворюються у двійкові коди, які при низькому рівні шуму змінюються тільки в молодших розрядах. Крім того, установлюється необґрунтовано високий коефіцієнт “сигнал / шум”, використовуючи цифрові компоненти з багатьма тисячами станів для розрізнення тільки двох режимів – нормального та аварійного. Але найбільше вона обмежується обробкою даних у паралельних кодах на однотактних ЦК з матричним паралелізмом, що стало традиційним для ІУС у прагненні забезпечити високий рівень продуктивності. Усі ці надлишкові розв'язки додатково знижують контролепридатність цифрових схем.

Для функціональної контролепридатності розроблено методи її оцінки та підвищення, що досягається наближенням контролепридатності до її верхньої границі та підняттям самої границі [7, 8].

Однак зазначені об’єктивні причини не дозволяють підняти функціональну контролепридатність ЦК до повного вирішення проблеми прихованих несправностей ІУС в нормальному режимі.

Тому важливим є наступний етап розвитку контролепридатності ЦК, який також реалізується в робочому діагностуванні ІУС критичного застосування, однак враховує функціонування схеми не тільки на обмежених вхідних даних нормального режиму, а також у аварійному режимі. Така двохрежимна функціональна модель контролепридатності визначається структурою схеми та вхідними даними обох режимів.

Основою для двохрежимної функціональної моделі служить диверсифікація контролепридатності, що утворилася слідом за диверсифікацією робочого режиму ІУС критичного застосування: контролепридатність стала різною для нормального та аварійного режимів завдяки різним в них вхідним даним.

Двохрежимна модель контролепридатності дозволяє виявляти та усувати потенційно-небезпечні точки цифрової схеми, в яких в нормальному режимі можуть накопичуватися приховані несправності, що проявляються в аварійному режимі, знижуючи рівень відмовостійкості та безпеки ЦК. Відкриваються нові шляхи для вирішення проблеми прихованих несправностей, спрямовані на зберігання рівня відмовостійкості ЦК.

Пропонуються такі два шляхи:

– зробити контролепридатність однаковою для обох режимів ІУС, щоб приховані несправності нормального режиму залишалися прихованими і в аварійному режимі;

– виявляти потенційно-небезпечні точки та усувати ті з них, які являють реальну загрозу функціональній безпеці ІУС.

Аналіз двохрежимної моделі контролепридатності показує можливості реалізації першого шляху кодуванням вхідних даних, коли вони стають однаковими. До таких методів можна віднести порозрядну конвеєризацію обчислень та обробку даних у двохпровідних кодах, а також вирівнювання контролепридатності із заготівлею результатів.

Перехід до порозрядної обробки даних дозволяє реалізувати перший шлях, утворюючи вхідні дані з однакових слів, якими є значення нуля й одиниці. Операція в послідовному коді може бути виконана порозрядною конвеєризацією обчислень. Необхідна продуктивність досягається при використанні в ЦК множини конвеєрів.

Використання двохпровідної логіки є надзвичайно важливим для вирівнювання функціональної контролепридатності ЦК, що працюють тільки в аварійному режимі. До таких ЦК відноситься, наприклад, цифрова затримка, що погодить за часом етапи включення захистів аварійного режиму. У нормальному режимі цей ЦК не ви-

користовується. Двохпровідне кодування дозволяє вирівняти контролепридатність цифрової затримки в нормальному та аварійному режимі, кодуючи її включений та виключений стан.

Метод вирівнювання контролепридатності із заготівлею результатів дозволяє обчислювати множину можливих результатів за мінливими вхідними даними та вибирати з них два результати: для нормального та перевірки аварійного режиму.

Другий шлях ґрунтується на методі виявлення потенційно небезпечних точок схеми ЦК, які ідентифікуються для константних несправностей одного виду (нуля чи одиниці) або обох видів відповідно за формулами (1) та (2) [9]:

$$(C_N + C_E = 3) \wedge (O_E > 0); \quad (1)$$

$$(O_N = 0) \wedge (O_E > 0), \quad (2)$$

де C_N та C_E – керованість точки в нормальному та аварійному режимі; керованість дорівнює 1, 2 або 3, якщо точка приймає значення 1, 0 або обидва значення, відповідно; O_N та O_E – спостережуваність точки в нормальному та в аварійному режимі; спостережуваність дорівнює 0, 1, 2 або 3, якщо точка не передає зміну значення на вихід схеми, передає, приймаючи значення 1, 2 або обидва значення, відповідно.

