УДК 629.039.58: 681.518.3

ЗАБЕЗПЕЧЕННЯ ТА ОЦІНЮВАННЯ ДІАГНОСТИЧНОГО ПОКРИТТЯ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ НА БАЗІ ПЛІС

Скляр В. В.

Публічне акціонерне товариство "Науково-виробниче підприємство "Радій" (м. Кіровоград)

Запропоновано підхід до забезпечення та оцінювання діагностичного покриття інформаційно-управляючих систем (ІУС) на базі ПЛІС, що є важливим показником, який впливає на функціональну безпеку.

Постановка проблеми. Цифрові системи на базі програмованих логічних інтегральних схем (ПЛІС) зайняли сталу нішу у промислової автоматиці, де складають конкуренцію традиційним програмованим логічним контролерам (ПЛК) з використанням мікропроцесорів.

Функціональна безпека ПЛК у складі інформаційно-управляючих систем (ІУС), як на базі мікропроцесорів, так і на базі ПЛІС залежить від того, наскільки повно охоплено діагностикою компоненти системи. Типові ПЛК включають до складу: шасі, модулі вводу / виводу для прийому та видачі аналогових та дискретних сигналів різних номіналів та модулів управління для виконання алгоритмів управляючої логіки. Такі ПЛК використовуються у якості бази для конфігурування ІУС різного об'єму та складності.

У теорії діагностики для оцінювання повноти діагностичного покриття використовується співвідношення D = ND / N, де ND – кількість компонентів ІУС, для яких реалізовано виконання діагностики, N – загальна кількість компонентів ІУС. Діагностика може бути вбудованою (самодіагностика) та зовнішньою. Оскільки ІУС, що виконують функції моніторингу та контролю складних об'єктів управління, є оздобленими засобами активної діагностики, як правило, для них річ йдеться про самодіагностику. Така самодіагностика може розглядатись для декількох ієрархічних рівнів, так як ця функція є досить складною і на верхньому рівні системи так чи інакше охоплює усі підсистеми. Таким чином, загальна картина може показувати 100% діагностичного покриття, однак, щоб визначити дійсне значення цього показника, необхідно провести більш глибокий аналіз самодіагностики компонентів ІУС.

Аналіз останніх досліджень і публікацій. Проблеми обчислення діагностичного покриття ставились та вирішувались з початку масового використовування ПЛІС для ІУС [1]. У сучасних дослідженнях [2] проведено аналіз фірмових алгоритмів розробника, які гарантують повноту діагностичного покриття апаратних ресурсів, до яких розробник не дає доступу користувачу. Важливим напрямком є також адаптація досягнень електроніки для використання у засобах ІУС, важливих для безпеки [3].

Однак, у відомих роботах не містяться у достатньому обсязі результати аналізу засобів діагностики ПЛК та ПЛІС, які б забезпечували високу ступінь діагностичного покриття з урахуванням різноманітних програмно-апаратних компонентів.

Мета статті. Таким чином, у статті пропонується підхід до забезпечення та оцінювання діагностичного покриття інформаційно-управляючих систем (ІУС) на базі ПЛІС з урахуванням наявних компонентів кристалу та ПЛК.

Основні матеріали дослідження.

Засоби діагностики залежать від типу компонентів, для яких вони передбачені. Для цифрових ІУС може бути розглянуто три типа таких компонентів: апаратні засоби (АЗ), програмні засоби (ПЗ) та комунікаційні лінії. Таким чином, формула повноти діагностичного покриття набуває виду

$$D = (ND_{HW} + ND_{SW} + ND_{COM}) / (N_{HW} + N_{SW} + N_{COM}),$$

де ND_{HW}, ND_{SW}, ND_{COM} – кількість компонентів АЗ, ПЗ та комунікацій, для яких реалізовано виконання діагностики, крім того, $ND = ND_{HW} + ND_{SW} + ND_{COM}$;

N_{HW}, N_{SW}, N_{COM} – загальна кількість компонентів АЗ, ПЗ та комунікацій, крім того, $N = N_{HW} + N_{SW} + N_{COM}$.

Крім того, для кожного з трьох компонентів може бути визначена особиста повнота діагностичного покриття за формулами:

$D_{HW} = ND_{HW} / N_{HW}$;

$D_{SW} = ND_{SW} / N_{SW}$;

$D_{COM} = ND_{COM} / N_{COM}$.

