

РЕЦЕНЗІЯ

кандидата технічних наук, доцента Куланова Віталія Олександровича
на дисертаційну роботу

Панаріна Артема Сергійовича

на тему «Методи та засоби забезпечення функційної безпечності інформаційно-керуючих систем АЕС на програмовних платформах з використанням комбінованої диверсності»,

подану на здобуття ступеня доктора філософії

у галузі знань 12 Інформаційні технології

за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дисертації

Перехід інформаційно-керуючих систем (ІКС) атомних електростанцій на програмовні платформи (FPGA, SoC) відкриває нові можливості для підвищення продуктивності та гнучкості, однак водночас загострює проблему відмов за загальною причиною (ВЗЗП) – сценаріїв, коли одна конструктивна, технологічна або програмна вада може одночасно вразити декілька каналів багатоверсійної системи. Існуючі класифікатори диверсності (NUREG/CR-6303, NUREG/CR-7007) мають переважно описовий характер і не надають формалізованих інструментів для обґрунтованого вибору конкретних видів диверсності з урахуванням вартісних обмежень. Дисертація Панаріна А.С. спрямована на подолання цього розриву шляхом розроблення розширеної класифікації, графових і матричних моделей, методу вибору диверсних рішень, а також методу модельно-базованої верифікації. Робота є безперечно актуальною як для наукової спільноти, так і для практики проєктування та сертифікації систем безпеки АЕС в Україні, особливо з огляду на модернізацію на платформах вітчизняного виробництва Radiy та RadICS.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукова новизна отриманих результатів полягає в наступному:

1. **Дістала** подальшого розвитку графова модель опису різних програмно-апаратних версій для інформаційно-керуючих систем на програмовних платформах з використанням деталізованого класифікатора видів диверсності – процесорних ядер, інтерфейсів, засобів синхронізації, технологічних процесів і обладнання, що дозволяє оцінювати метрики диверсності і складності залежно від множини видів і підвидів версійної надмірності.

2. **Удосконалено** метод вибору видів диверсності з урахуванням багаторівневої ієрархії видів версійної надмірності, включно з внутрішньою диверсністю каналів, а також відповідні метрики диверсності і складності, що дозволяє підвищити функційну безпечність і обґрунтувати структуру та процеси створення двоверсійних систем аварійного захисту реакторів АЕС.

3. **Удосконалено** методи програмно-апаратної диверсності, які базуються на процедурах функційно-просторової диверсифікації засобів шинної організації, контролю цілісності даних, налаштувань проєкту та синхронізації з керованими зсувами, що зменшує ризики завад і відмов спільних логічних елементів версій.

4. **Вперше запропоновано** метод модельно-базованого тестування систем програмовної логіки, який, на відміну від відомих, ґрунтується на порівнянні версій,

отриманих з використанням мови програмування Haskell та її конвертованої моделі у VHDL-код, а також еталонного проекту, розробленого за технологією SoC, що зменшує ризики залишкових прихованих дефектів.

Обґрунтованість результатів підтверджується коректним застосуванням математичного апарату (теорія множин, теорія графів, теорія надійності), відповідністю запропонованих рішень вимогам міжнародних стандартів IEC 61513, IEC 60880, IEC 62138, IEC 61508, а також узгодженістю теоретичних викладок з експериментальними даними. Достовірність забезпечена моделюванням кортежу тактування трьох каналів, де показано зниження максимальної кількості одночасних перемикачів з 25 до 22 та інтегральний ефект рівномірності -39,40 % (табл. 3.1-3.3); експериментальною перевіркою методу модельно-базованого тестування на прикладі порівняння еталонної реалізації soft-процесора Nios з диверсною моделлю ForSyDe, де розрахований інтегральний коефіцієнт диверсності $K_d = 0,9$ (табл. 4.1). Еквівалентність результатів перевірено на трьох рівнях опису: блок-схеми алгоритму мовою C, функційного опису Haskell/ForSyDe та VHDL-моделі, синтезованої у Quartus II, з порівнянням часових діаграм у середовищі ModelSim, а також позитивними актами впровадження на підприємствах атомної енергетики.

Відповідні акти впровадження на підприємствах галузі підтверджують практичну значущість роботи. Отже, представлені наукові результати відповідають темі дисертації, а поставлене в роботі наукове завдання – підвищення функційної безпечності багатоверсійних ІКС АЕС на програмовних платформах засобами комбінованої диверсності – вирішено, а здобувач демонструє належне володіння методологією наукових досліджень.

Оцінка змісту дисертації, її завершеності та дотримання принципів академічної доброчесності

Дисертаційна робота за своїм змістом узгоджується з освітньо-науковою програмою підготовки докторів філософії зі спеціальності 123 Комп'ютерна інженерія та охоплює широке коло питань – від аналізу нормативної бази до розроблення конкретних алгоритмів, апаратних прототипів і методичних рекомендацій.