Для усунення потенційно небезпечних точок в схемах арифметичних ЦК пропонується метод багатоверсійного виконання операції.

Наприклад, арифметичні операції можуть виконуватися в додавальному коді зі зміною знаків операндів і результату: додавання чисел з одночасною зміною знаків доданків і суми, множення або ділення з одночасною зміною знаків операндів або одного операнда та результату. Зміна знака в додавальному коді непарного двійкового числа інвертує всі його розряди крім молодшого, який, як правило, є керованим. Чергування версій виконання операції на слабко мінливих вхідних даних підвищує керованість схеми ЦК, порушуючи умову приналежності точок до множини потенційно небезпечних.

Метод показує високу ефективністю Для однотактного матричного помножувача мантис в додавальному коді використання двох версій операції (зі зміною та без змін знаків операндів) підіймає двохрежимну контролепридатність до 100% вже при трьох значеннях кожного з співмножників, тобто на дев'яти вхідних словах.

ІІІ. ВИСНОВОК

В умовах підвищених вимог до функціональної безпеки комп'ютерні системи одержують розвиток, перетворюючись у ІУС критичного застосування з диверсифікацією робочого режиму його розподілом на нормальний та аварійний. Це приводить до появи нових викликів, включаючи проблему прихованих несправностей, без вирішення якої відмовостійкість ЦК не гарантує функціональну безпеку ІУС.

Традиційне розв'язання цієї проблеми базується на підвищенні контролепридатності ЦК в режимі тестового діагностування імітуванням аварійного стану ІУС, що чревате несанкціонованим включенням імітації несправністю в нормальному режимі.

Перенесення задачі підвищення контролепридатності з тестового діагностування у робоче нормального режиму перетворює структурну модель контролепридатності до функціональної, що визначається не тільки структурою схеми ЦК, але й вхідними даними нормального режиму.

Це відкриває шлях для методів наближення контролепридатності до її верхньої границі та підняття цієї границі. Подальший розвиток моделей до двохрежимної контролепридатності визначає шляхи її вирівнювання в нормальному та аварійному режимах, а також виявлення та усунення потенційно небезпечних точок схем ЦК з розробкою методів кодування вхідних даних та реалізації версій виконання операції

ЛІТЕРАТУРА

1. Безопасность критических инфраструктур: математические инженерные методы анализа и обеспечения / Под ред. Харченко В. С. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», 2011. – 641 с.
2. **Yastrebenetsky M. A.** (edit.). Safety of Nuclear Power Plants Instrumentation and Control Systems / M. A. Yastrebenetsky. – Ukraine, Kyiv: Technika, 2004. – 472 p.
3. **Бахмач Е. С., Герасименко А. Д., Головир В. А.** и др. Отказобезопасные информационно-управляющие системы на программируемой логике / Под ред. Харченко В. С. и Скляра В. В. – Национальный аэрокосмический университет «ХАИ», Научно-производственное предприятие «Радий», 2008. – 380 с.
4. **Суліма Ю. Ю.** Аналіз ризиків при тестовому діагностуванні цифрових компонентів систем критичного застосування / Ю. Ю. Суліма, Ю. Б. Шугайло, О. В. Дрозд // Холодильна техніка і технологія. – 2011. – № 1. – С. 77 – 79.
5. **Щербаков Н. С.** Достоверность работы цифровых устройств / Н. С. Щербаков . – М.: Машиностроение, 1989. – 224 с.
6. **Беннетс, Р. Дж.** Проектирование тестопригодных логических схем / Р. Дж. Беннетс. – М.: Радио и связь, 1995. – 180 с.
7. **Drozd A.** Checkability of the digital components in safety-critical systems: problems and solutions / A. Drozd, V. Kharchenko, S. Antoshchuk, J. Sulima, M. Drozd // Proc. IEEE East-West Design & Test Symposium. – Sevastopol, Ukraine, 9 – 12 Sept. – P. 411 – 416, 2011.
8. **Суліма Ю. Ю.** Оцінка та метод підвищення контролепридатності цифрових компонентів в системах критичного застосування / Ю. Ю. Сулі-

