ВІДГУК

офіційного опонента професора кафедри автоматизації проектування обчислювальної техніки Харківського національного університету радіоелектроніки, доктора технічних наук, професора Кривулі Геннадія Федоровича на дисертаційну роботу Одарущенка Олега Миколайовича, що виконана на тему: «Методи і засоби забезпечення надійності та функційної безпечності програмно-технічних комплексів з урахуванням фізичних і проєктних дефектів компонентів», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми дисертації

Програмно-технічні комплекси інформаційно-керуючих систем (ПТК ІКС) входять до складу сучасних технічних комплексів критичного використання та впливають на їх безпеку. До таких комплексів відносяться літальні (авіаційні, ракетні і ракетно-космічні), системи управління АЕС та інших технічні і організаційно-технічні комплекси критичного використання, ядро яких на даний момент саме реалізується у вигляді спеціалізованих ПТК.

Порушення функцій, які вони виконують, може привести до порушення безпечного стану критичних та бізнес-критичних об'єктів. Одними з основних властивостей ПТК ІКС, необхідних для забезпечення їх якісного функціонування, є надійність та функційна безпечність. Постійне збільшення обсягу програмно реалізованих функцій призводить до необхідності забезпечення надійності та функційної безпечності як апаратної, так і програмної складової. Зрозуміло, що за цих умов розширюється перелік причин порушення працездатності ПТК ІКС внаслідок прояву дефектів їх апаратних, програмних, програмовних компонент. Істотно, що в умовах значної вартості і суспільної значущості таких систем, необхідно прийняття обґрунтованих технічних рішень щодо їх побудови на етапах розробки. Досягти цього можливо шляхом математичного моделювання процесів їх функціонування. Моделювання можливе в умовах існування достатньо розвинутого науково-методичного апарату. Автором доведено, що сучасні методи і засоби оцінювання та забезпечення надійності та функційної безпечності не враховують повну множину причин і характеристик відмов і

порушень функціонування ПТК, що породжує протиріччя, яке полягає у невідповідності між розширенням множини причин порушення працездатності ПТК ІКС технічних комплексів критичного використання і рівнем розвитку концептуальних засад, сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпечності. Подолати це протиріччя можливо шляхом вирішення актуальної науково-прикладної проблеми комплексного оцінювання і забезпечення надійності і функційної безпечності ПТК ІКС критичного використання в процесі розроблення, верифікації, валідації та використання за призначенням з урахуванням відмов, обумовлених проєктними, фізичними дефектами і вразливостями програмних і апаратних засобів, а також зміни параметрів потоків їх відмов і відновлень.

Тому тема дисертації, яку запропонував автор і поставлена науково-прикладна проблема, є актуальними.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Автор обґрунтовано використовує відомі та багаторазово апробовані математичні теорії, методи та моделі, на підставі яких коректно здійснюється отримання нових наукових результатів.

У першому розділі автором виконано аналіз методів і засобів оцінювання та забезпечення надійності та функційної безпечності ПТК ІКС критичного використання. Проведено аналіз факторів впливу різної природи на надійність, функційну безпечність систем досліджуваного класу, визначена вартість наслідків їх відмов. Систематизовано вимоги державних та міжнародних стандартів до надійності і функційної безпечності ПТК та вимоги до організації процесів розробки, верифікації та валідації для забезпечення виконання цих вимог. Розглянуто узагальнені структури ПТК та ІКС як об'єктів моделювання. Виконано огляд методів і засобів оцінювання надійності і функційної безпечності ІКС критичного використання, прокласифіковано моделі і методи. Проведено аналіз математичного апарату та обмежень використання існуючих методів оцінювання. Визначено протиріччя та сформульовано науково-прикладну проблему. Обґрунтовано задачі, математичний апарат, етапи і методику досліджень.

У другому розділі дисертації, на основі попередніх досліджень, розроблено структуру методології оцінювання і забезпечення надійності та

функційної безпечності ПТК ІКС критичного застосування за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушень внаслідок проєктних і фізичних дефектів і дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що обґрунтовано забезпечує підвищення точності оцінювання і повне виконання вимог до відповідних показників.

