УДК 004.315

В. В. Антонюк[1], О. В. Дрозд[1], М. 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

ОЦІНКА СПОСТЕРЕЖУВАНОСТІ ДЛЯ ТОЧОК КОНВЕЄРНОЇ СХЕМИ ЦИФРОВИХ КОМПОНЕНТІВ В СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Розглянуто проблему прихованих несправностей, без вирішення якої відмовостійке побудування цифрових компонентів не гарантує функціональної безпеки систем критичного застосування. Проблема проявляється в потенційно небезпечних точках схеми, які в нормальному режимі можуть накопичувати приховані несправності, що знижують відмовостійкість цифрового компонента при переході до аварійного режиму роботи системи. Запропоновано модель активованого шляху конвеєрної схеми цифрового компонента, що дозволяє визначити вхідні дані для обчислення спостережуваності точок у режимах системи. Розроблено метод ідентифікування потенційно небезпечних точок конвеєрної схеми цифрового компонента.
Ключові слова: *Система критичного застосування - Цифровий компонент - Конвеєрна схема - Прихована несправність - Потенційно небезпечна точка - Модель активованого шляху.*

В. В. Антонюк[1], А. В. Дрозд[1], М. А. 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

ОЦЕНКА НАБЛЮДАЕМОСТИ ДЛЯ ТОЧЕК КОНВЕЙЕРНОЙ СХЕМЫ ЦИФРОВЫХ КОМПОНЕНТОВ В СИСТЕМАХ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Рассмотрена проблема скрытых неисправностей, без решения которой отказоустойчивое построение цифровых компонентов не гарантирует функциональной безопасности систем критического применения. Проблема проявляется в потенциально опасных точках схемы, которые в нормальном режиме могут накапливать скрытые неисправности, снижающие отказоустойчивость цифрового компонента при переходе к аварийному режиму работы системы. Предложена модель активируемого пути конвейерной схемы цифрового компонента, что позволяет определить входные данные для вычисления наблюдаемости точек в режимах системы. Разработан метод идентификации потенциально опасных точек конвейерной схемы цифрового компонента.
Ключевые слова: *Система критического применения - Цифровой компонент - Конвейерная схема - Скрытая неисправность - Потенциально опасная точка - Модель активируемого пути.*

I. ВСТУП

Інформаційні управляючі системи критичного застосування (ІУС) обслуговують об'єкти підвищеного ризику, до яких належать енергомережі, енергоблоки електростанцій, швидкісний на- земний транспорт та літальні апарати. Об'єкти підвищеного ризику постійно поширюються й удосконалюються, підвищуючи складність та потужність, що посилює рівень небезпеки та вимоги до ІУС критичного застосування [1].

Вимоги до таких систем регламентуються міжнародними стандартами, що звертають основну увагу на забезпечення функціональної безпеки як частини загальної безпеки об'єкта та системи керування. В основу функціональної безпеки покладена побудова ІУС критичного застосування з відмовостійкою структурою, що складається з відмовостійких компонентів, проектування яких досить пророблено [2].

До особливостей ІУС критичного застосування слід віднести диверсифікацію робочого режиму з його розподілом на нормальний та аварійний. Причому, найменш дослідженим є аварійний режим, заради якого ІУС критичного застосування проектується, бо основний час її функціонування протікає у нормальному режимі. Відмічена особливість ускладнює задачу забезпечення відмовостійкості ІУС, що стає неможливим без вирішення проблеми прихованих несправностей, які можуть накопичуватись упродовж тривалого часу нормального режиму та проявлятися в аварійному, знижуючи рівень відмовостійкості та функціональної безпеки [3].