ма, О. В. Дрозд // Холодильна техніка і технологія. – 2013. – № 1. – С. 90 – 92.
9. Рабочее диагностирование безопасных информационно-управляющих систем / Под ред. Дрозда А. В., Харченко В. С. – Харьков: Национальный аэрокосмический ун-т им. Н.Е. Жуковского «ХАИ», 2012. – 614 с.

M. O. Drozd, O. V. Drozd, I. M. Nikolenko
Odessa National Polytechnical University, av. Shevchenko, 1, Odessa, 65044

THE MODELS OF DIGITAL COMPONENTS CHECKABILITY IN SAFETY-RELATED SYSTEMS

The problem of the hidden faults for which fault tolerant structure of the digital components does not guarantee function safety of the safety-critical systems is considered. The structural, functional and dual-modes models of checkability for the digital components are offered. The different ways for solving the problem by these models are determined. The expedience in use of the dual-modes model which opens the way for the methods of leveling of the checkability in normal and emergency modes and also detection and elimination of the potentially hazardous points in the digital components is shown.
Keywords: *Safety-critical computer systems – Digital components – Hidden faults – Models of checkability – Potentially hazardous points.*

REFERENCES

1. Safety of Critical Infrastructures: Mathematical and Engineering Methods of Analysis and Ensuring / Pod red. Kharchenko V. S. – Ministerstvo obrasovanija i nauki Ukraini, Nationalniy aerokosmixheskiy universitet im. N. E. Zhukovskogo «KhAI», 2011. – 641 p.
2. **Yastrebenetsky M. A.** (edit.). Safety of Nuclear Power Plants Instrumentation and Control Systems / M. A. Yastrebenetsky. – Ukraine, Kyiv: Technika, 2004. – 472 p.
3. **Bachmach E. S., Herasimenko A. D., Golovir V. A.** i dr. Otkazobezopasnie informacionno-upravlajushchie sistemi na programmiruemoy logike / Pod red. Kharchenko V. S. i Sklara V. V. – Nationalniy aerokosmixheskiy universitet «KhAI», Nauchno-proizvodstvennoe predprijatie «Radiy», 2008. – 380 p.
4. **Sulima J. J.** Analiz rizikiv pri testovomu diagnostuvanni cifrovich komponentiv system kritichnogo zastosuvannja / J. J. Sulima, J. B. Shugaylo, O. V. Drozd // Holodilna tehnika i tehnologija. – 2011. – № 1. – P. 77 – 79.
5. **Shcherbakov N. S.** Dostovernost raboti cifrovih ustroystv / N. S. Shcherbakov. – M.: Mashinostroenie, 1989. – 224 p.
6. **Bennets, R. G.** Proektirovanie testoprigodnih logicheskih shem / R. G. Bennets. – M.: Radio i svjaz, 1995. – 180 p.
7. **Drozd A.** Checkability of the digital components in safety-critical systems: problems and solutions / A. Drozd, V. Kharchenko, S. Antoshchuk, J. Sulima, M. Drozd // Proc. IEEE East-West Design & Test Symposium. – Sevastopol, Ukraine, 9 – 12 Sept. – P. 411 – 416, 2011.
8. **Sulima J. J.** Ozinka ta metod pidvishchennja kontrolepridatnosti cifrovih komponentov v sistemah kritichnogo zastosuvannja / J. J. Sulima, O. V. Drozd // Holodilna tehnika i tehnologija. – 2011. – № 1. – P. 90-92.
9. Rabochee diagnostirovanie bezopasnih informacionno-upravljaushchih system / Pod red. Drozda A. V. i Kharchenko V. S. – Kharkov: Nationalniy aerokosmixheskiy universitet im. N. E. Zhukovskogo «KhAI», 2012. – 614 p.

Отримана в редакції 18.03.2014, прийнята до друку 29.04.2014