НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
ім. М.Є. ЖУКОВСЬКОГО «ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ
В.Н. КАРАЗІНА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Одарущенко Олег Миколайович
(прізвище, ім'я, по батькові)

УДК 004.05,004.415.5
(індекс)

ДИСЕРТАЦІЯ

МЕТОДИ І ЗАСОБИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ З УРАХУВАННЯМ ФІЗИЧНИХ І ПРОЄКТНИХ ДЕФЕКТІВ КОМПОНЕНТІВ

(назва дисертації)

05.13.05 – Комп'ютерні системи та компоненти
(шифр і назва спеціальності)

Технічні науки
(галузь знань)

Подається на здобуття наукового
ступеня доктора технічних наук

Дисертація містить результати власних проваджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

О.М. Одарущенко
(підпис, ініціали та прізвище здобувача)

Науковий консультант
Харченко Вячеслав Сергійович, заслужений винахідник України,
доктор технічних наук, професор

Харків – 2021

АНОТАЦІЯ

Одарущенко О.М. Методи і засоби забезпечення надійності та функційної безпечності програмно-технічних комплексів з урахуванням фізичних і проєктних дефектів компонентів.- Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти.- Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харківський національний університет імені В.Н. Каразіна Міністерства освіти і науки України, Харків, 2021.

Безпека АЕС, авіаційних і ракетно-космічних комплексів інших критичних об'єктів в значній мірі залежить від інформаційно-керуючих системи (ІКС), ядром яких є програмно-технічні комплекси (ПТК). Вартість відмов апаратних, програмних, програмовних і комунікаційних (мережних) засобів ПТК ІКС АЕС, є надзвичайно високою. Найважливішою властивістю ІКС є функційна безпечність (ФБ), яка відповідно до міжнародних і національних стандартів (IEC 61508, IEC 26262) визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та/або його наслідки. Сучасні процеси модернізації існуючих та розробки перспективних ПТК ІКС ґрунтуються на використанні нової елементної бази, сучасних технологіях розробки їх апаратної (АК) та програмної компонент (ПК). Це, з одного боку, розширює можливості ПТК ІКС, приводить до підвищення ефективності технологічних процесів, знижує ресурсємність виробництва, а з іншого боку – до зростання ризиків підвищення залежності функціональності, надійності і безпеки від якості проєктних рішень. Тобто збільшення можливостей сучасної елементної бази, впровадження індустріальних технологій розробки програмного забезпечення (ПЗ) не привело до такого ж прогресу у проєктуванні ПТК з необхідним і гарантованим рівнем надійності і безпеки. Сучасні ПТК ІКС критичного застосування (КЗ) зберігають набір «дефіцитів безпеки», які визначаються: недостатнім рівнем надійності і ФБ

(НіФБ) технічних засобів і ПЗ; недостатнім рівнем діагностики АК та ПК; неповним задоволенням вимог до сейсмостійкості; різноманітністю елементної бази та технічних рішень для різних ПТК.

В ході виконання аналітичних досліджень предметної галузі було встановлено, що не зважаючи на інтенсивні дослідження за обраною тематикою впродовж останніх десятиліть, за напрямами: розвитку теоретичних засад, загальних методів оцінювання та підвищення надійності та функційної безпечності (A. Avizienis, J.-C. Laprie, G. Johnson, B. Randell, E. Zaitseva, Б.Ю. Волочий, Б.М. Конорєв, В.С. Харченко, М.О. Ястребенецький та інші); розроблення методів і засобів оцінювання та забезпечення надійності програмного забезпечення для різних застосунків (B. Littlewood, P. Popov, A. Romanovsky, S. Russo, L. Strigini, J. Vain, В.В. Ліпаєв, Д.А. Маєвський, В.С. Яковина та інші); розроблення й дослідження моделей та методів діагностування і забезпечення стійкості інформаційно-керуючих систем і ПТК до фізичних та проєктних дефектів (T. Anderson, F. Saglietti, K. Trivedi, О.В. Дрозд, В.А. Краснобаєв, Г.Ф. Кривуля, В.М. Опанасенко, О.М. Романкевич, В.О. Романкевич, В.В. Скляр, В.І. Хаханов та інші), залишається низка нерозв’язаних задач і обмежень існуючих методів і засобів оцінювання та забезпечення необхідного рівня властивостей, а саме: моделі, які описують надійнісну і безпекову (як інформаційну так і функціональну) складові, не ураховують реальну розмірність задач оцінювання з огляду на складність індустріальних ІКС та їх ПТК; змінність параметрів відмов і відновлень; у методах оцінювання НіФБ, насамперед, аспекти безвідмовності АЗ і ПЗ розглядаються відокремлено, без спільного комплексного кількісного аналізу; методи розроблення й забезпечення відмовостійкості ПТК з використанням програмовних платформ недостатньо ураховують можливості, обмеження і похибки вбудованих засобів контролю і діагностування (КД) на рівні електронних проєктів, модулів і каналів тощо.

У першому розділі проведено аналіз методів і засобів оцінювання та забезпечення НіФБ ПТК ІКС критичного використання. Проведено аналіз

факторів впливу різної природи на НіФБ ІКС критичного використання. Визначена вартість наслідків відмов ПТК ІКС критичного використання. Систематизовано вимоги державних та міжнародних стандартів до НіФБ ПТК та вимоги до організації процесів розробки, верифікації та валідації для забезпечення виконання цих вимог. Встановлено, що існуючі стандарти не дають рекомендацій щодо комплексного оцінювання систем з урахуванням того, що сучасні обчислювальні системи інтегрують апаратні і програмні засоби, які в ході роботи мають взаємний вплив. На прикладі базового стандарту IEC 61508 доведено, що стандарти не вільні великої кількості недоліків. Виконано аналіз основних тенденцій розвитку ІКС КЗ. За результатами аналізу встановлено, що сучасні тенденції розвитку ІКС КЗ забезпечують підвищення кількості функцій що автоматизуються, зростає рівень автоматизації технологічних процесів з одного боку. З іншого боку впровадження нових цифрових та інформаційних технологій породжує нові ризики, які впливають на безпеку систем та відповідно стають актуальними завдання розроблення і впровадження методів, технік та програмно-апаратних засобів розроблення, верифікації і валідації компонент та в цілому ІКС КЗ. Виконано огляд методів і засобів оцінювання НіФБ ІКС КЗ, 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.

Другий розділ присвячено розробці методології оцінювання і забезпечення НіФБ ПТК ІКС КЗ. Методологія базується на використанні системи принципів, об'єднаних загальною концепцією і покладених в основу розроблених в дисертації моделей і методів. Базові ідеї досліджень грунтуються на парадигмі фон Неймана створення надійної системи із ненадійних елементів, яка розвивається стосовно ПТК ІКС КЗ шляхом їх комплексного оцінювання і забезпечення надійності і функційної безпечності. Комплексність базується, по-перше, на розширенні поняття технічного стану системи до інформаційно-технічного стану (ІТС), по-

друге, на врахуванні множин: компонентів; дефектів; відмов; властивостей (атрибутів безпеки, готовності). Дано опис властивостей операцій перетворення станів моделі ІТС, а саме: асоціативності; комутативності; транзитивності і дистрибутивності. Це дало змогу дослідити можливості взаємних впливів різної природи на систему, деталізувати множини станів системи.

