УДК 004.315

Ю. Ю. Суліма, О. В. Дрозд
Одеський національний політехнічний університет, пр. Шевченко, 1, Одеса, 65044

ОЦІНКА ТА МЕТОД ПІДВИЩЕННЯ КОНТРОЛЕПРИДАТНОСТІ ЦИФРОВИХ КОМПОНЕНТІВ В СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Розглянуто проблему низької контролепридатності цифрових компонентів інформаційно-управляючих систем критичного застосування, що спрямовані на підтримку функціональної безпеки об'єктів підвищеного ризику. Запропоновано оцінку контролепридатності цифрових компонентів у штатному режимі та метод її підвищення шляхом перетворення неконтролепридатних точок схеми у контролепридатні та частково контролепридатні точки. Метод демонструє найбільше підвищення контролепридатності для наймеш контролепридатних цифрових компонентів, гарантуючи рівень, що перевищує 50%.
Ключові слова: *Інформаційно-управляючі системи критичного застосування – Цифрові компоненти – Штатний режим – Контролепридатність – Контролепридатні та частково контролепридатні точки.*

The problem of the low control suitability for the digital components of the safety-critical Instrumentation and control systems aimed at the support in the functional safety of the objects with increased risk is considered. The estimation in control suitability of the digital components in a normal mode and a method of its increase by the way of transformation of non-checkable points of a circuit in checkable and partial checkable ones is offered. The method shows maximum increase of checkability for least checkable digital components guaranteeing the level which exceeds 50%.
Keywords: *Safety-critical Instrumentation and Control systems – Digital components – Normal mode – Control suitability – Suitable and partial suitable points.*

I. ВСТУП

Поширення об'єктів підвищеного ризику в енергетиці, включаючи атомні, теплові та гідроелектростанції, на транспорті, враховуючи підвищення швидкості наземного транспорту та традиційні загрози, пов'язані з повітряним транспортом, в оборонній та космічній галузях стає можливим завдяки успіхам в розвитку комп'ютерних та інформаційних технологій, що спрямовані на забезпечення необхідного рівня безпеки [1].

Значна роль в цьому відводиться інформаційно-управляючим системам (ІУС) критичного застосування, безпосередньо задіяним для контролю та керування об'єктами підвищеного ризику. До ІУС критичного застосування та компонентів, що їх складають, в свою чергу, пред'являються високі вимоги щодо функціональної безпеки [2].

Для цифрових компонентів ІУС функціональна безпека традиційно забезпечується їх побудовою за відмовостійкими структурними рішеннями. До них належать розробки цифрових компонентів за мажоритарним принципом, використання корегуючих кодів, застосування різних видів резервування та реконфігурації, а також багатоверсійних технологій [3].

Для комерційних ІУС, що не мають статуту критичного застосування, побудування відмовостійких цифрових компонентів, як правило, є достатньою умовою для забезпечення функціональної безпеки.

Критичне застосування накладає на ІУС додатковий відбиток, що проявляється в їх особливостях. Першою з них є проектування таких ІУС для роботи у двох режимах: штатному або нормальному та критичному, що найчастіше розуміється як аварійний. Причому основний час ІУС критичного застосування перебуває у штатному режимі, а створюється заради використання в аварійному режимі [4].

Наявність двох режимів обумовлює роботу цифрових компонентів в кожному з них на різній та обмеженій множині вхідних слів. Обмеженість множини вхідних слів у штатному режимі створює проблему низької контролепридатності цифрових компонентів ІУС, за якою в них виникають умови для накопичення скритих несправностей, що можуть порушити функціональну безпеку в аварійному режимі. Причому відмовостійкість ІУС ніяк не завадить процесу накопичення скритих несправностей, чому сприяє значна тривалість штатного режиму. Навпаки, як відомо, структурна надмірність відмовостійких цифрових компонентів сприяє зниженню їх контролепридатності [5].

Тому оцінка та підвищення контролепридатності цифрових компонентів ІУС критичного застосування є важливою актуальною задачею й потребує свого розв'язання.

II. КОНТРОЛЕПРИДАТНІСТЬ ЦИФРОВИХ КОМПОНЕНТІВ ТА МЕТОД ЇЇ ПІДВИЩЕННЯ В ІУС КРИТИЧНОГО ЗАСТОСУВАННЯ

Під контролепридатністю розуміють властивість пристрою, що обумовлює пристосованість до проведення контролю його технічного стану в процесі виготовлення й експлуатації. Контролепридатність цифрових пристроїв, як правило, розглядається та аналізується в тестовому діагностуванні, де вона оцінюється за керованістю та спостерігаємістю [6].