На підставі трьох наведених вище показників може бути визначено приблизне значення загальної повноти діагностичного покриття, як $D \approx (D_{HW} + D_{SW} + D_{COM}) / 3$.

Графічна інтерпретація повноти діагностичного покриття представлено на рисунку 1.

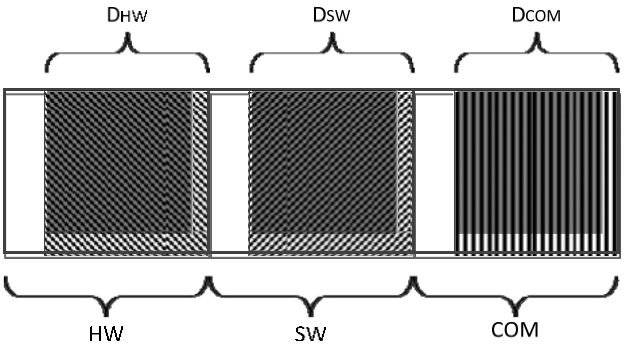

Рисунок 1 – Графічна інтерпретація повноти діагностичного покриття

Стандарт МЕК 61508 "Функціональна безпека електричних / електронних / електронних програмованих систем, що відносяться до безпеки" застосовується у ряді країн, в тому числі, й в Росії, у якості ос-

нови регулюючих вимог з безпеки, що висуваються до критичних ІУС.

В основі вимог з функціональної безпеки лежить поняття рівня інтегрованості (повноти, цілісності) безпеки (Safety Integrity Level – SIL). Найвищий рівень безпеки відповідає SIL4. Системи безпеки АЕС, наприклад, повинні відповідати рівню SIL3. Для кожного з рівнів SIL встановлюється перелік вимог з безпеки, включаючи відповідні значення показників безпеки, а також перелік заходів, які полягають у дотриманні вимог до процесів життєвого циклу, спрямованим на досягнення вимог з безпеки.

Згідно МЕК 61508 відмови системи діляться на наступні групи. З точки зору впливу на безпеку системи розрізняються небезпечні відмови (такі відмови, які призводять до відмови функції безпеки або знижують ймовірність коректного виконання функції безпеки за запитом) і безпечні відмови (такі відмови, які призводять до помилкового спрацьовування функцій безпеки, що переводить систему в безпечний стан, або підвищують ймовірність помилкового спрацьовування функцій безпеки). З точки зору детектування відмов засобами самодіагностики розрізняються виявлені і приховані відмови. Таким чином, маємо чотири групи відмов: небезпечні приховані , небезпечні виявлені, безпечні приховані та безпечні виявлені. Очевидно, що перша група відмов являє собою найбільшу небезпеку. Саме з наявністю цієї групи відмов пов'язане поняття частки (фракції) безпечних відмов (Safe Failure Fraction – SFF), під якою розуміється відношення суми інтенсивностей всіх безпечних відмов і небезпечних виявлення відмов до загальної інтенсивності відмов (тобто в чисельнику відсутня інтенсивність небезпечних прихованих відмов).

SFF є важливим показником безпеки, від якого залежить досягнення того чи іншого рівня SIL (див. таблицю 1). SFF залежить від повноти діагностичного покриття , яке повинно знижувати частку небезпечних прихованих відмов до необхідного рівня. Для спрощених розрахунків можна прийняти SFF рівній повноті діагностичного покриття. Самодіагностика реалізується для всіх компонентів ІУС: АЗ, ПЗ, а також ліній комунікації. SFF залежить також від ступеня резервування системи , яка в МЕК 61508 трактується як стійкість АЗ до відмов (Hardware Fault Tolerance, HFT).