Ця проблема більш відома історією боротьби з прихованими несправностями, що неодноразово приводило до аварійних ситуацій. Заради виявлення прихованих несправностей на ІУС критичного застосування проводиться періодичний контроль з використанням у тестовому режимі імітації аварійного режиму з відключенням аварійного захисту. Це неодноразово приводило до несанкціонованого включення імітації аварійного режиму людиною або несправністю. Небезпеку також

складало відключення аварійного захисту. В робочому діагностуванні періодичний контроль використовується у форма ручного регулювання високостабільних вхідних параметрів уздовж всього діапазону нормального режиму, що, з одного боку, не гарантує виявлення прихованих несправностей, а з іншого боку, складає додаткову небезпеку при наближенні значень вхідних параметрів до умов функціонування ІУС в аварійному режимі [4].

Таким чином, проблема прихованих несправностей потребує більш небезпечного розв'язання. В [5] була запропонована модель дворежимної структурно-функціональної контролепридатності, за якою проблема постає у виникненні в нормальному режимі прихованих несправностей, що знижують відмовостійкість компонента в аварійному режимі. Визначено умови виявлення потенційно небезпечних точок однотактної цифрової схеми, в яких виникають такі приховані несправності [6]. Ці умови ґрунтуються на знанні спостережуваності точок схеми у нормальному та аварійному режимах, що можуть обчислюватися при моделюванні цифрового компонента [7].

Цифрові компоненти ІУС критичного застосування, як правило, будуються конвеєрними з однотактними матричними вузлами за ділянки конвеєра. Тому постає задача визначення спостережуваності точок конвеєрної схеми цифрового компонента.

II. ВИЗНАЧЕННЯ СПОСТЕРЕЖУВАНОСТІ ТОЧОК КОНВЕЄРНИХ СХЕМ ЦИФРОВИХ КОМПОНЕНТІВ

Для визначення спостережуваності пропонується наступна модель активованого шляху конвеєрної схеми цифрового компонента:

$$AP(U_1, ..., U_I, ..., U_K),$$

де $U_1, ..., U_K$ - описи вузлів обробки даних на ділянках конвеєра, що становлять шлях AP;

K - кількість вузлів U_I, $I = \overline{1,K}$.

Кожний вузол U_I представляється моделлю

$$U_I(F_I, Z_{I1}, ..., Z_{IJ}, ..., Z_{IMi}),$$

де F_I - операція, виконувана вузлом U_I;

$Z_{I1}, ..., Z_{IMi}$ - описи входів вузла U_I;

Mi - кількість входів вузла U_I;

Кожний вхід Z_{IJ} характеризується дистанцією D_{IJ} між власним і поточним словом, а також значеннями, які обчислюються на вхідних словах конвеєрної схеми цифрового компонента.

Дистанція виміряється в тактах по формулі

$$D_{IJ} = |Y_I - Y_{IJ}| \qquad (1)$$

де Y_I *і* Y_{IJ} номер поточного слова, яке надходить на вузол U_I по входу Z_I, що належить шляху AP, і номер власного слова на вході Z_{IJ};

вхід Z_I - один з входів Z_{IJ}, для якого $D_{IJ} = 0$.

У випадку $\forall(I,J)$, $D_{IJ} = 0$ вузол U_I моделюється на входах Z_{IJ}, кожний з яких приймає значення, що обчислюється для поточного слова. Модель активованого шляху AP спрощується так, що оцінка спостережуваності може накопичуватися при послідовному моделюванні шляху AP на окремих словах режиму ІУС.

У випадку $\exists(I, J)$, $D_{IJ} > 0$ вузол U_I моделюється на вході Z_{IJ}, який приймає значення, що обчислюється для поточного слова й слова, що надходить на вхід цифрового компонента на D_{IJ} тактів раніше або пізніше. У загальному випадку, цим словом може бути будь-яке вхідне слово розглянутого режиму. Тому вузол U_I повинен моделюватися для кожного вхідного слова на значеннях входу Z_{IJ} які їм приймаються на всіх словах розглянутого режиму.