Робота є логічно завершеною науковою працею, в якій простежується особистий внесок автора: ним сформульовано мету та завдання дослідження, розроблено розширену класифікацію, графову та матричну моделі, метод вибору видів диверсності, методи програмно-апаратної диверсності та метод модельно-базованої верифікації, проведено експерименти, здійснено впровадження та узагальнено результати.

Перевірка на текстові збіги засвідчує, що дисертація є оригінальним авторським дослідженням, у якому відсутні ознаки академічного плагіату, фабрикації чи фальсифікації. Усі запозичені ідеї, результати та цитати супроводжуються посиланнями на першоджерела. Це дозволяє зробити висновок про дотримання здобувачем принципів академічної доброчесності.

Мова та стиль викладення результатів

Дисертацію викладено українською мовою з дотриманням наукового стилю. Текст відзначається послідовністю, логічністю та аргументованістю. Автор коректно використовує професійну термінологію, визначає нові поняття («графова модель диверсності», «диверсна синхронізація», «інтегральний коефіцієнт диверсності»), що полегшує сприйняття матеріалу. Рисунки та таблиці органічно доповнюють текст і

сприяють розумінню складних залежностей. Стиль викладення є зрозумілим для фахівців у галузі комп'ютерної інженерії та функційної безпечності.

Структура роботи

Дисертація має класичну структуру: анотація двома мовами, зміст, перелік умовних скорочень, вступ, чотири розділи, висновки, список використаних джерел (138 позицій) та два додатки. Загальний обсяг відповідає встановленим вимогам.

У вступі чітко окреслено проблемне поле, обґрунтовано актуальність, сформульовано мету, завдання, об'єкт, предмет, методи, новизну та практичне значення.

Перший розділ присвячено аналізу вимог міжнародних і національних стандартів до функційної безпечності ІКС АЕС, аналізу відмов, зокрема відмов за загальною причиною, а також наявних класифікаційних схем і методів оцінювання диверсності; виявлено їх обмеження для програмовних платформ і обґрунтовано мету, задачі та методику досліджень.

Другий розділ є ключовим з погляду новизни: розроблено розширену чотирирівневу класифікацію видів і підвидів диверсності, графову та матричну моделі, метод вибору видів диверсності з алгоритмами пошуку за одним шляхом і за комбінацією шляхів, а також виконано оцінювання імовірності безвідмовної роботи двоверсійної системи аварійного захисту реактора.

Третій розділ присвячений методам реалізації програмно-апаратної диверсності – диверсній синхронізації каналів, структурно-просторовій диверсності матриць логічних елементів і таймінгу проходження сигналів, диверсифікації засобів і процедур підрахунку контрольної суми, а також методів передачі даних і перевірки цілісності пам'яті; наведено результати моделювання.

Четвертий розділ описує метод модельно-базованої верифікації систем програмовної логіки, його експериментальну перевірку на прикладі диверсної моделі soft-процесора, узагальнену послідовність розроблення та верифікації двоверсійних систем, а також упровадження результатів досліджень.

Висновки узагальнюють отримані результати та співвіднесені з поставленими завданнями; окремі неузгодженості їх формулювань з основним текстом зазначено нижче.

Дисертаційну роботу оформлено з дотриманням вимог наказу МОН України № 40 від 12.01.2017.

Практичне значення отриманих результатів

Практичне значення роботи полягає у доведенні теоретичних положень до конкретних методик, алгоритмів та апаратних рішень – розширеного класифікатора і графової моделі диверсності, методу вибору видів диверсності, методів диверсної синхронізації каналів, структурно-просторової диверсності матриць логічних елементів, диверсифікації засобів контролю цілісності даних, а також методу модельно-базованої верифікації. Результати впроваджено у ПАТ «НВП “Радій”» при розробленні та постачанні платформних рішень для інформаційно-керуючих систем енергоблоків Запорізької, Рівненської, Хмельницької та Південноукраїнської АЕС, у ТОВ «НВП “РАДІКС”» – у науково-дослідних проєктах і розробках, а також у навчальному процесі та науково-дослідних роботах кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут», що підтверджено відповідними актами впровадження (Додаток А).

Оприлюднення результатів дисертаційної роботи

Основні наукові положення дисертації опубліковано у 15 наукових працях, серед яких: 6 статей у наукових фахових виданнях України; 1 стаття у виданні Springer з індексацією у базі Scopus; 3 колективні монографії, одна з яких індексується у базі Scopus; 4 публікації у матеріалах міжнародних наукових конференцій, що індексуються у базі Scopus (IDT, IDAACS, DESSERT, ICONE); 1 стаття у науковому виданні Національного аерокосмічного університету «Харківський авіаційний інститут».