Третій розділ присвячено розробленню моделей надійності програмних засобів (МНПЗ). Удосконалено МНПЗ шляхом урахування вторинних дефектів (ВД), які вносяться за результатами тестування, рефакторінгу і супроводу, та аналізу різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання кількісних показників. Модифікація МНПЗ Муси дозволила зняти одне з основних припущень про не змінність параметрів моделювання систем та реалізувати встановлений принцип визначення змінних параметрів відмов за різними ознаками і відновлень компонентів і систем за рахунок впровадження ідеї про умовну апроксимацію функцій, що описують параметри моделі, наприклад $\lambda(t)$ – інтенсивність прояву дефекту або $\mu(t)$ – інтенсивність відновлення після прояву, кусково-неперервною функцією. При цьому після зміни станів системи (моделі) відбувається стрибкоподібна зміна величин інтенсивностей λ або μ на певні значення $\Delta\lambda$ або $\Delta\mu$. Результатом аналізу досвіду розроблення, рефакторінга, тестування програмних проєктів та встановлених фактів внесення ВД стало розроблення переліку можливих сценаріїв внесення та усунення ВД ПЗ. Дана множина сценаріїв дає можливість виконати уточнення поведінки ПЗ в умовах відповідного сценарію за рахунок перебору співвідношень параметрів. Одержано модифіковані функції ризиків обраних МНПЗ, а саме: Джелінського-Моранди; простої експоненційної; Шика-Уолвертона; моделі Муси, моделі Ліпова, які враховують можливість внесення ВД ПЗ і дозволяють одержувати оцінки інтенсивності прояву ДППЗ з урахуванням означеного фактору. Запропонована послідовність прогнозування кількості ВД об’єднала попередні результати і дозволяє отримувати оцінку кількості вторинних дефектів та уточнювати параметри ПЗ, зокрема інтенсивність прояву ДППЗ. Порівняння

результатів обчислення інтенсивності прояву ДППЗ дає висновок про те, що значення означеного параметру уточнюється до 5%.

В четвертому розділі розроблено метод оцінювання НіФБ ПТК 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. В основу метода покладено наступне: принципи розроблення багатофрагментних марковських моделей (БММ), які відображають основну ідею про доцільність оцінювання показників надійності і функційної безпечності із урахуванням зміни параметрів апаратної і програмної компонент ПТК в часі; систематизація змінних параметрів; модель прояву та усунення ДППЗ; загальна модель прояву дефектів та вразливостей; сценарії зміни параметрів; систематизація БММ. Це дозволило розробити комплекс базових багатофрагментних моделей (ББМ) оцінювання НіФБ ПТК для базових архітектур їх побудови. Систематизація змінних параметрів дозволила окреслити їх перелік на основі аналізу множин дефектів, груп причин виникнення дефектів та визначити множини коефіцієнтів зміни параметрів і перейти до розроблення комбінації змінних і незмінних параметрів, та коєфіцієнтів їх зміни. Це дозволило одержати множину сценаріїв зміни параметрів для подальшого застосування в моделях оцінювання НіФБ ПТК. Множини сценаріїв зміни параметрів дали змогу розробити комплекс макромоделей оцінювання надійності і функційної безпечності ПТК та на їх основі комплекс багатофрагментних марковських моделей (БММ), основними перевагами яких є можливість урахування змінності параметрів програмних та апаратних компонентів у часі, що підвищило точність оцінювання шуканих показників до 5%. Дослідження результатів моделювання із використанням комплексу розроблених БММ дозволили одержати нову інформацію про НіФБ існуючих і перспективних ПТК, що дозволяє формулювати вчасні рекомендації особі, яка приймає рішення. Основними перевагами розробленого метода є

наступні: можливість реалізації комплексного оцінювання надійності та функційної безпечності ПТК, побудови пріоритетних рядів досліджених архітектур; можливість виконання спрямованого пошуку архітектури побудови ПТК з урахуванням множин обраних параметрів та варіантів зміни цих параметрів у часі.

В п’ятому розділі розроблено моделі оцінювання НіФБ ПТК на самодіагностовних програмовних платформах (СПП), які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки НіФБ, можливість обґрунтування вимог до засобів контролю та дыагностування. Дані моделі відображають переваги технології ПЛІС, які за результатами аналізу є найбільш ефективними для реалізації ПТК функцій захисту, блокування, управління й регулювання, що відповідають вимогам державних і міжнародних нормативно-технічних документів з безпеки. Практика довела переваги використання технології ПЛІС, які заключаються в тому, що вона ще на етапі проєктування дозволяє закладати алгоритми самодіагностування. які далі будуть виконуватись окремими підсистемами контролю та діагностування. Дане твердження доведено результатами класифікації підсистем контролю й діагностування перспективної СПП ЦІУП RadICS. Для урахування глибини контроля і діагностування введено показник діагностичного охоплення, який в свою чергу враховує різні види інтенсивностей відмов. Відповідно до видів інтенсивностей відмов модель включає відповідні функційні стани і особливо важливим є те, що модель враховує стан недектованої небезпечної відмови, що підвищує точність оцінювання (прогнозування) НіФБ. Розроблені БММ оцінювання НіФБ ПТК системи нормальної експлуатації (СНЕ) та аварійного і попереджувального захисту (АЗ ПЗ) з урахуванням помилок засобів контролю та діагностування. Дослідження моделей дозволило відстежити характер зміни функції готовності кожного ПТК з урахуванням набору значень параметру діагностичного охоплення. Підтверджено, що забезпечення максимального значення цього параметру є вкрай вагомим для систем важливих

для безпеки і має бути забезпечено на ранніх етапах проєктування системи шляхом розробки й впровадження спеціальних організаційних та технічних заходів. До даних заходів можуть бути віднесені розробка концепції безпеки системи та її архітектурної побудови, а саме розробка структури підсистем контролю та діагностування. Застосування розробленого метода зменшує ризики відмов за загальною причиною за умови того, що оцінці підлягають диверсні архітектури ПТК. Основними перевагами метода є наступні: можливість сформулювати рекомендації щодо структурної (архітектурної) побудови ПТК; отримання більш точних оцінок показників надійності і функційної безпечності. Точність оцінок зростає до 5%.

