УДК 004.315

М.О. Дрозд
Одеський національний політехнічний університет, пр. Шевченка, 1, м. Одеса, 65044

ПРОБЛЕМА КОНТРОЛЕПРИДАТНОСТІ ЦИФРОВИХ КОМПОНЕНТІВ В СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Розглянуто проблему контролепридатності цифрових компонентів систем критичного застосування, що створює загрозу функціональній безпеці об'єктів підвищеного ризику. Проаналізовано особливості оцінки контролепридатності у тестовому імітаційному та робочому діагностуванні цифрових компонентів систем критичного застосування як дворежимних комп'ютерних систем. Показана доцільність ідентифікації потенційно небезпечних точок цифрових компонентів. Визначено умови виявлення потенційно небезпечних точок цифрових компонентів у складі систем критичного застосування.
Ключові слова: *Комп'ютерні системи критичного застосування – Цифрові компоненти – Нормальний та аварійний режим – Контролепридатність – Потенційно небезпечні точки.*

The problem in checkability of the digital components in safety-critical systems is considered in content of threat created in the functional safety of the objects with increased risks. The particularities of estimation in checkability for both imitated and on-line testing of the digital components in safety-critical systems like two-modes computer systems is analyzed. The expedience in identification of the potentially dangerous points for the digital components is shown. Conditions in detection of the potentially dangerous points for the digital components in structure of safety-critical systems are determined.
Keywords: *Safety-critical computer systems – Digital components – Normal and emergency modes – Checkability – Potentially dangerous points.*

I. ВСТУП

Одною з найвідповідальніших ланок використання інформаційних та комп'ютерних технологій є область їх критичного застосування для обслуговування об'єктів підвищеного ризику, кількість та складність яких постійно зростає. До таких об'єктів належить транспорт, що характеризується високою швидкістю та подальшим її зростанням, атомні, теплові та гідроелектростанції, які мають значну потужність та продовжують її нарощувати, медичні апарати, використання яких пов'язано з підтримкою життєвих функцій, та ін.

Основне питання, що ставиться до таких об'єктів та перекладається на обслуговуючі їх інформаційні комп'ютерні системи критичного застосування, полягає в підтримці їхньої функціональної безпеки [1].

Інформаційні комп'ютерні системи критичного застосування будуються, використовуючи до них компонентний підхід (OTS – Off-The-Shelf), що полягає в їх комплектації, перш за все, з компонентів, випробуваних в комерційних (COTS – Commercial-Off-The-Shelf) та критичних (CrOTS – Critical-Off-The-Shelf) областях призначення, а також доповнених при необхідності компонентами власної розробки [2].

Інформаційні комп'ютерні системи критичного застосування суттєво відрізняються від комерційних систем їх спрямованістю на критичні умови функціонування. Разом з тим, такі умови є, як правило, виключними. Тому системи критичного застосування проектуються для роботи у двох режимах: нормальному та аварійному, а їх функціонування протягом основного часу проходить у нормальному режимі [3].

За таких обставин складаються несприятливі умови для підтримки функціональної безпеки системи критичного застосування та її цифрових компонентів. До таких умов слід віднести обмежену множину вхідних слів, що надходять на входи цифрових компонентів у нормальному режимі. Це призводить до створення штучної надмірності схем цифрових компонентів, за якою, як звісно, знижується їхня контролепридатність [4].

Проблема низької контролепридатності схем цифрових компонентів полягає у загрозі накопичення скритих відмов в нормальному режимі роботи систем критичного застосування.

Цифрові компоненти систем критичного застосування проектуються відмовостійкими. Однак такі рішення суттєво ускладнюють апаратну реалізацію, що обмежує кількість врахованих відмов, і, як правило, приймається одна відмова [5].

Разом з тим, нормальний режим має завелику тривалість, протягом якої може накопичуватись значно більше за одну відмову, що порушує умови функціональної безпеки цифрових компонентів та комп'ютерних систем критичного застосування з виникненням аварійного режиму.

Таким чином, гостро стає проблема контролепридатності цифрових компонентів систем критичного застосування, що потребує, перш за все, її вивчення.

