

РЕЦЕНЗІЯ

кандидата технічних наук, доцента Куланова Віталія Олександровича

на дисертаційну роботу

Леонтієва Костянтина Петровича

на тему «Методи і засоби оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з урахуванням критичності припущень і помилок аналізу»,

подану на здобуття ступеня доктора філософії

у галузі знань 12 Інформаційні технології

за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дисертації

Сучасний розвиток інформаційно-керуючих систем (ІКС) критичного призначення, зокрема для атомних електростанцій, нерозривно пов'язаний із застосуванням програмовних логічних платформ (FPGA, SoC, ПЛК). Це дозволяє реалізовувати складні алгоритми управління та діагностування, але водночас породжує нові класи дефектів – від фізичних збоїв до систематичних помилок проектування й конфігурації.

Існуючі методи оцінювання функційної безпечності, такі як FMECA/FMEDA, орієнтовані переважно на одиничні відмови та не враховують належним чином багаторівневу природу дефектів, множинні комбінації, а також суб'єктивний вплив експертних припущень, що може призводити до некоректних висновків про рівень безпечності. Додатковим чинником є те, що ліцензування платформ і систем потребує значних ресурсів, а більшість сучасних технік оцінювання функційної безпечності ІКС АЕС потребують експертної підтримки навіть за наявності інструментальних засобів.

Дисертація Леонтієва К. П. пропонує системне вирішення цих проблем шляхом розроблення вдосконалених моделей, методів та інструментальних засобів, що враховують критичність припущень і дозволяють зменшити вплив помилок експертного аналізу. Таким чином, тема роботи є своєчасною та має безсумнівну актуальність як для науково-методологічної, так і для прикладної інженерної практики.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукова новизна отриманих результатів полягає в наступному:

1. **Удосконалено** моделі і показники для оцінювання функційної безпечності ІКС на програмовних платформах з використанням табличного методу аналізу видів і наслідків відмов (FMECA/FMEDA) шляхом визначення і зменшення кількості критичних припущень і обмежень при формуванні та заповненні таблиць, а також детермінованого представлення і перебору причин відмов і рівнів небезпеки внаслідок різних дефектів. Особливістю є введення формального апарату для ідентифікації, класифікації та оцінювання критичності припущень (методика АМЕСА), що дозволяє не лише кількісно оцінити ризики, але й контролювати повноту охоплення дефектів, чого бракує традиційним підходам.

2. **Удосконалено** метод експертного оцінювання функційної безпечності ІКС на програмовній логіці при використанні процедур FMECA/FMEDA шляхом зменшення кількості операцій із залученням експертів та впровадження спеціальних сценаріїв узгодження експертних оцінок у вигляді вербальної, нечіткої і кількісної інформації. Це підвищує об'єктивність і відтворюваність результатів, особливо в умовах недостатньої статистичної інформації.

3. **Уперше розроблено** метод оцінювання функційної безпечності двохверсійних ІКС на програмовних платформах з використанням комбінованих процедур аналізу дефектів версій, який відрізняється від відомих тим, що при аналізі видів та наслідків відмов формуються профілі відносних і абсолютних дефектів, а також використовуються регресійні процедури ін'єктування множинних дефектів з урахуванням їхнього самомаскування і блокування системи. У межах цього результату побудовано багаторівневу модель дефектів (фізичний L1, проєктно-логічний L2, архітектурно-платформний L3 та системно-мережевий L4 рівні), модель вразливостей багатоверсійності та метод MVSD-FMEA, що інтегрує дефекти, вразливості та механізми їх трансформації і дозволяє виявляти корельовані, спільні (CCF) та каскадні відмови, які залишаються поза межами традиційного FMEA/FMECA-аналізу.

Обґрунтованість результатів підтверджується коректним вибором математичного апарату: методів системного аналізу, теоретико-множинного опису, теорії графів та теорії імовірностей, теорії надійності та технічної діагностики, методів ризик-орієнтованого FMECA-аналізу і експертних оцінок. Достовірність забезпечена внутрішньою узгодженістю запропонованих моделей, відповідністю отриманих показників (DC, SFF, PFH, PFD_{avg}) вимогам стандартів IEC 61508 та IEC 61513, а також позитивними актами впровадження на провідних підприємствах атомної енергетики.