В шостому розділі розроблено методи верифікації і валідації програмовних платформ і ПТК 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 та набув подальшого розвитку метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на ПЛІС, 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. Модифікація процедури FMEDA базується на аналізі еволюції техніки оцінки надійності FMEA до FMEDA, а також проєктного досвіду використання метода FMEDA. В результаті аналізу було встановлено, існуюча техніка FMEDA має ряд суттєвих недоліків, а саме: вимагає багато рутинної та складної роботи для простих і складних електронних компонент системи; не існують нормативні документи, які описують FMEDA та визначають вимоги до її продуктивності для різних типів систем; не враховується ненадійність, що вноситься програмною компонентою. Здійснена модифікація дозволила автоматизувати найбільш трудомісткі етапи

техніки та за рахунок впровадження FMEA для програмних компонент врахувати ненадійність програмної компоненти. Все це знизило в два рази часові затрати на виконання FMEDA та підвищило точність оцінювання функційної безпечності системи в цілому до 5%. Модифікована процедура FIT є результатом аналізу етапів еволюції атрибутів надійності та функційної безпечності складних систем, а саме простоти (simplicity), здатності до перевірки (checkability), здатності до реконфігурування (reconfigurability), верифікуємості (verifiability) та результатів проєктного впровадження результаів виконання техніки FMEDA (встановлених режимів відмов). Перевірка встановлених режимів відмов базується та техніці FIT, а саме техніці тестування апаратних і програмних компонент із внесенням дефектів в компоненти системи. Як результат виконання цієї техніки встановлено новий атрибут надійності та функційної безпечності, а саме FIT - придатність. Де FIT - придатність - це придатність до ін’єктування дефектів у електричні схеми та окремі компоненти схеми (HW FIT-здатність) або програмного коду (SW FIT-здатність). Модифікована FIT процедура була застосована для SIL-орієнтованого процесу сертифікації ЦІУП RadICS і дозволила виконати тести на ін'єкцію дефектів за результатами FMEA або FMEDA на різному рівні ієрархії системи: (модуль, юніт модуля, електронний проєкт); системний SW, реалізований з кодом HDL (Chip); програми SW -конфігураційні файли, що генеруються інтегрованим середовищем розробки, що сприяло визначенню рівня функційної безпечності системи SIL-3. Метод оцінювання та забезпечення надійності і функційної безпечності ПТК ІКС КЗ акумулює всі попередні наукові результати та їх переваги. Він дозволяє виконувати комплексне оцінювання вказаних властивостей враховуючи: розширення поняття технічного стану системи до ІТС. Метод застосовується на протязі життєвого циклу системи, який описується V-моделлю. Сумарний ефект щодо підвищення точності оцінювання показників досягає 10%. Програмно-апаратні засоби виконання тестування реалізують розроблені теоретичні положення і є частиною впровадженої системи менеджменту якості підприємства, яка визначає умови та послідовність

виконання активностей верифікації та валідації СПП та ПТК ІКС КЗ, які розробляються на їх основі.

Отримані в роботі результати дозволили вирішити 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.

Ключові слова: інформаційні-керуючі системи, програмно-технічні комлекси, надійність та функційна безпечність, апаратні засоби, програмні засоби, множина дефектів, дефект проєктування програмних засобів, моделі надійності програмних засобів, марковський аналіз, багатофрагментні марковські моделі, самодіагностовні програмовні платформи, життєвий цикл, верифікація, валідація.

ABSTRACT

Odarushchenko O.M. Methods and means for ensuring reliability and functional safety of instrumentation and control systems with considering the physical and design defects of the components.- As the manuscript.

Dissertation for the degree of Doctor of Technical Sciences in the specialty of 05.13.05 – Computer Systems and Components. –National Aerospace University “Kharkiv Aviation Institute”, V. N. Karazin Kharkiv National University of the Ministry of Education and Science of Ukraine, Kharkiv, 2021.

The safety of nuclear power plants, aerospace and other critical facilities depends to a large extent on the instrumentation and control systems (I&C). The cost of failures of hardware, software, software and communication (network) facilities of I&C is extremely high. The most important property of I&C is functional safety (FS), which in

accordance with international and national standards (IEC 61508, IEC 26262) determines the ability of systems to minimize the risks of transition to an emergency (dangerous) state and/or its consequences. Modern processes of modernization of existing and development of promising I&C are based on the use of a new element base, modern technologies for the development of their hardware and software components. This, on the one hand, expands the capabilities of I&C, leads to increased efficiency of technological processes, reduces the resource intensity of production, and on the other hand - to increase the risks of increasing the dependence of functionality, reliability and safety on the quality of design solutions. That is, the increase in the capabilities of the modern element base, the introduction of industrial software development technologies (software) has not led to the same progress in the design of I&C with the necessary and guaranteed level of reliability and safety. Modern I&C of critical application retain a set of "safety deficits", which are determined by: insufficient level of reliability and FS of hardware and software; insufficient level of diagnosis of hardware and software; incomplete satisfaction of seismic requirements; variety of element base and technical solutions for different I&C. During the analytical research of the subject area it was found that despite intensive research on selected topics in recent decades, in the areas of: development of theoretical foundations, general methods of evaluation and improving reliability and functional safety (A. Avizienis, J.-C. Laprie , G. Johnson, B. Randell, E. Zaitseva, B.Yu. Volochy, B.M. Konorev, V.S. Kharchenko, M.O. Yastrebenetsky and others); development of methods and tools for evaluating and ensuring the reliability of software for various applications (V. Littlewood, P. Popov, A. Romanovsky, S. Russo, L. Strigini, J. Vain, V.V. Lipayev, D.A. Maevsky, V.S. Yakovina and others); development and research of models and methods for diagnosing and ensuring the stability of information control systems and I&C to physical and design defects (T. Anderson, F. Saglietti, K. Trivedi, O.V. Drozd, V.A. Krasnobaev, G.F. Kryvulya, V.M. Opanasenko, O.M. Romankevich, V.O. Romankevich, V.V. Sklyar, V.I. Khakhanov and others), there are a number of unsolved problems and limitations of existing methods and means of evaluation and provision the required level

of properties, namely: models that describe the reliable and safe (both informational and functional) components, do not take into account the real dimension of the evaluation tasks given the complexity of industrial I&C; variability of failure and recovery parameters; in the Reliability ans FS (RFS) assessment methods, first of all, the aspects of hardware and software reliability are considered separately, without a joint comprehensive quantitative analysis; methods of developing and ensuring the resilience of I&Cs using software platforms do not sufficiently take into account the capabilities, limitations and errors of embedded control and diagnostic tools at the level of electronic projects, modules and channels, etc.

In the first section the analysis of methods and means of estimation and maintenance of RFS of I&C of critical use is carried out. The analysis of factors of influence of different nature on RFS of I&C of critical use is carried out. The cost of consequences of failures of I&C of critical use is determined. The requirements of state and international standards to the RFS of I&C and the requirements for the organization of development, verification and validation processes to ensure compliance with these requirements are systematized. It is established that the existing standards do not provide recommendations for comprehensive evaluation of systems, taking into account the fact that modern computer systems integrate hardware and software, which in the course of work have a mutual influence. On the example of the basic standard IEC 61508 it is proved that the standards are not free from a large number of shortcomings. The analysis of the basic tendencies of development of I&C is executed. According to the results of the analysis, it is established that the current trends in the development of I&C provide an increase in the number of automated functions, increasing the level of automation of technological processes on the one hand. On the other hand, the introduction of new digital and information technologies creates new risks that affect the safety of systems and, accordingly, become relevant tasks of development and implementation of methods, techniques and software and hardware development, verification and validation of components and I&C short circuits in general. The review of methods and means of assessment of RFS of I&C is performed, models and methods

are classified. The analysis of the mathematical apparatus and restrictions of use of existing estimation methods is carried out. Contradictions have been identified and a scientific and applied problem has been formulated. Problems, mathematical apparatus, stages and research methods are substantiated.