У третьому розділі на підставі отриманого автором досвіду розроблення, рефакторинга та тестування програмних проєктів і базуючись на твердженні про внесення вторинних дефектів ПЗ в ході реалізації цих процесів розроблено множину сценаріїв внесення-усунення вторинних дефектів, що дало можливість виконати уточнення поведінки ПЗ в умовах відповідного сценарію за рахунок перебору співвідношень параметрів, що сценарій описують. З метою аналізу впливу процесів внесення-усунення вторинних дефектів на кількісні значення надійнісних параметрів виконано завдання вибору типу моделей оцінки надійності програмних засобів (МНПЗ). Для цього було виконано аналіз МНПЗ різних класифікаційних ознак, який дозволив сформулювати висновок про те, що для оцінювання надійності ПЗ з урахуванням фактора вторинних дефектів доцільно використовувати імовірнісні моделі, оскільки вони містять параметр, який характеризує інтенсивність їх прояву, яка обчислюється за допомогою функції ризику моделі. Виконано спрямований аналіз з метою вибору функцій ризику моделей, які можливо модифікувати для урахування встановленого фактору. За результатами цього аналізу обрано та модифіковано функції ризику наступних моделей оцінки програмних засобів: Джелінського-Моранди; Муси; простої експоненційної; Шика-Уолвертона.

У четвертому розділі, для реалізації визначеної концепції комплексного оцінювання надійності і функційної безпечності ПТК ІКС, виконано: систематизацію змінних параметрів; розроблено сценарії зміни параметрів; розроблено комплекс багатофрагментних марковських моделей та виконана їх класифікація і дослідження. Розроблено комплекс математичних моделей оцінювання та забезпечення надійності і функційної безпечності ПТК, які будуються за типовими багатокаскадними структурами. Істотним є те, що на базі виконаних досліджень та отриманих висновків побудовано пріоритетні ряди для типових архітектур ПТК, що полегшує їх вибір інженерам-проєктувальникам.

П'ятий розділ дисертації присвячено розробленню і дослідженню моделей оцінювання надійності та функційної безпечності ПТК на самодіагностовних платформах. Автор, доводить, що системи досліджуваного класу та їх ядро, програмовні логічні контролери, повинні

мати розвинуті підсистеми програмно-апаратного діагностування. Аналіз результатів дослідження розроблених моделей обгрунтовано дозволяють формулювати вимоги щодо підсистем програмно-апаратного самодіагностування програмвних логічних контролерів та ПТК, які будуються на їх основі.

Шостий розділ присвячено розробленню методів верифікації, валідації самодіагностовних платформ і ПТК ІКС критичного використання, які будуються на їх основі. Предсавлено перелік програмно-апаратних засобів, які підтримують зазначені процеси. Представлено інформацію, що результати досліджень впроваджено у виробництво, як частину існуючої системи менеджмента якості підприємств, які виконують розробку, тестування, впровадження та супроводження в експлуатації ПТК ІКС критичного використання.

Достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації

Достовірність результатів дослідження, наведених в дисертаційній роботі, висновки і рекомендації щодо їх використання, підтверджуються обгрунтованістю сформульованих припущень, які походять з досвіду проектування та експлуатації ПТК ІКС критичного використання, використанням експериментальних даних відомих фірм про відмови пристроїв та їх елементної бази, збігом результатів експериментальних досліджень та теоретичних результатів, фактами практичного використання отриманих результатів.

Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

Нові наукові результати дисертації відображені у наступних пункутах.

1. Уперше розроблено метод оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю, який на відміну від відомих враховує різні сценарії зміни параметрів потоків відмов і відновлень програмних, програмовних і апаратних засобів, що забезпечує підвищення точності розрахунку функції готовності та імовірності відмов за загальною причиною.

2. Уперше розроблено моделі оцінювання готовності та функційної безпечності програмно-технічних комплексів на самодіагностовних платформах, які на відміну від відомих враховують помилки контролю та

змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функційної безпечності, можливість обґрунтування вимог до засобів контролю й діагностування та формування рекомендацій щодо їх виконання.

3. Уперше розроблено методи верифікації і валідації програмовних платформ і програмно-технічних комплексів на їх основі, які на відміну від відомих, базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов та ін'єктування фізичних і проєктних дефектів, що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності за рахунок збільшення імовірності виявлення прихованих дефектів.

4. Уперше розроблено метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах, який на відміну від відомих ураховує фізичні та проєктні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3.

5. Удосконалено ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та аналізу різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання кількісних показників.