Оскільки в ІУС критичного застосування протистояння відмовам має оперативний характер, то основна роль у забезпеченні відмовостійкості належить методам та засобам робочого діагностування [7]. При тому слід зауважити, що робоче діагностування цифрових компонентів обмежено їхньою контролепридатністю не в меншій мірі ніж тестове діагностування.

Контролепридатність цифрових компонентів у тестовому та робочому діагностуванні спрямована на різні цілі. В тестовому діагностуванні контролепридатність оцінюється для визначення можливості синтезу тесту, обчислюючи в кожній точці схеми добуток її керованості на спостерігаємість. В робочому діагностуванні контролепридатність важлива з позиції врахування потенціальної загрози з боку скритих несправностей.

Тому контролепридатність повинна оцінюватися у робочому діагностуванні з інших позицій ніж у тестовому. На відміну від тестового діагностування, де вхідна послідовність слів визначається розробником тесту, можливості робочого діагностування суттєво залежать від робочої послідовності вхідних слів, яка суттєво впливає також на контролепридатність точок схеми цифрового компонента. Оскільки керованість точок схеми забезпечується на робочій послідовності вхідних слів, то контролепридатність цих точок повністю визначається їх спостерігаємістю.

Для найбільш поширених однотактних цифрових компонентів робочі послідовності достатньо розглядати множиною вхідних слів.

При оцінці контролепридатності доцільно враховувати також часткову можливість накопичення скритих несправностей.

Визначення 1. Точка схеми є частково спостерігаємою: 0-спостерігаємою або 1-спостерігаємою, якщо на множині вхідних слів активується шлях від цієї точки тільки при її значенні «0» або «1», відповідно. Якщо шлях активується при всіх її значеннях, то точка є спостерігаємою, а в противному випадку – неспостерігаємою. Шлях активується при передачі зміни значення точки в контрольну точку схеми, що підключається до схеми контролю цифрового компонента.

Визначення 2. Точка схеми називаєтья контролепридатною або частково контролепридатною, якщо є відповідно спостерігаємою або частково спостерігаємою, та неконтролепридатною в противному випадку.

Контролепридатність цифрового компонента може бути оцінена за наступною формулою:

$$C = (N_C + 0{,}5\,N_P) / N_T, \qquad (1)$$

де N_C, N_P, N_T – кількість контролепридатних, частково контролепридатних та всіх точок схеми, відповідно.

Введені визначення дозволяють виявити неконтролепридатні точки схеми однотактного цифрового компонента на його моделі, яка розглядається на множині вхідних робочих слів, що є обмеженою умовами роботи ІУС критичного застосування в штатному режимі.

В основу методу підвищення контролепридатності цифрового компонента може бути покладене перетворення неконтролепридатних точок у контролепридатні або частково контролепридатні точки схеми шляхом підвищення їх спостерігаємості до рівня спостерігаємих або частково спостерігаємих точок.

Таке перетворення може бути здійснено включенням неконтролепридатних точок до множини контрольних точок схеми цифрового компонента. Таке рішення має той недолік, що при значній кількості неконтролепридатних точок веде до відповідно значного ускладнення засобів робочого діагностування внаслідок суттєвого збільшення множини контрольних точок схеми.

Більш просте рішення реалізується при організації додаткових шляхів, що активуються та підключають неконтролепридатні точки до обмеженої кількості додаткових контрольних точок. Кожний такий шлях складається з ланцюга послідовно з'єднаних додавачів за модулем два. Один з входів першого додавача підключається до контролепридатної точки (або неконтролепридатної, що переключається), яка виступає за базову точку шляху, та один з входів наступних додавачів використовується для зв'язку з попереднім додавачем. Інші входи підключаються до неконтролепридатних точок.

Завдяки властивостям додавача за модулем два, що є умовним інвертором, шлях є активованим для кожної підключеної до нього точки.

Введення декількох шляхів може бути доцільним з позиції спрощення контролю додаткових контрольних точок. Таке спрощення досягається при об'єднанні за одним шляхом тільки неконтролепридатних точок, що не переключаються та є незалежними, тобто попарно розташованими не на одній гілці схеми. Тоді додаткова контрольна точка перевіряється на кожне переключення базової контролепридатної точки.