The second section is devoted to the development of a methodology for assessing and providing RFS of I&C. The methodology is based on the use of a system of principles united by a general concept and based on the models and methods developed in the dissertation. The basic ideas of the research are based on von Neumann's paradigm of creating a reliable system of unreliable elements, which is being developed in relation to the RFS of I&C by their comprehensive assessment and ensuring reliability and functional safety. Complexity is based, firstly, on the expansion of the concept of technical condition of the system to information and technical condition (ITS), and secondly, on the consideration of sets: components; defects; failures; properties (security attributes, readiness). A description of the properties of state transformation operations of the ITS model is given, namely: associativity; commutativity; transitivity and distributivity. This made it possible to explore the possibilities of mutual influences of different nature on the system, to detail the many states of the system.

The third section is devoted to the development of software reliability growth models (SRGM). Improved SRGM by taking into account secondary defects, which are introduced as a result of testing, refactoring and maintenance, and analysis of different scenarios of their introduction, which provides increased accuracy in estimating quantitative indicators. Modification of SRGM refineries allowed to remove one of the main assumptions about the invariance of system modeling parameters and to implement the established principle of determining variable failure parameters on various grounds and recovery of components and systems by introducing the idea of conditional approximation of functions describing model parameters, eg λ (t) – failure rate or μ (t) - recovery rate, piecewise continuous function. In this case, after changing the states of the system (model) there is an abrupt change in the values of failure rate or

recovery rate to certain values of $\Delta\lambda$ or $\Delta\mu$. The result of the analysis of the experience of development, refactoring, testing of software projects and the established facts of secondary defects introduction was the development of a list of possible scenarios of introduction and elimination of software secondary defects. This set of scenarios makes it possible to refine the behavior of the software in the corresponding scenario by searching the ratios of the parameters. Modified risk functions of selected SRGM were obtained, namely: Dzhelinsky-Moranda; simple exponential; Chic-Wolverton; Musa models, Lipov models, which take into account the possibility of making software secondary defects and allow to obtain estimates of the failure rate of SRGM taking into account the specified factor. The proposed sequence of predicting the number of secondary defects combined the previous results and allows to obtain an estimate of the number of secondary defects and to clarify the parameters of the software, in particular the failure rate. Comparison of the results of calculating the failure rate gives the conclusion that the estimation accuracy increases to 5%.

In the fourth section, a method for estimating RFS of I&C with structural-version redundancy is developed, which, unlike the known ones, takes into account different scenarios of changes in failure flow parameters and software, software and hardware upgrades, which provides accuracy of calculation of readiness function and failure probability for common cause. The method is based on the following: principles of development of multi-fragment Markov models (MMM), which reflect the basic idea of the feasibility of assessing the reliability and functional safety, taking into account changes in the parameters of hardware and software components of I&C over time; systematization of variable parameters; model of manifestation and elimination of failure rate; general model of defects and vulnerabilities; parameter change scenarios; systematization of MMM. This allowed to develop a set of basic multi-fragment models (BMM) of RFS of I&C estimation for basic architectures of their construction. Systematization of variable parameters allowed to outline their list based on the analysis of sets of defects, groups of causes of defects and determine the sets of coefficients of change of parameters and proceed to the development of a combination of variable and

invariant parameters and coefficients of their change. This allowed to obtain a set of scenarios for changing the parameters for further application in the models of RFS assessment of I&C. Many scenarios of parameter changes allowed to develop a set of macromodels for assessing the reliability and functional safety of I&C and based on a set of multi-fragment Markov models, the main advantages of which are the ability to take into account the variability of software and hardware components over time. Investigation of simulation results using a set of developed BMM allowed to obtain new information about the RFS of existing and prospective I&C, which allows to formulate timely recommendations to the decision maker. The main advantages of the developed method are the following: the possibility of implementing a comprehensive assessment of the reliability and functional safety of I&C, the construction of priority series of studied architectures; the ability to perform a directed search of the architecture of I&C construction, taking into account the sets of selected parameters and options for changing these parameters over time.

The fifth section develops models for assessing the RFS of I&C on self-diagnostic software platforms, which, in contrast to the known ones, take into account control errors and variability of system parameters, which increases the accuracy of RFS assessment, the ability to justify requirements. These models reflect the advantages of FPGA technology, which according to the analysis are the most effective for the implementation of software and hardware complexes of protection, blocking, control and regulation functions that meet the requirements of state and international safety regulations. Practice has proven the advantages of using FPGA technology, which are that it allows you to lay the algorithms for self-diagnosis at the design stage. which will then be performed by separate subsystems of control and diagnosis. This statement is proved by the results of classification of subsystems of control and diagnostics of perspective NGN CIUP RadICS. To take into account the depth of control and diagnosis, an indicator of diagnostic coverage was introduced, which in turn takes into account different types of failure rates. According to the types of failure intensities, the model includes the corresponding functional states and it is especially important that the

model takes into account the state of undetected dangerous failure, which increases the accuracy of estimation (forecasting) of the NSF. BMM evaluations of NIF PTC systems of normal operation (SNE) and emergency and warning protection (AZ PZ) are developed taking into account errors of means of control and diagnostics. The study of the models allowed us to track the nature of the change in the readiness function of each PTC, taking into account the set of values of the parameter of diagnostic coverage. It is confirmed that ensuring the maximum value of this parameter is extremely important for systems important for security and should be ensured in the early stages of system design through the development and implementation of special organizational and technical measures. These measures may include the development of the concept of system security and its architectural construction, namely the development of the structure of control and diagnostic subsystems. The application of the developed method reduces the risks of failure for a common cause, provided that the subversive architectures of PTC are subject to evaluation. The main advantages of the method are the following: the ability to formulate recommendations for structural (architectural) construction of PTC; obtaining more accurate estimates of reliability and functional safety. The accuracy of estimates increases to 5%.