6. Набула подальшого розвитку методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушень внаслідок проєктних і фізичних дефектів і дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і повне виконання вимог до відповідних показників.

7. Набув подальшого розвитку метод забезпечення функційної безпечності програмно-технічних комплексів на самодіагностовних програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною.

Повнота викладення наукових положень, висновків і рекомендацій, сформульованих у дисертації, в опублікованих працях

Усі основні результати дисертаційної роботи досить повно відображені у 68 друкованих працях, до складу яких входять: 5 монографій; 2 навчальних посібника; настанова Національного космічного агентства України; 25 статей у наукових фахових виданнях України та інших держав, з яких 3 індексовано у науково-метричній базі Scopus, отримано свідоцтво про реєстрацію авторського права на твір. Положення дисертації доповідались на 30 науково-технічних конференціях і семінарах державного та міжнародного рівней, відповідно опубліковано 30 тез доповідей в збірниках матеріалів конференцій, з яких 12 індексовано у науково-метричній базі Scopus.

Практичне значення наукових положень, висновків і рекомендацій, сформульованих у дисертації

Практичне значення одержаних результатів полягає в тому, що розроблені моделі та методи доведено до прикладних інженерних методик та процедур, рекомендацій щодо побудови архітектур ПТК, використанням інструментальних засобів оцінювання, програмно-апаратних засобів забезпечення надійності та функційної безпечності ПТК в організаціях, які займаються розробленням, виробництвом, модернізацією та експлуатацією інформаційно-керуючих систем, важливих для безпеки. Це дозволило покращити показники надійності і функційної безпечності ПТК ІКС, які використовуються у атомній енергетиці, авіаційних системах та інших критичних системах.

Результати досліджень впроваджено на наступних підприємствах:

1. Публічному акціонерному товаристві «Науково-виробниче підприємство «Радій» (м. Кропивницький) при оцінюванні надійності і функційної безпечності перспективної цифрової інформаційно-управляючої платформи RadICS в процесі її SIL-3 сертифікації на відповідність вимогам стандарту IEC 61508.
2. Товаристві з обмеженою відповідальністю «Науково-виробниче підприємство «Радікс» в ході розроблення процедур і інструкцій системи менеджменту якості підприємства і виконанні низки проєктів (I&C Test Platform for Electricite de France, Франція; I&C system of IEA-R1 Research

Reactor Control Console and Nuclear Channels Modernization, Бразилія; Embalse Refurbishment, MCR and SCA Window Annunciators, Аргентина).

3. Державному науково-виробничому підприємстві «Об'єднання «Комунар» СКБ «Полісвіт» при розробленні бортових інформаційно-керуючих систем для літаків АН-70, АН-148, що підвищило значення показників надійності і функційної безпечності з урахуванням різних типів дефектів і відмов програмно-апаратних засобів, ПЛІС і засобів контролю і самодіагностування.

4. Державному підприємстві «Державний науково-технічний центр з ядерної та радіаційної безпеки» в процесі розроблення проєктів нормативних документів і методик оцінювання відповідності ІКС АЕС вимогам стандартів, що надало змогу покращити повноту оцінювання і якість відповідних документів.

5. Приватному підприємстві ЛітСофт в ході розроблення технології модельної розробки і тестування апаратного забезпечення (програмовних плат, чіпів, систем електроніки) з використанням комбінації методів машинного навчання та алгебраїчного підходу , що дозволяє звільнитись від суб'єктивності синтезу тестових наборів, підвищити ефективність тестування і відповідно рівень надійності і функційної безпечності.

6. Національному аерокосмічному університеті ім. М.Є. Жуковського «ХАІ» при виконанні 5 науково-дослідних робіт в рамках держбюджетних науково-дослідних робіт МОН України: «Розробка науково-методичних основ й інформаційних технологій оцінки і забезпечення відмовостійкості та безпеки комп'ютеризованих систем аерокосмічних комплексів, інших комплексів критичного застосування» (№Г503-42/2003, №104U003502, 2003-2004); «Теоретичні основи, методи та інструментальні засоби аналізу, розробки та верифікації гарантоздатних інформаційно-управляючих систем для аерокосмічних об'єктів і комплексів критичного застосування» (ДР № №0106U001071, 2006-2008); «Теоретичні основи, методи та технології забезпечення гарантоздатності еволюціонуючих комп'ютеризованих інфраструктур для аерокосмічних і критичних об'єктів» (ДР№0108U010994, 2009-2011); «Теоретичні основи, методи та інформаційні технології розробки програмно-технічних комплексів критичного застосування в умовах ресурсних обмежень» (ДР№ 0112U001058, 2012-2014); Наукові основи, методи і засоби зеленого комп'ютингу і комунікацій (ДР№0115U000996, 2015-2017), при виконанні міжнародних проєктів за програмою Європейського Союзу: «MASTAC» (Msc and PhD Studies in Aerospace Critical Computing , 2006-2009 pp); «SAFEGUARD» (National Safeware Engineering Network of Centres of Innovative Academia-Industry