Якщо одна з цих точок переключилася, а інша ні, то це вказує на виявлення несправності, бо сталося додаткове переключення одної з незалежних точок, що не переключаються у справному стані.

За таким методом неконтролепридатні точки, що переключаються та не переключаються у штатному режимі, стають відповідно контролепридатними та частково контролепридатними.

Врахування тільки точок, що перетворилися з неконтролепридатних у частково контролепридатні підвищує контролепридатність цифрового компонента до рівня, що оцінюється наступною формулою:

$$C^* = 0{,}5 + 0{,}5P_C, \qquad (2)$$

де $P_C = N_C / N_T$.

Аналіз формули (2) показує, що запропонований метод гарантовано підіймає контролепридатність цифрового компонента вище за 50%.

При наявності N_Z точок, що були неконтролепридатними та є такими, що переключаються у штатному режимі, контролепрдатність C^* ще збільшується на величину N_Z / N_T.

При моделюванні матричного помножувача подібно до умов, що викладені у [8], його контролепридатність C склала 85% та 36,6% при зміні співмножників в штатному режимі у діапазоні 80 та 10 значень відповідно. Контролепридатні, частково контролепридатні та неконтролепридатні точки склали для цих випадків відповідно 78,5%, 13%, 8,5% та 30,2%, 12,8%, 57%.

В результаті застосування запропонованого метода контролепридатність матричного помножувача піднялася для розглянутих випадків відповідно до $C^* = 89{,}3\%$ та $C^* = 65{,}1\%$, тобто на 5% та 78%.

ІІІ. ВИСНОВОК

Розвиток ІУС критичного застосування є важливою умовою забезпечення функціональної безпеки об'єктів підвищеного ризику.

До важливих складових функціональної безпеки самих ІУС критичного застосування та їх компонентів слід відносити не тільки їхню відмовостійкість, але й контролепридатність, яку вони демонструють у штатному режимі на обмежених множинах вхідних слів.

Проблема низької контролепридатності цифрових компонентів не тільки не вирішується завдяки їх відмовостійкості, а ще й посилюється внаслідок значної структурної надмірності таких рішень.

Оцінка контролепридатності цифрових компонентів ІУС критичного застосування показує на її залежність від частково контролепридатних точок схеми.

Запропонований метод суттєво підвищує контролепридатність цифрових компонентів, перетворюючи неконтролепридатні точки, що переключаються та не переключаються у штатному режимі, відповідно у контролепридатні та частково контролепридатні точки схеми. Тільки за рахунок перетворення точок у частково контролепридатні точки схеми контролепридатність гарантовано перевищує 50%, що особливо важливо для цифрових компонентів з низькою контролепридатністю. Розглянутий приклад показує, що метод демонструє найбільшу ефективність саме для таких компонентів.

ЛІТЕРАТУРА

1. Безопасность критических инфраструктур: математические инженерные методы анализа и обеспечения / Под ред. Харченко В.С. – Министерство образования и науки Украины, Национальный аэрокосмический ун-т им. Н.Е.Жуковского «ХАИ», 2011. – 641 с.

2. 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 ун-т «ХАИ», Научно-производственное предприятие «Радий», 2008. – 380 с.

3. Kharchenko V., Multi-version Systems: Models, Reliability, Design Technologies // 10th European Conference on Safety and Reliability. – Munich, Germany. – 1999. – Vol. 1. – P. 73-77.

4. Drozd A., Kharchenko V., Antoshchuk S., Drozd M. On-line testing of safety-critical I&C systems in normal and emergency modes: Problems and solutions // First International Workshop "Critical Infrastructure Safety and Security". – Kirovograd, Ukraine. – 2011. – P. 139-147.

5. Щербаков Н.С. Достоверность работы цифровых устройств. – М.: Машиностроение, 1989. – 224 с.

6. Беннетс, Р.Дж. Проектирование тестопригодных логических схем / Р.Дж. Беннетс. – М.: Радио и связь, 1995. – 180 с.

7. 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.

8. Дрозд А.В., Харченко В.С., Антощук С.Г., Дрозд М.А., Сулима Ю.Ю. Оценка контролепригодности цифровых компонентов встроенных систем критического применения // Радіоелектронні і комп'ютерні системи. – 2012. – № 6 (58). – С. 184-190.

Получена в редакции 21.01.2013, принята к печати 23.01.2013