Для інерційних процесів зміни вхідних даних, оброблюваних у цифровому компоненті, модель шляху AP може бути уточнена з урахуванням максимально можливого кроку Δ зміни вхідних слів або складових їх операндів. Нехай $\Delta \geq 1$. Тоді вузол U_I повинен моделюватися для кожного вхідного слова з номером G на значеннях входу Z_{IJ}, які їм приймаються в діапазоні слів з номерами $G \pm \Delta \cdot D_{IJ}$, де $G > \Delta \cdot D_{IJ}$. Для $G \leq \Delta \cdot D_{IJ}$ використовуються вихідні настановні значення входу D_{IJ}. У випадку $\Delta < 1$, коли значення вхідних слів змінюються не частіше, чим один раз за $1 / \Delta$ тактів, діапазон номерів округляється до значення $G \pm] \Delta \cdot D_{IJ} [$.

Побудова моделі шляху AP виконується аналізом структури конвеєра з урахуванням кількості ділянок, що передають вузлу обробки даних U_I по його входах Z_{IJ}. Кількість цих ділянок визначає кількість тактів, необхідне для доставки даних від входів схеми цифрового компонента до вузла U_I. Нехай H_{IJ} - кількість ділянок (тактів), що передають входу Z_{IJ}, а $H_{MAX} = \mathrm{MAX}(H_{IJ})$. Тоді в такті H_{MAX} для вузла U_I виконується рівність $H_{IJ} + Y_{IJ} = H_{MAX} + 1$, з якого випливає формула

$$Y_{IJ} = H_{MAX} + 1 - H_{IJ}, \qquad (2)$$

включаючи Y_I для входу Z_I.

Підстановка (2) в (1) визначає значення дистанції $D_{IJ} = |H_I - H_{IJ}|$ у моделі шляху AP за структурою конвеєра схеми цифрового компонента.

Спостережуваність точки схеми обчислюється в процесі моделювання конвеєрної схеми компонента на вхідних даних, які визначаються з урахуванням моделі шляху AP.

Моделювання цифрового компонента виконується по наступному методу. Зорганізується перебір вхідних слів розглянутого режиму і перебір точок схеми по ходу конвеєра. Значення обра-

ної точки обчислюється на заданому вхідному слові й доповнюється інверсним значенням. Значення всіх наступних точок схеми обчислюються для двох значень обраної точки до досягнення контрольної точки або точки, де результати обчислень збігаються. Якщо в контрольній точці результати є інверсними, то всі точки, що належать шляху, відносяться до 0-спостережуваних або 1-спостережуваних залежно від прийнятого ними значення. Якщо на попередніх вхідних слова точка була ідентифікована як спостережувана із протилежним значенням, то ця точка відноситься до спостережуваних і не розглядається на наступних вхідних словах. Значення точок з $D_{IJ} > 0$ обчислюються на розширеній множині вхідних слів. Моделювання виконується з урахуванням усіх їхніх значень.

Слід зазначити, що неповне моделювання схеми цифрового компонента у випадку обмеження вхідних даних, характерних для розглянутого режиму роботи, веде до недооцінки спостережуваності точок. Така недооцінка, допущена для нормального й аварійного режиму, веде до помилкового виявлення потенційно небезпечних точок та їх пропуску відповідно.

ІІІ. ВИСНОВОК

Два режими роботи, характерні для ІУС критичного застосування, породжують проблему прихованих несправностей, які можуть накопичуватися в нормальному режимі та знижувати відмовостійкість цифрового компонента у самому відповідальному аварійному режимі. В однорежимних системах такої проблеми немає, оскільки прихована несправність ніколи не прояв ляється, а якщо несправність виявилася, то вона не є прихованою.

Потенційно небезпечні точки, в яких виникає проблема прихованих несправностей, можуть бути виявлені за умови коректної оцінки спостережуваності точок схеми в кожному з обох режимів системи критичного застосування. Це, в свою чергу, потребує коректного визначення вхідних даних, на яких необхідно моделювати схему цифрового компонента. Повнота врахування вхідних даних, характерних для кожного режиму ІУС, забезпечується запропонованою моделлю активованого шляху конвеєрної схеми цифрового компонента. При неповному врахуванні вхідних даних обчислюється занижена оцінка спостережуваності, що приводить до неправильного виявлення потенційно небезпечних точок або їх пропуску відповідно у нормальному та аварійному режимах. Запропонована модель активованого шляху уточнює множину вхідних даних для визначення спостережуваності точок у конвеєрних схемах цифрових компонентів.

