ВІДГУК

офіційного опонента Опанасенка Володимира Миколайовича на дисертаційну роботу Одарущенка Олега Миколайовича 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. До складу сучасних технічних комплексів критичного застосування входять інформаційно-керуючі системи, які безпосередньо впливають на їх безпеку та надійність. В свою чергу, важливою складовою ІКС є їх програмно-технічні комплекси (ПТК). Порушення функцій, які виконують ПКТ ІКС, може привести до порушення безпечного стану критичних та бізнес-критичних об'єктів. Основними властивостями ПТК ІКС критичного застосування є надійність та функціональна безпечність. Постійне збільшення обсягу вже існуючих програмно-апаратних рішень і відповідно збільшення причин порушення працездатності, призводить до необхідності розроблення та застосування та протязі життєвого циклу систем спеціальних та взаємозв'язаних процедур розробки, верифікації та валідації. Ця тенденція повною мірою характерна для ПТК ІКС систем безпеки АЕС.

Тому, зроблений автором висновок про існування протиріччя, яке полягає у невідповідності між розширенням множини причин порушення працездатності програмно-технічних комплексів інформаційно-керуючих систем атомних станцій та інших індустріальних об'єктів критичного застосування внаслідок фізичних і проєктних дефектів їх апаратних, програмних і програмовних компонентів, зміною параметрів потоків їх відмов і відновлень, з одного боку, і рівнем розвитку концептуальних засад, сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпечності, які не враховують повну множину причин і характеристик відмов і порушень ПТК, – з іншого боку, є обґрунтованим. Подолати це протиріччя автор дисертації пропонує шляхом вирішення актуальної науково-прикладної проблеми комплексного оцінювання і забезпечення надійності і 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

уразливостями програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень.

Тому дисертаційна робота Одарущенка О.М., метою якої є розвиток методологічних основ, розроблення методів і засобів оцінювання та забезпечення надійності та функційної безпечності програмно-технічних комплексів на різних етапах життєвого циклу з урахуванням відмов, обумовлених фізичними та проєктними дефектами і вразливостями, а також їх практичне впровадження в інформаційно-керуючих системах критичного застосування для зниження ризиків небезпечних відмов є актуальною.

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

У першому розділі 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 ІКС критичного використання. Визначена вартість наслідків відмов ПТК ІКС критичного використання, що обґрунтовує важливість і актуальність проведення досліджень. 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 математичних методів оцінювання і забезпечення надійності і функційної безпечності систем досліджуваного класу. Визначено протиріччя та сформульовано науково-прикладну проблему.

У другому розділі розроблена методологія оцінювання і забезпечення надійності і функційної безпечності ПТК ІКС критичного застосування, яка є першим науковим результатом. Методологія оцінювання і забезпечення надійності та функційної безпечності ПТК ІКС критичного застосування базується на використанні системи принципів, об'єднаних загальною концепцією і покладених в основу розроблених в дисертації моделей і методів. Важливо, що базові ідеї досліджень грунтуються на парадигмі фон Неймана створення надійної системи із ненадійних елементів, яка розвивається стосовно ПТК ІКС критичного застосування шляхом їх комплексного оцінювання і забезпечення надійності і функційної безпечності.

Третій розділ присвячено розробленню моделей оцінювання надійності програмних засобів (МНПЗ) (англ. SRGM Software Reliability Growth Models). Автором, спираючись на досвід 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. Обґрунтовано, що процеси внесення-усунення вторинних дефектів мають значний вплив на кількісні значення надійнісних параметрів ПЗ. Тому постало завдання вибору типу SRGM. Для цього було виконано аналіз SRGM різних класифікаційних ознак (емпірічних, статистичних, ймовірнісних), 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 SRGM: Джелінського-Моранди; Муси; простої експоненційної; Шика-Уолвертона, які стали другим науковим результатом.

Четвертий розділ присвячено розробленню моделей та методу оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю, який є третім науковим результатом. Використовуючи розроблений метод вдалося виконати дослідження надійності базових архітектур ПТК і побудувати їх пріоритетні ряди, які є рекомендаціями розробникам систем.