ІІ. АНАЛІЗ КОНТРОЛЕПРИДАТНОСТІ ЦИФРОВИХ КОМПОНЕНТІВ СИСТЕМ КРИТИЧНОГО ЗАСТОСУВАННЯ

Контролепридатність цифрових схем традиційно розглядалася як їх характеристика стосовно можливості успішного здійснення тестового діагностування й оцінювалася визначенням для точок схеми їхньої керованості від її входів та спостережуваності на виходах [6].

Тестове діагностування відбувається на контрольних прикладах, тобто тестах, що дозволяє імітувати роботу цифрових компонентів у аварійному режимі, виявляючи загрозливі для нього відмови, що накопичуються у нормальному режимі. Однак використання імітаційних тестових режимів створює додаткові суттєві ризики, що можуть виключати цифровий компонент з одного з режимів або провокувати аварійний режим [7].

До того ж оперативне протистояння відмовам вимагає використання в системах критичного застосування методів та засобів робочого діагностування цифрових компонентів [8].

Як показано в [9], зі зміною тестового діагностування на робоче контролепридатність також трансформується, переорієнтовуючи спрямованість з аналізу придатності цифрової схеми до розробки до неї тестів на виявлення точок схеми, де можуть накопичуватися скриті несправності. Як наслідок, контролепридатність цифрових компонентів у робочому діагностуванні повністю визначається їх спостережуваністю, а верхня межа контролепридатності – керованістю.

Необхідно зауважити, що керованість цифрового компонента в нормальному режимі системи критичного застосування не перевищує його керованості при тестовому діагностуванні, що витікає з обмеженості множини вхідних слів, що використовуються у нормальному режимі.

Разом з тим, в тестовому діагностуванні цифрових схем контролепридатність визначається добутком керованості та спостережуваності, які нормовані до одиниці, а отже верхньою межею контролепридатності є кожен із співмножників, тобто мінімальне із значень керованості та спостережуваності.

Слід зауважити, що в імітаційному тестовому та робочому діагностуванні оцінюється різна контролепридатність цифрових компонентів систем критичного застосування. Імітація аварійного режиму дозволяє тестувати контролепридатність у тій частині, порушення якої безпосередньо загрожує функціональній безпеці системи критичного застосування. З оцінки контролепридатності цифрових компонентів виключається аналіз скритих несправностей, що не мають наслідків у аварійному режимі. В робочому діагностуванні нормального режиму такі несправності враховуються, що можна віднести до недоліків в оцінці контролепридатності цифрових компонентів систем критичного застосування.

Для наближення до оцінки контролепридатності, що визначається в імітаційному стані тестового діагностування, необхідно враховувати не тільки особливості робочого діагностування відносно тестового, але й особливості систем критичного застосування як дворежимних комп'ютерних систем, тобто враховувати в оцінці контролепридатності обидва режими – і нормальний, і аварійний. Контролепридатність повинна визначатися як функція керованості та спостережуваності, що оцінюються для кожного з двох режимів.

В керованості точки схеми цифрового компонента доцільно розрізняти три стани. Два з них характеризують точку як частково-керовану: 1-керовану або 0-керовану, якщо на множині вхідних слів в цій точці приймається тільки значення «1» або «0», відповідно. Якщо приймаються обидва значення, то визначається третій стан точки, яка у такому разі є керованою. Номери 1, 2 і 3 трьох описаних станів точки складають три значення її керованості.

При визначенні спостережуваності для точки схеми цифрового компонента доцільно розрізняти чотири стани. Точка схеми цифрового компонента може бути частково-спостережуваною: 1-спостережуваною або 0-спостережуваною, якщо на множині вхідних слів активується шлях від цієї точки тільки при її значенні «0» або «1», відповідно. Якщо приймаються обидва значення, то точка знаходиться у наступному за номером стані та є спостережуваною, а якщо ні, то характеризується попереднім станом та є неспостережуваною.

Шлях активується при передачі зміни значення точки в контрольну точку схеми. Такими точками є розряди результату, що обчислюється та підключаються до схем контролю при робочому діагностуванні цифрового компонента.

Таким чином, спостережуваність точки цифрового компонента може приймати чотири значення, у якості яких використовуються номери 0, 1, 2 і 3 відповідно для неспостережуваної, 1-спостережуваної, 0-спостережуваної й спостережуваної точки.