Таблиця 1 – Значення SFF для різних рівнів SIL залежно від ступеня резервування системи

SFF	Нерезервована система (HFT=0)	Резервована система "1 з 2", "2 з 3" (HFT=1)	Резервована система "1 з 3", "2 з 3" з переходом в "1 з 2" або "1 з 1" (HFT=2)
> 60%	–	SIL1	SIL2
60% – < 90%	SIL1	SIL2	SIL3
90% – < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

Особливості ІУС на базі ПЛІС з точки зору діагностування полягають, по-перше, у використанні програмного коду на специфічних язиках опису АЗ (так звані Hardware Description Languages – HDL), а по-друге, у особливості апаратних ресурсів кристалу. Найбільш розповсюдженими у дійсний час є ПЛІС з використанням технології SRAM (енергозалежна пам'ять) та EEPROM або flash (енергонезалежна пам'ять). Для ПЛІС типу SRAM можуть наступати події, які залежать у перекручені даних, що зберігаються у пам'яті, за рахунок пошкодження напівпровідникових структур нейтронами (так званий Single Event Upset – SEU). Таким чином, процедури діагностування ІУС з використанням ПЛІС типу SRAM мають включати дії контролю інтегрованості області пам'яті та даних, які там зберігаються. Що стосується кодів на язиках HDL, які для ПЛІС получили назву електронних проектів, для них можуть бути застосовані типові процедури діагностування ПЗ.

Класифікація засобів самодіагностування (СД) ІУС на базі ПЛІС може бути представлена у вигляді, як на рисунку 2. При розрахунки повноти діагностичного покриття мають бути враховані усі ідентифіковані засоби.

На рисунку 3 представлена проста схема реалізації системи з самодіагностикою на базі ПЛІС. Архітектура кристалів ПЛІС дозволяє виконувати паралельну обробку діагностичних та управляючих даних. Тактуючу частоту для цього треба задавати з окремих генераторів (CLK). У системах безпеки досить розповсюдженими є зовнішні сторожеві таймери (ватчдоги), які працюють у окремому частотному домені CLK A. При виявленні проблеми засобами діагностики відсилається сигнал у ватчдог, за яким ватчдог виконує перезавантаження системи за сигналом Reset. Наведена на рисунку 3 архітектура є досить розповсюдженою у системах, важливих для безпеки.

Що до діагностування компонентів АЗ та комунікацій, для ІУС на базі ПЛІС, вони також можуть бути досить типовими. Типові компоненти діагностування АЗ включають, наприклад, додаткові контрольні ключі для ліній дискретних сигналів, дубльовані аналогово-цифрові та цифро-аналогові перетворювачі (АЦП та ЦАП).

Типові компоненти діагностування комунікацій використовують циклічні надлишкові коди (Cyclic Redundancy Check – CRC). Надлишковість (порядок поліному) CRC залежить від припустимої імовірності перекручення біту інформації у пакеті, що, у свою чергу, визначається впливом ІУС на безпеку об’єкту управління. Наприклад, для передачі даних у кристалі між компонентами електронного проекту ПЛІС для кожного шістнадцяти бітного слова може застосовуватися поліном п’ятого ступеню CRC-5 ($x^5+ x^2+ 1$).

Висновки. Таким чином, для повного аналізу діагностичного покриття ІУС на базі ПЛІС необхідно розглядати повний обсяг компонентів програмно-апаратних модулів та шасі, що входять до складу, а саме, самодіагностування АЗ, ПЗ та ліній комунікацій.

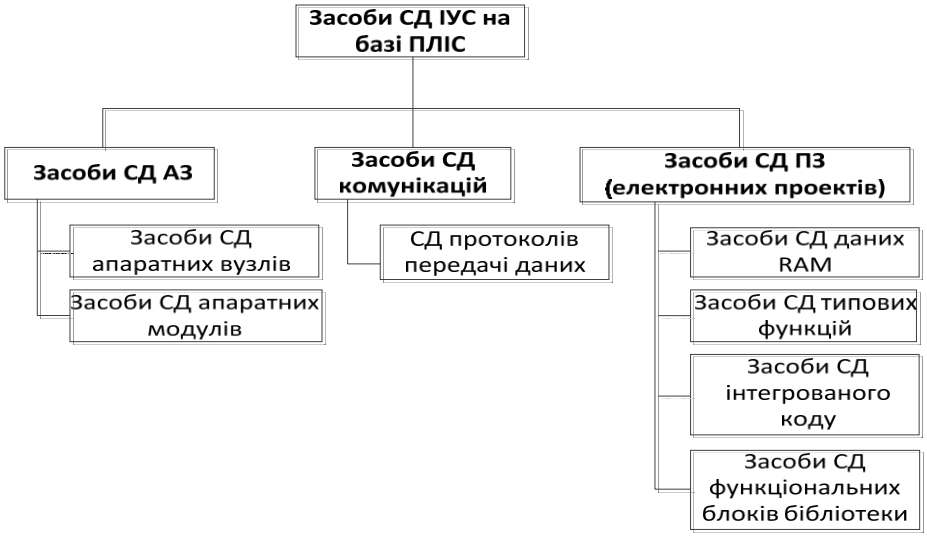

Рисунок 2 – Класифікація засобів самодіагностування (СД) ІУС на базі ПЛІС (варіант 1)