The fifth section develops models for assessing the RFS of I&C on self-diagnostic software platforms, which, in contrast to the known ones, take into account control errors and variability of system parameters, which increases the accuracy of RFS assessment, the ability to justify requirements. These models reflect the advantages of FPGA technology, which according to the analysis are the most effective for the implementation of software and hardware complexes of protection, blocking, control and regulation functions that meet the requirements of state and international safety regulations. Practice has proven the advantages of using FPGA technology, which are that it allows you to lay the algorithms for self-diagnosis at the design stage, which will then be performed by separate subsystems of control and diagnosis. This statement is proved by the results of classification of subsystems of control and diagnostics of perspective RadICS Platform. To take into account the depth of control and diagnosis,

an indicator of diagnostic coverage was introduced, which in turn takes into account different types of failure rates. According to the types of failure i rates, the model includes the corresponding functional states and it is especially important that the model takes into account the state of undetected dangerous failure, which increases the accuracy of estimation (forecasting) of the RSF. BMM evaluations of RSF of I&C systems of normal operation and emergency and warning protection are developed taking into account errors of means of control and diagnostics. The invastigation of the models allowed us to track the nature of the change in the readiness function of each I&C, taking into account the set of values of the parameter of diagnostic coverage. It is confirmed that ensuring the maximum value of this parameter is extremely important for systems important for security and should be ensured in the early stages of system design through the development and implementation of special organizational and technical measures. These measures may include the development of the concept of system security and its architectural construction, namely the development of the structure of control and diagnostic subsystems. The application of the developed method reduces the risks of failure for a common cause, provided that the subversive architectures of I&C are subject to evaluation. The main advantages of the method are the following: the ability to formulate recommendations for structural (architectural) construction of The application of the developed method reduces the risks of failure for a common cause, provided that the subversive architectures of I&C are subject to evaluation. The main advantages of the method are the following: the ability to formulate recommendations for structural (architectural) construction of I&C; obtaining more accurate estimates of reliability and functional safety. The accuracy of estimates increases to 5%.

The sixth section develops methods for verification and validation of software platforms and I&C based on them, which, unlike the known ones, are based on a combination of procedures for analysis of types, consequences and criticality of failures and injection of physical and design defects. Functional safety by increasing the probability of detection of hidden defects and further development of the method of

assessing and ensuring functional safety in the development and licensing of modules and platforms for information and control systems at FPGA, which in contrast to the known takes into account physical and design defects and failure parameters and restorations, and ensures compliance with the requirements of international standards to the level of functional safety of SIL3. The modification of the FMEDA procedure is based on the analysis of the evolution of the FMEA reliability assessment technique to FMEDA, as well as the design experience of using the FMEDA method. As a result of the analysis, it was found that the existing FMEDA technique has a number of significant disadvantages, namely: it requires a lot of routine and complex work for simple and complex electronic components of the system; there are no regulations that describe FMEDA and define its performance requirements for different types of systems; the unreliability introduced by the software component is not taken into account. The implemented modification allowed to automate the most time-consuming stages of technology and due to the introduction of FMEA for software components to take into account the unreliability of the software component. All this has halved the time spent on FMEDA and increased the accuracy of assessing the functional safety of the system as a whole to 5%. The modified FIT procedure is the result of the analysis of the stages of evolution of the attributes of reliability and functional safety of complex systems, namely simplicity, checkability, reconfigurability, verifiability and the results of project implementation of FMEDA results. Verification of established failure modes is based on the FIT technique, namely the technique of testing hardware and software components with the introduction of defects in system components. As a result of this technique, a new attribute of reliability and functional safety has been established, namely FIT - suitability. Where FIT suitability is the suitability for injecting defects into electrical circuits and individual circuit components (HW FIT capability) or program code (SW FIT capability). The modified FIT procedure was used for the SIL-oriented certification process of RadICS Platform and allowed to perform tests for injection of defects according to the results of FMEA or FMEDA at different levels of the system hierarchy: (module, unit, electronic project); implemented with HDL code (Chip);

programs SW - configuration files generated by the integrated development environment, which helped to determine the level of functional security of the SIL-3 system. The method of assessing and ensuring the reliability and functional safety of I&C accumulates all previous scientific results and their benefits. It allows you to perform a comprehensive assessment of these properties, taking into account: the expansion of the concept of technical condition of the system to ITS. The method is applied during the life cycle of the system, which is described by the V-model. The total effect of improving the accuracy of indicators reaches 10%. Software and hardware tools for testing implement the developed theoretical provisions and are part of the implemented quality management system of the enterprise, which determines the conditions and sequence of verification and validation of I&C, which are developed on their basis.

The results obtained in this work allowed to solve the scientific and applied problem of complex assessment and ensure the reliability and functional security of software and hardware systems of information and control systems of critical application in the development, verification, validation and intended use, taking into account failures due to design, physical defects and vulnerabilities, software and hardware (including failures for a common reason), as well as changes in the parameters of the flows of their failures and restores.

Keywords: instrumentation and control systems, reliability and functional safety, hardware, software, set of defects, software design defect, software reliability models, Markov analysis, multi-fragment Markov models, self-diagnostic programs platforms, life cycle, verification, validation.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації:

1. Харченко В.С., Одарущенко О.Н., Поночовный Ю.Л., Одарущенко Е.Б., Скляр В.В. Технологии высокой готовности для программно-технических комплексов космических систем : монография. Харьков, 2010. 372 с. *(Особистий внесок здобувача: моделювання і оцінка готовності ПТК з урахуванням зміни параметрів процессів відмов та відновлень).*

2. Боярчук А.В., Брежнев Е.В., Горбенко А.В., Дубницкий В.Ю., Епифанов А.С., Зайцева Е.В., Засуха С.А., Иванченко О.В., Кочкарь Д.А., Левашенко В.Н., Одарущенко О.Н., Орехов А.А., Резчиков А.Ф., Сиора А.А., Скатков А.В., Скляр В.В., Тарасюк О.М. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : монография. Харьков, 2011. 641с. *(Особистий внесок здобувача: методи визначення параметрів потоків відмов та відновлення ПЗ та величин їх зміни, послідовність розробки і аналіз моделей готовності ІТ-інфраструктур з змінними параметрами).*

3. Одарущенко О.Н., Харченко В.С., Маевский Д.А., Поночовный Ю.Л., Руденко А.А, Одарущенко Е.Б., Засуха С.А., Жадан В.О., Живило С.В. CASE-оценка критических программных систем. Надежность: монография. Т.2. Харьков, 2012. 292с. *(Особистий внесок здобувача: методи контроля випадкових відмов обладнання, методи виключення систематичних відмов обладнання).*

4. Odarushchenko O., Sklyar V., Bulba E., Horbenko R., Ivasyuk A., Kotov D. Assessment of Energy Consumption for Safety-Related PLC-based Systems. *Green IT Engineering: Concepts, Models, Complex Systems Architectures, Studies in Systems, Decision and Control series*. Springer. Springer International Publishing Switzerland, 2017. P. 269 – 281. *(Особистий внесок здобувача: методика оцінювання енергоспоживання ПЛК).* (Видання входить до міжнародної наукометричної бази Scopus).