Дослідження виконано на кафедрі кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут» у межах державних і галузевих програм модернізації ІКС АЕС під науковим керівництвом члена-кореспондента НАН України, д. т. н., професора Харченка В. С.

Отже, поставлене в роботі наукове завдання – підвищення повноти та достовірності оцінювання функційної безпечності одно- та багатоверсійних ІКС на програмовних платформах – 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 і програмних засобів.

Робота є логічно завершеною науковою працею, в якій простежується особистий внесок автора: ним сформульовано мету та завдання дослідження, розроблено базові моделі,

удосконалено методи експертного оцінювання, створено метод MVSD-FMEA, 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 («профіль дефектів», «профіль вразливостей», «AMECA-аналіз»), 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: вступ, чотири розділи, висновки, список використаних джерел (90 позицій) та три додатки. Загальний обсяг – 208 сторінок, з них основного тексту – 168 сторінок; робота містить 21 рисунок і 15 таблиць.

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

Перший розділ присвячено аналізу нормативних вимог (IEC 61508, IEC 61513, IEC 61226, IEC 60880, IEC 62138, IEEE 7-4.3.2 тощо), методів FMECA/FMEDA, FIT, FTA та інструментальних засобів. Виявлено основні обмеження, пов'язані з експертними припущеннями та неповнотою моделей, сформовано профіль вимог до ІКС на програмовних платформах.

У другому розділі розроблено базову таблично-множинну модель FMECA/FMEDA, формалізовано множину припущень, запропоновано методику AMECA для оцінювання їх критичності, а також удосконалену модель EFMECA, яка забезпечує трасування залежності підсумкової оцінки безпечності від прийнятих припущень. Введено показники повноти та достовірності оцінювання.

Третій розділ присвячений експертному оцінюванню: визначено множини експертів, експертних задач і можливих рішень; запропоновано три базові сценарії узгодження — консервативний (ScC), оптимістичний (ScO) та зважений (ScW) — і додаткові сценарії ScDT та ScDW, що враховують різну кваліфікацію фахівців; розроблено процедури оцінювання критичності припущень і помилок аналізу за трирівневою шкалою Н/М/Л та алгоритм експертного оцінювання (рис. 3.9).

Четвертий розділ є найбільш змістовним з погляду новизни: побудовано багаторівневу модель дефектів (L1–L4), модель вразливостей багатоверсійності, запропоновано метод MVSD-FMEA, який об'єднує дефекти, вразливості, механізми трансформації та ефекти CCF. Наведено розрахункові співвідношення для показників DC,

SFF, PFH і PFD_{avg} , структуру розширеної таблиці MVSD-FMEA, що забезпечує перехід від показника RPN до кількісних показників функційної безпечності, а також результати практичного впровадження.

Висновки узгоджуються з поставленими завданнями та підкреслюють наукову і практичну цінність роботи.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України № 40 від 12.01.2017.

Практичне значення отриманих результатів

Практичне значення роботи полягає у доведенні теоретичних положень до конкретних алгоритмів і програмних засобів – AMECA-аналізу критичності припущень, процедур експертного оцінювання результатів FMECA/FMEDA та формування узгоджених експертних оцінок. Результати впроваджено у НВП «Радій» при розробленні ІКС енергоблоків Рівненської, Хмельницької та Південноукраїнської АЕС, у ТОВ «НВП «Радікс» – при сертифікації платформи RadICS на відповідність вимогам IEC 61508 (SIL3) та US NRC, а також у навчальному процесі Національного аерокосмічного університету «ХАІ», що підтверджено відповідними актами впровадження.