Наукові результати, викладені у публікаціях, відповідають темі дисертації та розкривають її основні положення. У спільних публікаціях особистий внесок здобувача виокремлено; він стосується безпосередньо розроблення класифікаційних схем, графової та матричної моделей, методу вибору видів диверсності та модельно-базованого тестування. Порушень академічної доброчесності у публікаціях не виявлено, посилання на роботи інших авторів оформлено належним чином.

Таким чином, наукові результати дисертаційної роботи повністю та своєчасно оприлюднені, що відповідає вимогам до робіт на здобуття ступеня доктора філософії.

Недоліки та зауваження до дисертаційної роботи

Загалом позитивно оцінюючи роботу, вважаю за необхідне зазначити такі зауваження.

1. Моделювання диверсної синхронізації наведено для одного випадку з трьома каналами та індивідуальними циклічними зсувами (табл. 3.1-3.3); мультикластерні конфігурації описано текстом і подано на рис. 3.1-3.2, проте без кількісних результатів. Рекомендацію щодо застосування FPGA різних виробників (Xilinx та Intel/Altera) і різних інструментальних середовищ проєктування, сформульовану в підрозділі 1.3, в експериментальній частині застосовано не було: обидві версії синтезуються та компілюються одним інструментальним ланцюжком (Quartus II). Доцільно було б доповнити експериментальну частину хоча б одним мультикластерним прикладом.

2. Метрики диверсності та відносної вартості (підрозділ 2.4) отримано усередненням рангових оцінок десяти експертів, компетентність яких прийнято однаковою. Узгодженість цих оцінок кількісно не оцінювалася, хоча вихідні дані табл. 2.1 показують певний розкид рангів для окремих альтернатив; аналізу чутливості результатів вибору до варіації вагових коефіцієнтів також не наведено. Оскільки на цих метриках побудовано графову модель і метод вибору видів диверсності, робота виграла б від такої перевірки.

3. У формулюваннях наукової новизни наявні окремі розбіжності між анотацією, вступом і висновками: метод вибору видів диверсності в анотації подано як розроблений, у вступі – як удосконалений. У висновках наведено характеристики, які в основному тексті не деталізовано (модифікація алгоритму Дейкстри, «понад 60 підвидів диверсності»), а чотирирівневу класифікацію описано як сукупність архітектурного, апаратного, програмно-алгоритмічного та експлуатаційного рівнів, тоді як у підрозділі 2.1 і на рис. 2.1 це рівні деталізації класифікатора. Ці формулювання варто було б привести до єдиної редакції.

4. Наявні окремі недоліки термінології та оформлення. У тексті паралельно вживаються «відмова за загальною причиною» та «відмова за спільною причиною», у табл. 2.2 використано скорочення «ВЗП», відсутнє в переліку умовних скорочень, а у

висновках зустрічаються «програмні платформи» і «системи програмної логіки» замість «програмовні». Також рисунки 2.1 і 2.7 через високу щільність вузлів у форматі сторінки важко читаються.

Наведені зауваження не є принциповими: вони стосуються переважно повноти викладу та редакційного узгодження тексту і можуть бути враховані в подальших публікаціях. Загалом вони не знижують наукової цінності та практичної значущості роботи. Як перспективні напрями подальших досліджень варто відзначити оцінювання економічного ефекту впровадження методів диверсності, який у роботі розглянуто через відносні нормовані метрики вартості, та адаптацію запропонованих рішень до умов воєнного часу – живучості й відновлюваності систем безпеки АЕС за зовнішніх впливів на критичну інфраструктуру.

Висновок про дисертаційну роботу

Дисертаційна робота Панаріна Артема Сергійовича на тему «Методи та засоби забезпечення функційної безпечності інформаційно-керуючих систем АЕС на програмовних платформах з використанням комбінованої диверсності» виконана на належному науковому рівні, є завершеним дослідженням, не містить ознак академічної недобросовісності та розв'язує важливе наукове завдання – підвищення функційної безпечності багатоверсійних ІКС атомних електростанцій на програмовних платформах шляхом застосування комбінованої диверсності та модельно-базованої верифікації, що має суттєве значення для галузі знань 12 Інформаційні технології та спеціальності 123 Комп'ютерна інженерія.

За актуальністю, науковою новизною, практичною реалізацією та обсягом публікацій робота відповідає вимогам п.п. 6-9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44. Здобувач Панарін Артем Сергійович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:

кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та інтелектуальних
інформаційних технологій
Національного аерокосмічного університету
«Харківський авіаційний інститут»

Віталій КУЛАНОВ