5. Odarushchenko, O. Odarushchenko, E, .Butenko, V., Ruchkov, E. Tool-Based Assessment of Reactor Trip Systems Availability and Safety Using Markov Modeling. *Cyber Security and Safety of Nucler Power Plant Instrumentation and Control Systems*. Hershey, Pennsylvania, United States of America, IGI Global, 2020. P. 175-203. *(Особистий внесок здобувача: аналіз недоліків IEC 61508, багатофрагментні марковські моделі та розв'язання систем диференційних рівнянь).*

6. Одарущенко О.Н., Одарущенко Е.Б., Стороженко А.В., Гроза П.Н. Оценка надежности программно-технических комплексов на основе многофрагментных марковских моделей. *Системи обробки інформації*. 2001. Вип. 3(13). С. 110-116. *(Особистий внесок здобувача: багатофрагментна марковська модель).*

7. Одарущенко О.Н., Одарущенко Е.Б., Поночовный Ю.Л. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем. *Авіаційно-космічна техніка і технологія*. 2002. Вип. 35. С. 187-191. *(Особистий внесок здобувача: алгоритм модифікованого експоненційного методу розв'язання систем лінійних алгебраїчних рівнянь).*

8. Одарущенко О.Н., Поночовный Ю.Л. Одарущенко Е.Б. Терминологические аспекты теории надежности программных средств. *Радіоелектронні і комп'ютерні системи*. 2004. Вип. 2(6), С. 88-94. *(Особистий внесок здобувача: визначення термінів дефект ПЗ, відмова ПЗ).*

9. Харченко В.С., Одарущенко О.Н., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов. *Радіоелектронні і комп'ютерні системи*. 2006. Вип. 5(17). С.62-70. *(Особистий внесок здобувача: визначення термінів дефект ПЗ, відмова ПЗ).*

10. Руденко А.А., Одарущенко О.Н., Харченко В.С. Модели оценки надежности программных средств с учетом недетерминированного числа вторичных дефектов. *Радіоелектронні і комп'ютерні системи.* 2010. Вип.6(47).

С.197-203. *(Особистий внесок здобувача: МНПЗ з урахуванням недетермінованого числа вторинних дефектів).*

11. Харченко В.С., Одарущенко О.Н., Модель информационно-технического состояния компьютерной системы. *Системи обробки інформації.* 2008. Вип. 7(74). С.128-130. *(Особистий внесок здобувача: модель інформаційно-технічного стану з урахуванням рівней працездатності, показники гарантоздатності).*

12. Харченко В.С., Одарущенко О.Н., Руденко А.А., Одарущенко Е.Б., Поночовный Ю.Л. Моделирование обслуживаемых компьютерных систем с учетом вторичных дефектов программных средств. *Радіоелектронні і комп'ютерні системи*. 2009. № 7. С.245-249. *(Особистий внесок здобувача*: *марковські моделі з урахуванням прояву вторинних дефектів ПЗ).*

13. Одарущенко О.Н., Харченко В.С. Информационно-технические состояния компьютеризированных систем: модель событий и показатели гарантоспособности. *Системи управління, навігації та зв'язк*. 2009. Вип. 3(11). С.156-159. *(Особистий внесок здобувача: модель подій, показники гарантоздатності).*

14. Летичевский О.О., Песчаненко В.С., Харченко В.С., Волков В.А.. Одарущенко О.М. Модельний спосіб розроблення алгоритмів цифрових систем на програмованих логічних інтегральних схемах. *Кібернетика і системний аналіз*. 2020. Т. 56. №5. С.29-37. *(Особистий внесок здобувач: елементи технології модельної розробки апаратного забезпечення з використанням комбінації методів машинного навчання та алгебраїчного підходу).* (Видання входить до міжнародної наукометричної бази Scopus).

15. Одарущенко О.Н.. Руденко А.А., Харченко В.С. Учет вторичных дефектов в моделях надежности программных средств. *Математичні машини і системи.* 2010. Вип.1. С.205-217. *(Особистий внесок здобувача*: *визначення параметрів функцій ризику моделей надійності програмних засобів для урахування вторинних дефектів).*

16. Харченко В.С., Одарущенко О.Н., Руденко А.А., Одарущенко Е.Б. Анализ сценариев и определение параметров для оценки надежности программных средств с учетом вторичных дефектов. *Системи управління, навігації та зв'язку.* 2011. Вип.3(11). С.273-280. *(Особистий внесок здобувача*: *список параметрів, які застосовуються в моделях надійності програмних засобів для урахування вторинних дефектів).*

17. Odarushchenko O., Kharchenko V., Popov P., Zhadan V. Empirical evaluation accuracy of mathematical software used for availability assessment of fault-tolerant computer systems. *Electronic Jornal Reliability & risk Analysis: Theory & Applications*. 2012. 3(26), Vol.7. P.85-97. *(Особистий внесок здобувача*: *етапи розроблення багатофрагментних марковських моделей).*

18. Одарущенко О.Н., Руденко А.А., Харченко В.С. Метод оценивания надежности программных средств с учетом вторичных дефетков. *Радіоелектронні і комп'ютерні системи*. 2012. Вип.7(59). С.313-318. *(Особистий внесок здобувача*: *метод оцінювання надійності ПЗ з урахуванням прояву вторинних дефектів).*

19. Ивасюк А.О., Одарущенко О.Н., Фадеева Е.К., Барвинко А.П. Модель и инструментальная поддержка анализа сигналов при оценке функциональной безопасности FPGA-модулей. *Системи обробки інформації.* 2013. Вип. 4(111). С.20-23. *(Особистий внесок здобувача*: *інструментальні засоби функціонального покриття для електронних проектів ПЛІС в ході виконання їх функціонального тестування).*

20. Скляр В.В.. Резуненко А.А., Одарущенко О.Н., Гудзь А.С., Щербаченко С.С., Сенаторо А.А, Вовк Е.Д. Обеспечение тестового покрытия для электронных проектов FPGA при оценивании функциональной безопасности по критериям SIL3. *Системи обробки інформації.* 2013. Вип. 5(112). С. 62-65. *(Особистий внесок здобувача*: *модель функціонального покриття для електронних проєктів ПЛІС).*

21. Odarushchenko O., Kharchenko V., Butenko V. Metric-based analysis of Markov models for computer systems availability assessment. *Радіоелектронні і комп'ютерні системи*. 2013. Вип. 5(64). С.214-220. *(Особистий внесок здобувача*: *марковські моделі оцінювання готовності комп'ютерних систем).*

22. Одарущенко О.Н., Харченко В.С., Руденко А.А., Одарущенко Е.Б. Учет фактора вторичных дефектов при оценке надежности программных средств. *Научные ведомости Белгородского государственного университета. "История. Политология. Экономика. Информатика".* 2013. №22(165). Вып. 28/1. С.153-160. *(Особистий внесок здобувача: сценарії внесення та усунення дефектів програмних засобів, аналіз моделей надійності програмних засобів з метою визначення переліку моделей для модифікації їх функцій ризику).*

23. Харченко В.С., Бутенко В.О., Одарущенко О.Н. Метрико-интервальные модели и инструментальные средства для оценивания готовности информационно-управляющих систем с использованием марковских процессов. *Системи обробки інформації.* 2014. Вип. 9(125). С.59-64. *(Особистий внесок здобувача: алгоритм обрання інструментальних засобів).*

24. Kharchenko V, Butenko V, Odarushchenko O., Sklyar V. Multi-fragmentation Markov Modeling of a Reactor Trip System. *Journal of Nuclear Engineering and Radiation Science*. 2015. Vol. 1, Iss. 3. 031005 (10 pages). URL: https: // asmedigitalcollection.asme.org/ nuclearengineering/ articleabstract/1/3/031005/472772/ Multifragmentation-Markov-Modeling-of-a-Reactor?redirectedFrom=fulltext (дата звернення: 18.01.2021). *(Особистий внесок здобувача: однофрагментні та багатофрагментні моделі оцінювання надійності комп'ютерних систем).* (Видання входить до міжнародної наукометричної бази Scopus).