Оприлюднення результатів дисертаційної роботи

Основні наукові положення дисертації опубліковано у 19 наукових працях, серед яких:

- 4 статті у наукових фахових виданнях України (одна з них – у виданні «Радіоелектронні і комп'ютерні системи», індексованому в базі Scopus);
- 1 стаття у міжнародному журналі «Mathematics» (MDPI), індексованому в базі Scopus;
- 1 розділ у колективній монографії видавництва IGI Global;
- 13 доповідей і статей у матеріалах міжнародних наукових конференцій (IDT, NPIC&HMIT, ICONE, DESSERT, DepCoS-RELCOMEX).

Наукові результати, викладені у публікаціях, відповідають темі дисертації та розкривають її основні положення. У спільних публікаціях особистий внесок здобувача виокремлено; він стосується безпосередньо розроблення процедур експертного оцінювання, удосконалення методів FMECA/FMEDA та оцінювання критичності припущень і помилок аналізу. 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. У третьому розділі автор пропонує три базові сценарії узгодження експертних оцінок (ScC, ScO, ScW) і наводить алгоритм їх реалізації (рис. 3.9). Проте єдиним критерієм розгалуження в алгоритмі є однорідність кваліфікації експертів. Критерії вибору конкретного сценарію залежно від типу ІКС, необхідного рівня повноти безпеки (SIL) чи стадії життєвого

циклу системи не сформульовано, що ускладнює відтворюване застосування методу різними групами експертів.

2. У четвертому розділі при введенні операторів трансформації дефектів $T_{Lk \rightarrow Lk+1}$ (вирази 4.9–4.11) автор використовує коефіцієнти переходу $P_{k,k+1}$ (вираз 4.12), однак не наводить методик їх кількісного визначення для конкретних апаратних платформ, наприклад для FPGA різних виробників. Оскільки саме через ці коефіцієнти обчислюється еквівалентна інтенсивність системної відмови (вираз 4.13), відсутність такої методики ускладнює безпосереднє застосування методу на практиці без додаткових експериментальних досліджень.

3. У роботі застосовано розгалужений термінологічний апарат: поряд із відомими FMESA та FMEDA автор вводить AMESA, EFMECA, XMECA, MVSD-FMEA, «профіль дефектів» і «профіль вразливостей». Узагальнювальної схеми, яка показувала б співвідношення цих понять між собою та їх місце відносно відомих методик, у роботі немає, тому зв'язки доводиться відновлювати за текстом. Перелік умовних скорочень при цьому неповний: скорочення XMECA та EFMECA, які вживаються багаторазово, до нього не внесено і в тексті не розшифровано, а на с. 97 і 100 фігурує нерозшифроване скорочення EUMESA.

4. Рисунок 4.1 (с. 171), заявлений як узагальнена послідовність методу аналізу видів і наслідків відмов багатоверсійних ІКС, подано у вигляді однорядкового символного ланцюга, тоді як у тексті метод розгорнуто у вісім етапів. Доцільною була б розгорнута блок-діаграма з відображенням вхідних і вихідних даних кожного етапу за зразком рис. 3.9.

5. Третій науковий результат передбачає формування профілів відносних і абсолютних дефектів та використання регресійних процедур ін'єктування множинних дефектів з урахуванням їхнього саомаскування і блокування системи. У четвертому розділі профілювання дефектів подано за рівнями ієрархії L1–L4 (вираз 4.15), а зазначені процедури ін'єктування в тексті не деталізовано. Доцільно було б розкрити їх реалізацію та роль у зменшенні часу і підвищенні достовірності оцінювання ризиків відмов за спільною причиною (CCF).

Наведені зауваження стосуються переважно форми подання результатів та окремих деталей, які можуть бути усунуті в подальших публікаціях. Загалом наведені зауваження не знижують наукової цінності та практичної значущості роботи.

Висновок про дисертаційну роботу

Дисертаційна робота Леонтієва Костянтина Петровича на тему «Методи і засоби оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з урахуванням критичності припущень і помилок аналізу» виконана на належному науковому рівні, є завершеним дослідженням, не містить ознак академічної недоброчесності та розв'язує важливе наукове завдання – підвищення повноти та достовірності оцінювання функційної безпечності критичних ІКС на програмовних платформах, 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 Леонтієв Костянтин Петрович 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