Handshaking , 2010-2013 pp); SEREIN» (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains , 2013-2016 pp), а також в навчальному процесі для розроблення навчального контенту навчальних дисциплін: «Технології забезпечення якості ПТК»; «Технології проєктування програмних систем»; «Теорія ризиків та технології управління безпекою ІКС»; «Технології розроблення та забезпечення функційної безпеки ІУС».

Зауваження щодо змісту дисертації

1. В ході аналізу існуючого науково-методичного апарату оцінювання та забезпечення надійності і функційної безпечності автор стверджує, що дослідниками активно використовуються методи теорії дослідження операцій, зокрема метод статистичних випробувань Монте-Карло. На використанні цього методу базується розробка імітаційних моделей оцінки надійності систем за умови, коли розробка аналітичних моделей неможлива (наприклад, унеможливлено отримання ймовірнісних параметрів надійністної поведінки систем – ймовірностей переходу систем з одного стану в інші). Було б доцільним доповнити роботу такими дослідженнями з порівнянням їх результатів із наведеними.

2. Автором доведено, що незважаючи на значний прогрес розвитку теорії надійності програмного забезпечення практичне застосування МНПЗ обмежується великою кількістю факторів, зокрема: значним обмеженням статистичного матеріалу, щодо результатів функціонування програмного забезпечення (статистика прояву дефектів та інше). За умови виконання автором тестування ПЗ було б доцільним навести розширену статистику дефектів ПЗ, за етапами тестування.

3. Автором обрано базовим математичним апаратом марковський аналіз. Було б доцільно доповнити роботу з урахуванням обмежень використання марковського аналізу, а саме розмірності, розрідженості та жорсткості матриці коефіцієнтів диференційних рівнянь.

4. Автором зроблено висновок, що стандарт IEC 61508 має певну кількість недоліків: неточних визначень, методологічних невизначеностей або некоректних рекомендацій, що потребує розроблення рекомендацій щодо вдосконалення нормативної бази. Було б доцільним більш чітко і точно сформулювати рекомендації щодо вдосконалення стандартів, як частини отриманих в роботі результатів.

Вказані зауваження не впливають на загальну позитивну оцінку дисертаційної роботи, її наукову цінність та практичну значимість.

Загальний висновок

Дисертаційна робота Одарущенка Олега Миколайовича є завершеною науково-дослідницькою працею, в якій отримано нові науково-обгрунтовані результати, що в сукупності вирішують важливу та актуальну прикладну проблему комплексного оцінювання і забезпечення надійності, функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування в процесі розроблення, верифікації, валідації та використання за призначенням з урахуванням відмов, обумовлених проєктними, фізичними дефектами і вразливостями програмних і апаратних засобів (включаючи відмови з загальних причин), а також зміни параметрів потоків їх відмов і відновлень.

Дисертація відповідає вимогам «Порядку присудження наукових ступенів» (постанова Кабінету Міністрів України від 24 липня 2013 року № 567 зі змінами, внесеними згідно з Постановою Кабінету Міністрів №656 від 19 серпня 2015 року та №1159 від 30 грудня 2015 року), та вимогам до оформлення дисертації (Наказом Міністерства освіти і науки України від 12.01.2017 №40), а її автор, Одарущенко О.М., заслуговує присудження йому наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент

професор кафедри автоматизації
проектування обчислювальної техніки
Харківського національного університету
радіоелектроніки,
доктор технічних наук, професор _____ Г.Ф.Кривуля
«21» 04 2021р.

Підпис проф. Кривулі Г.Ф. підтверджую
Учений секретар ХНУРЕ _____ І.В. Магдаліна