Слід відмітити, що в імітаційному тестовому діагностуванні точки цифрового компонента оцінюються не зовсім з позиції контролепридатності, бо перевірки відбуваються на обмежених вхідних послідовностях або множинах вхідних слів, які характерні безпосередньо аварійного режиму.

У робочому діагностуванні більш коректно характеризувати точки з позиції потенційної небезпеки, яка загрожує системі критичного застосування в цій точці у випадку прояву в ній накопиченої відмови у аварійному режимі.

Для виявлення потенційно небезпечних точок, необхідно визначити дві умови: існує ризик накопичення прихованої несправності в нормальному режимі й припустимий її прояв в аварійному режимі.

Перша умова виконується в нормальному режимі у двох випадках: якщо точка є частково керованою, і значення в точці збігається зі значенням, що задається константною несправністю, а також, якщо точка є неспостережуваною.

Друга умова виконується в аварійному режимі також у двох випадках: якщо точка є спостережуваною й некерованою і її значення, як некерованої точки, відмінно від значення, що задається константною несправністю, а, крім того, якщо точка є й керованою, й спостережуваною.

Описані умови дозволяють ідентифікувати потенційно небезпечні точки цифрового компонента, аналізуючи на істинність наступну формулу:

$$((C_N + C_E = 3) \text{ or } (O_N + C_E = 3) \text{ or } (O_N = 0)) \text{ and } (O_E > 0), \quad (1)$$

де C_N і O_N – керованість і спостережуваність точки в нормальному режимі;

C_E і O_E – керованість і спостережуваність точки в аварійному режимі.

Обчислення для кожної точки цифрового компонента її керованості і спостережуваності в нормальному та аварійному режимі та перевірка за ними умови (1) дозволяє виявити всі потенційно небезпечні точки кожного цифрового компонента системи критичного застосування.

ІІІ. ВИСНОВОК

Функціональна безпека комп'ютерних систем критичного застосування, що є запорукою функціональної безпеки об'єктів підвищеного ризику, не може бути досягнена тільки за рахунок її побудови за відмовостійкими технологіями. Особливості цих систем як дворежимних створюють проблему обмеженої контролепридатності їх цифрових компонентів, яка полягає в загрозі накопичення кількості відмов, що перевищує можливості відмовостійких рішень їм протистояти.

Традиційне тлумачення контролепридатності з позиції тестування цифрових схем не враховує особливостей дворежимних комп'ютерних систем.

Імітаційне тестове діагностування дає об'єктивну оцінку цифрових компонентів з боку протистояння відмовам у аварійному режимі, однак його використання пов'язане з високим ризиком викликання такого режиму.

Для одержання об'єктивної оцінки у робочому діагностуванні цифрових компонентів, методи та засоби якого безпосередньо задіяні у відмовостійких рішеннях, доцільно ідентифікувати потенційно небезпечні точки схем. Виявлення таких точок забезпечується за умови, що визначають можливості накопичення скритих несправностей у нормальному режимі та їх прояву у аварійному режимі.

ЛІТЕРАТУРА

1. **Yastrebenetsky M.A.** (edit.). NPP I&Cs: Problems of Safety / M.A. Yastrebenetsky. – Ukraine, Kyiv: Technika, 2004.
2. **Scott J.A.** Using Commercial-Off-The-Shelf (COTS) Software in High-Consequence Safety Systems / J.A. Scott, G.G. Preckshot, J.M. Gallagher // Lawrence Livermore National Laboratory, UCRL – 122246. – 1995.
3. 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.
4. **Щербаков Н.С.** Достоверность работы цифровых устройств. – М.: Машиностроение, 1989. – 224 с.
5. **Siora A.A.** Fault Tolerant Systems with Version-Information Redundancy / A.A. Siora, V.A. Krasnobayev, V.S. Kharchenko // National Aerospace University "KhAI, 2009. – 321 p.
6. **Беннетс, Р.Дж.** Проектирование тестопригодных логических схем / Р.Дж. Беннетс. – М.: Радио и связь, 1995. – 180 с.
7. **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.
8. 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.
9. **Сулима Ю.Ю.** Контролепригодность цифровых компонентов систем критического применения / Ю.Ю. Сулима, А.В. Дрозд // Тр. Одес. политехн. ун-та. – Одесса, 2012. – Вып. 2 (39). – С. 156 – 159.

Получена в редакции 20.03.2013, принята к печати 22.03.2013