У п'ятому розділу розроблено моделі оцінювання готовності та функційної безпечності ПТК на самодіагностованих платформах (СДПП). Розглянуто СДПП на програмовних логічних інтегральних схемах (ПЛІС), як такі, що найбільш ефективним засобом реалізують функції захисту, блокування, управління та регулювання. Автором обґрунтовано, що використання ПЛІС для ПТК ІКС критичного використання дозволяє на етапі проєктування закласти алгоритми самодіагностування, які виконуються окремою функціональною підсистемою, яка називається системою контролю і діагностики (СКД). Дослідження розроблених багатофрагментних марковських моделей дозволяє сформулювати рекомендації розробникам систем щодо необхідного рівня програмно-апаратного контроля та діагностування.

Шостий розділ присвячено методам верифікації та валідації програмовних платформ і ПТК побудованих на їх основі, а також методу забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах, який став основним об'єднуючим попередні дослідження результатом. Важливим є те, що в цілому, одержані результати дозволяють забезпечити необхідний рівень функційної безпечності (SIL-3) ПТК ІКС за умови застосування V-моделі життєвого циклу згідно вимог стандарту IEC 61508, що підтверджено результатами сертифікації цифрової інформаційно-керуючої платформи RadICS виробництва «Науково-виробничого підприємства «Радій» (м. Кропивницький).

Достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації. Достовірність нових наукових положень і висновків дисертаційної роботи підтверджується: збігом з результатами, отриманими з використанням відомих моделей і методів теорії надійності технічних систем та теорії надійності програмного забезпечення; обґрунтованістю припущень, прийнятих при розробленні моделей і методів оцінювання надійності та функційної безпечності, виходячи з досвіду експлуатації ПТК ІКС; результатами практичного використання розроблених моделей, методів та інструментальних засобів в ході створення, сертифікації та експлуатації ПТК ІКС критичного застосування на програмовних платформах.

Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації.

До нових результатів, одержаних у дисертаційної роботі, можуть бути віднесені:

- 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; 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; 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; 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 проектні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3;

- 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;

- набули 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 проектних 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; метод забезпечення функційної безпечності програмно-технічних комплексів на 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. Одержані нові наукові результати доведено до прикладних інженерних методик, які є частиною систем менеджмента якості підприємств що спеціалізується на розроблені, впроваджені, супроводженні в експлуатації ПТК ІКС критичного застосування.

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. Загалом позитивно оцінюючи дане дослідження, слід зазначити, що окремі його положення потребують додаткової аргументації, або викликають певні зауваження та побажання.

1. В роботі запропоновано модель «система-фізичне та інформаційне середовище», яка базується на понятті, що розширює поняття технічного стану системи до інформаційно-технічного і дозволяє розробляти моделі інформаційно-технічного стану (ІТС). Інформаційно-технічний стан враховує властивості і ознаки як технічного, так і інформаційного характеру, притаманних системі в певний момент часу. Модель ІТС дозволяє розробляти моделі оцінювання надійності і забезпечення функційної безпечності ПТК з урахуванням впливу зовнішніх і внутрішніх інформаційно-технічних факторів, розширеного простору станів. В цілому в роботі йде мова про функційну безпечність. Робота значно виграла за умови наведення інформації, як підвищення і забезпечення функційної безпечності систем досліджуваного класу впливає на інформаційну безпечність.

2. Автором розроблено комплекс багатофрагментних макромоделей і багатофрагментних марковських моделей оцінювання надійності ПТК із різними архітектурами. Аналіз цих моделей доводе, що за умови урахування змінності параметрів розмірність обчислювальної задачі значно зростає. Виникає питання, чи існують умови адаптивного оцінювання (досягнення системою рівня надійності, що вимагається) і відповідно до цього зменшення розмірності обчислювальної задачі?

3. В роботі наведено методи верифікації і валідації ПТК, зокрема методи із внесенням дефектів в програмні і апаратні компоненти. Не досить зрозуміло, яким чином досягається достатній рівень тестового покриття в ході реалізації цих методів?

Загальний висновок по дисертаційній роботі. Дисертаційна робота Одарущенка Олега Миколайовича є завершеною науково-дослідницькою працею, в якій отримано нові науково-обгрунтовані результати, що в сукупності розв'язують важливу та актуальну науково-прикладну проблему комплексного оцінювання і забезпечення надійності і 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 загальної причини), 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

Провідний науковий співробітник
відділу мікропроцесорної техніки
Інституту кібернетики
ім. В.М. Глушкова НАН України
доктор технічних наук, професор _____ В.М. Опанасенко