25. Скляр В.В., Одарущенко О.Н., Поночовный Ю.Л., Бульба Е.Н., Ивасюк А.О. Модели отказов информационно-управляющих систем на основе самодиагностируемых программируемых платформ в системах аварийной защиты

реакторов. *Радіоелектронні і комп'ютерні системи науково-технічний журнал.* 2015. №4. С.19-24. (*Особистий внесок здобувача: базова марковська модель відмов ІКС, структурна модель системи контроля та діагностики на основі самодіагностовних програмовних платформ).*

26. Kharchenko V., Odarushchenko O., Butenko V., Moskalets V., Odarushchenko E., Strjuk O. Application of Markov Modeling for Safety Modeling for Safety Assessment of Self-Diagnostic Programmable Instrumentations and Control Systems. *Central European Researchers Journal*. 2016. Vol.2, Iss. 2. P. 61-69. URL: http://ceres-journal.eu/iss160202 (дата звернення: 18.01.2021). *(Особистий внесок здобувача: однофрагмента та багатофрагментна марковські моделі оцінювання надійності двохканальної комп'ютеризованої системи).*

27. Одарущенко О.Б., Одарущенко О.М., Бутенко В.О., Москалець В.В., Стрюк О.Ю. Моделі математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів. *Системи управління, навігації та зв'язку.* 2017. Вип. 4(44). С.40-45. *(Особистий внесок здобувача: постановка завдання розроблення моделей математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів).*

28. Одарущенко О.М., Одарущенко О.Б., Харченко В.С. Марковьскі моделі оцінювання функціональної безпеки програмно-технічних комплексів на самодіагностовних програмовних платформах з урахуванням помилок засобів контролю. *Радіоелектронні і комп'ютерні системи.* 2019. №4(92). С.17-29. *(Особистий внесок здобувача: структурні схеми систем нормальної експлуатаціїта аварійного захисту, дерева відмов, багатофрагментні моделі з урахуванням помилок засобів контролю).*

29. Руденко О.А., Одарущенко О.М., Руденко З.М., Одарущенко О.Б. Оцінювання кількості вторинних дефектів програмних засобів шляхом комплексування модифікованих моделей росту надійності Джелінські-Моранди і

Шика-Волвертона. *Системи управління, навігації та зв'язку.* 2020. Вип.1(59). С.97-100. *(Особистий внесок здобувача: модифікована МНПЗ Джелінські-Моранди).*

30. Одарущенко О.Н. Оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для програмно-технічних комплексів інформаційно-керуючих систем. *Системи управління, навігації та зв'язку.* 2020. Вип. 3(61). С.90-93.

Праці апробаційного характеру:

31.Odarushchenko, O., Kharchenko, V. Availability models of critical infrastructures with variable system dependability parameters. *Proceedings of the first International Workshop Critical Infrastructure Safety and Security. CrISS-DESSERT,* May 11-13, 2011, Kirovograd, Ukraine, 2011. P. 319-330. (*Особистий внесок здобувача: математичні моделі готовності критичних інфраструктур з змінними параметрами).*

32. Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Selecting mathematical software for dependability assessment of computer systems described by stiff Markov chains. *ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer. ICTERI 2013: Procceding of the 9th International Conference,* June 19-22, 2013, Kherson, Ukraine, 2013. P. 146 – 162. (*Особистий внесок здобувача: структурна схема надійності, багатофрагмента марковська модель).* (Видання входить до міжнародної наукометричної бази Scopus).

33.Odarushchenko O., Ivasyuk O., Bulba E. Fault injection-based technique and tool for FPGA modules safety assessment. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013,* May 23-26, 2013, Sevastopol, Ukraine, 2013. P.14. (*Особистий внесок здобувача: процедура тестування з внесенням дефектів).*

34. Butenko V., Odarushchenko O., Kharchenko V. Analysis of markov chains for high availability systems: metric-based approach. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013,* May 23-26, 2013, Sevastopol, Ukraine, 2013. P.16. (*Особистий внесок здобувача: етапи оцінювання готовності ПТК).*

35. Odarushchenko O., Kharchenko V., Sklyar V, Ivasuyk A. Fault-Injection Testing: FIT-Ability. *Proceedings of East-West Design&Test Symposium EWDTS"2013*, September 27-30, 2013, Ростов-на-Дону, Росссия, 2013. P.188-192. (*Особистий внесок здобувача: – оптимальна FIT – процедура, алгоритм та приклад виконання процедури).*

36. Odarushchenko, O., Kharchenko, V, Butenko, D, Butenko V. Assessment of the Reactor Trip System Dependability Two Markov Chains - based Cases. *Proceedings of the 10th International Conference on Digital Technologiesю,* July 9-11, 2014, Zilina, Slovakia, 2014. P. 103-109. (*Особистий внесок здобувача: багатофрагментна марковська модель, індустріальний приклад).* (Видання входить до міжнародної наукометричної бази Scopus).

37. Butenko V., Kharchenko V., Odarushchenko O., Popov P., Sklyar V., Odarushchenko E. Markov's Model and Tool-Based Assessment of Safety-Critical I&C Systems: Gaps of the IEC 61508. *12-th International Conference on Probabilistic Safety Assessment and Modeling*: *Proceeding of 12-th International conference on probabilistic safety assessment and modeling,* June 22-27, 2014, Honolulu, Hawaii, USA, 2014. P. 455-458. URL: http: // iapsam.org/ psam12/ proceedings/paper/ paper_455_1.pdf (дата звернення 18.01.2021). (*Особистий внесок здобувача: результати аналізу недоліків стандарту IEC 61508, структурна схема надійності та марковська модель системи аварійного захисту).* (Видання входить до міжнародної наукометричної бази Scopus).

38. Odarushchenko O., Kharchenko V, Sklyar V, Ivasyuk A. Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues. *Proceedings of 22nd*

International Conference on Nuclear Engineering. Technical Publication ICONE22, July 7-11, 2014, Prague, Czech Republic, 2014. Vol. 6: Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. URL: https: // asmedigitalcollection.asme.org /ICONE/ICONE22/volume/45967. ICONE22-31163, V006T13A022; 5 pages. (Дата звереннння: 18.01.2021). (*Особистий внесок здобувача: етапи виконання HW FIT процедури).* (Видання входить до міжнародної наукометричної бази Scopus).

39. Odarushchenko O., Kharchenko V, Gordieiev O., Vilkomir S. t-Wise-Based Multi-Fault Injection Technique for the Verification of Safety Critical I&C Systems. *Procceding of 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT,* February 22-26, 2015, Charlotte, USA, 2015. P. 1827-1836. (*Особистий внесок здобувача: основні етапи реалізації процедури тестування АК з внесенням мультидефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

40. Odarushchenko O., Kharchenko, Sklyar, V. Multi-Fault Injection Testing: Cases for FPGA-Based NPP I&C Systems. *Proceedings of 23rd International Conference on Nuclear Engineering ICONE-23*, May 17-21, 2015, Chiba, Japan, 2015. URL: https://inis.iaea.org/search/search.aspx?orig_q=RN:48025087 (Дата звереннння: 18.01.2021). (*Особистий внесок здобувача: індустріальний приклад виконання процедури тестування з внесення мультидефекту).* (Видання входить до міжнародної наукометричної бази Scopus).