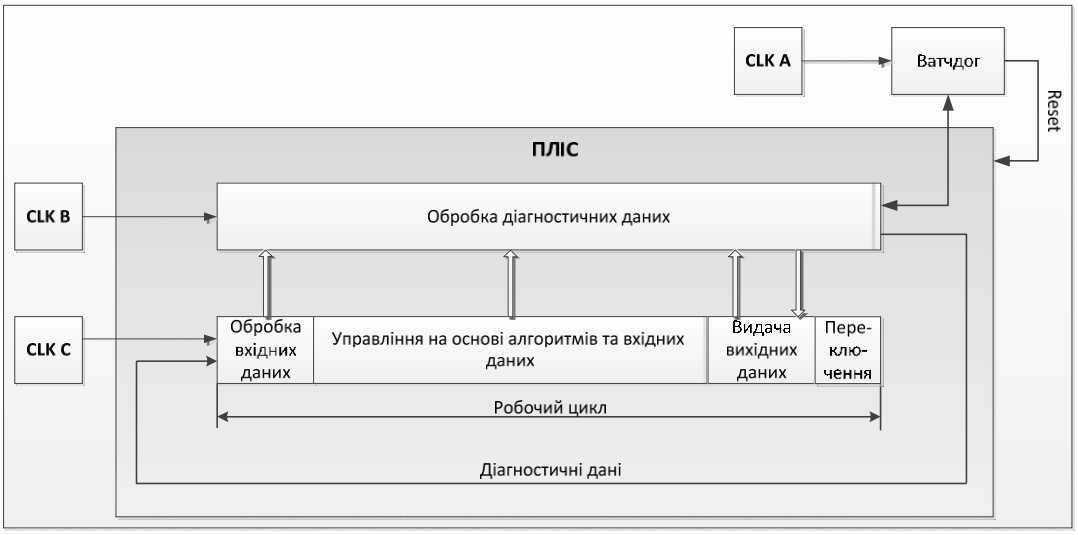

Рисунок 3 – Класифікація засобів самодіагностування (СД) ІУС на базі ПЛІС (варіант 2)

Список використаних джерел

1. Бутаков Е. А. Диагностика программируемых логических матриц / Е. А. Бутаков, М. Б. Волынский, В. Г. Новоселов – М.: Радио и связь, 1991 – 160 с.

2. Naber N. Real-Time Fault Detection and Diagnostics Using FPGA-based Architectures / N. Naber, T. Getz, Yong Kim, J. Petrosky. – Proceeding of the International Conference on Field Programmable Logic and Applications (FPL), 2010, Aug. 31 2010-Sept. 2 2010, Milan, Italy. – P. 346-351.

3. Системы управления и защиты ядерных реакторов / М. А. Ястребенецкий, Ю. В. Розен, С. В. Виноградская, Г. Джонсон, В. В. Елисеев, А. А. Сиора, В. В. Скляр, Л. И. Спектор, В. С. Харченко; под. ред. М. А. Ястребенецкого. – К: Основа – Принт, 2011. – 768 с.

Аннотация

ОБЕСПЕЧЕНИЕ И ОЦЕНИВАНИЕ ДИАГНОСТИЧЕСКОГО ПОКРЫТИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ НА БАЗЕ ПЛИС

Скляр В. В.

Предложен подход к обеспечению и оцениванию диагностического покрытия информационно-управляющих систем (ИУС) на базе ПЛИС, с учетом тренований к функциональной безопасности.

Abstract

ASSURANCE AND ASSESSMENT OF DIAGNOSTIC COVERAGE FOR INSTRUMENTATION AND CONTROL SYSTEMS BASED ON FPGA

V. Sklyar

The paper discusses an approach to the assurance and assessment of the diagnostic coverage of FPGA-based I&C systems taking into account functional safety needs.