ЛІТЕРАТУРА

1. Yastrebenetsky M. A. (edit.). Safety of Nuclear Power Plants Instrumentation and Control Systems / M. A. Yastrebenetsky. - Ukraine, Kyiv: Technika, 2004. - 472 p.
2. IEC 61508-1:2010, Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems - Part 1: General requirements. Geneva: Intemational Electrotechnical Commission, 2010.
3. 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.
4. FPGA-based NPP I&C Systems: Development and Safety Assessment / V. S. Kharchenko, V. V. Sklyar (edits). - RPC Radiy, National Aerospace University "KhAI", SSTC on Nuclear and Radiation Safety, 2008. - 188 p.
5. 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.
6. Drozd M. Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults / M. Drozd, A. Drozd // The 10th International Conference on Digital Technologies 2014. - Zhilina, Slovak Republic, 9 - 11 July, P. 137 - 140, 2014.
7. Drozd A. A new approach to solving a Problem of the Hidden Faults in Safety-Related Systems / A. Drozd, M. Drozd // Joumal of Information, Control and Management Systems. - 2014. - Vol. 12, No. 2. - P. 125 - 132.

V.V. Antoniuk[1], O. V. Drozd[1], M. O. Drozd[1], I. M. Nikolenko[2]
1 Odessa National Polytechnical University, ave Shevchenko, 1, Odessa, 65044
2 Odessa National Academy of food technology, Str. Dvoryanskaya, 1/3, Odessa, 65082

ASSESSMENT OF OBSERVABILITY FOR THE POINTS OF A PIPELINE CIRCUIT OF THE DIGITAL COMPONENTS IN SAFETY-RELATED SYSTEMS

A problem of the hidden faults without solving of which the fault tolerant structure of the digital components does not guarantee function safety of the safety-critical systems is considered. The problem is shown in the potentially hazardous circuit points, which in a normal mode can accumulate the hidden faults reducing the fault tolerance of the digital component at transition to an emergency mode of the system operation. A model of the activated path for pipeline circuit of the digital component is offered. It allows determining input data for calculation of point observabllity in modes of the system. A method of potentially hazardous point identification for pipeline circuit of the digital component is developed.
***Keywords**: Safety-critical system - Digital component - Pipeline circuit - Hidden fault - Potentially hazardous points - Model of the activated path.*

REFERENCES

1. Yastrebenetsky M. A. (edit.). Safety of Nuclear Power Plants Instrumentation and Control Systems / M. A. Yastrebenetsky. - Ukraine, Kyiv: Technika, 2004. - 472 p.
2. IEC 61508-1:2010. Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems - Part 1: General requirements. Geneva: Intemational Electrotechnical Commission, 2010.
3. 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.
4. FPGA-based NPP I&C Systems: Development and Safety Assessment / V. S. Kharchenko, V. V. Sklyar (edits). - RPC Radiy, National Aerospace University "KhAI", SSTC on Nuclear and Radiation Safety, 2008. - 188 p.
5. Rabochee diagnostirovanie bezopasnyh informacionno-upravljaushchih system / Pod red. Drozda A. V. i Kharchenko V. S. - Kharkov: Nationalniy aerokosmicheskiy universitet im. N. E. Zhukovskogo «KhAI», 2012. - 614 p.
6. Drozd M. Safety-Related Instrumentation and Control Systems and a Problem of the Hidden Faults / M. Drozd, A. Drozd // The 10th International Conference on Digital Technologies 2014. - Zhilina, Slovak Republic, 9-11 July, P. 137 - 140, 2014.
7. Drozd A. A new approach to solving a Problem of the Hidden Faults in Safety-Related Systems / A. Drozd, M. Drozd // Joumal of Information, Control and Management Systems. - 2014. - Vol. 12, No. 2. - P. 125 - 132.