41. Odarushchenko O., Babeshko E., Kharchenko V., Sklyar V. Toward automated FMEDA for complex electronic products. *Proceedings of the International Conference on Information and Digital Technologies,* July 7-9, 2015, Zilina, Slovakia, 2015. P. 17-22. (*Особистий внесок здобувача: етапи автоматизації техніки FMEDA).* (Видання входить до міжнародної наукометричної бази Scopus).

42. Odarushchenko O., Kharchenko, V. Butenko V., Odarushchenko, E. Markov's Modeling of NPP I&C Reliability and Safety Optimization of tool-and-technique selection. *Proceeding of Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management,* February 15-18, 2016, Beer Sheva, Israel, 2016. P. 328 – 336. (*Особистий внесок здобувача: процедура обрання інструментальних засобів для оцінювання надійності ПТК).* (Видання входить до міжнародної наукометричної бази Scopus).

43. Odarushchenko O., Strjuk O., Bulba Y., Leontiiev K., Ivasyuk A., Kharchenko V. Fault insertion software and hardware testing for safety PLC-based system SIL certification. *Proceeding of the 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018,* May 24-27, 2018, Kyiv, Ukraine, 2018. P. 202-206. (*Особистий внесок здобувача: визначення FIT – здатності, SW та HW процедури з внесенням дефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

44. Babeshko, E., Kharchenko, V., Odarushchenko, O., Leontiiev, K., Strjuk, O. NPP I&C Safety Assessment by Aggregation of Formal Techniques. *Proceedings of the 2018. 26th International Conference on Nuclear Engineering ICONE26,* July 22-26, 2018, London, England, 2018. P. 1-6. (*Особистий внесок здобувача:процедура SW FMEA).* (Видання входить до міжнародної наукометричної бази Scopus).

45. Одарущенко О.Н., Одарущенко Е.Б. Оценка надежности восстанавливаемых управляющих и вычислительных систем с учетом характеристик средств контроля в условиях дефектов программных и аппаратных средств // Науково-технічна конференція, 10-11 лист. 1999р.:тези доп. Харків, 1999. С.38-39. (*Особистий внесок здобувача: модель оцінювання надійності відновлюваних управлючих систем з урахуванням засобів контролю).*

46.Одарущенко О.Н., Одарущенко Е.Б., Яковлев В.И. Оценка надежности вычислительных систем с учетом изменения параметров отказов и восстановлений их программных средств // 8-я Международная конференция

«Теория и техника передачи, приема и обработки информации» (Интегрированные информационные системы, сети и технологии), 17-19 сентября 2002р.: тез. докл. Харьков, 2002. С. 269-271. (*Особистий внесок здобувача*: *методика оцінка надійності обчислювальних систем).*

47. Одарущенко О.Н., Поночовный Ю.Л. Надежность, как критерий качества программного обеспечения// Матеріали Міжнародної науково-технічної конференції «Інтегровані комп'ютерні технології в машинобудуванні – ІКТМ-2003», тези доп. Харків, 2003. С.221. (*Особистий внесок здобувача*: *визначення надійності як критерія якості програмного забезпечення).*

48. Одарущенко О.Н., Харченко В.С., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем// Матеріали 1-ої Міжнар. науково-техн. конф. „Гарантоспроможні (надійні та безпечні) системи, сервіси та технології - DESSERT-2006", 25-28 квітня 2006р.: тези доп. Полтава, 2006. С. 12. (*Особистий внесок здобувача*: *багатофрагмента модель для дубльованої архітектури ПТК).*

49. Одарущенко О.Н., Руденко А.А. Модель Джелинского-Моранды с учетом недетерминированного числа вторичных дефектов. Матеріали Третьої міжнародної науково-технічної конференції „Комп'ютерна математика в інженерії, науці та освіті" (CMSEE-2009), 1-31 жовтня 2009р: тези доп. Київ, 2009. С. 49-50. (*Особистий внесок здобувача*: *модифікація МНПЗ Джелинського-Моранди).*

50. Одарущенко О.Н., Руденко А.А. Использование корреляционных зависимостей при прогнозировании числа вторичных дефектов программных средств// Матеріали Четвертої міжнародної науково-технічної конференції „Комп'ютерна математика в інженерії, науці та освіті" (CMSEE-2010), 1-31 жовтня 2010р.: тези доп. Полтава, 2010. С. 53-54. (*Особистий внесок здобувача*: *приклад формування кореляційної залежності).*

51. Одарущенко О.Н., Живило С.В. Методология оценки гарантоспособности на основе фактического информационно-технического состояния// Материалы междунар одной научно-практической конференции «Информационные технологии и информационная безопасность в науке, технике и образовании (ИНФОТЕХ -2011), 05-10 вер. 2011р.: тези доп. Севастополь, 2011. С.38-39. (*Особистий внесок здобувача*: *визначенння інформаційно-технічного стану, елементи методології).*

52. Одарущенко О.Н., Руденко А.А. Определение параметров оценки надежности программных средств с учетом вторичных дефектов// Шоста науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання систем. МОДС ’2011’’, 27-30 черв. 2011р.: тези доп. Чернігів, 2010. С. 391-392. (*Особистий внесок здобувача*: *перелік параметрів оцінювання надійності ПЗ з урахуванням вторинних дефектів).*

53. Одарущенко О.Н., Руденко А.А., Руденко З.Н., Мельник М.А. Метод оценивания надежности программных средств с учетом вторичных дефектов// Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013», 24-27 червня 2013р.: тези доп. Чернігів-Жукин, 2013. С. 336-339. (*Особистий внесок здобувача*: *визначення етапів метода оцінювання надійності програмних засобів).*

54. Одарущенко О.Н., Харченко В.С. Моделирование и оценивание функциональной безопасности программно-технических комплексов в контексте стандарта IEC 61508. Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013», 24-27 червня 2013р.: тези доп. Чернігів-Жукин, 2013. С. 339-339. (*Особистий внесок здобувача*: *аналіз IEC 61508, перелік недоліків стандарта, підходи до їх усунення).*

55.Odarushchenko O., Kharchenko V., Butenko V., Odarushchenko E. Assessing of programmable system availability in context of the IEC 61508. *Program 7th International conference - Dependable Systems, Services and Technologies*

DESSERT2014, May 16-18, 2014. Kiev, Ukraine. 2014. P.21. (*Особистий внесок здобувача*: *етапи оцінювання надійности ПТК в контексті 61508).*

56. Odarushchenko O., Odarushchenko E, Strjuk O., Leontiiev K., Software Fault Insertion Testing for SIL Certification of Safety PLC-based System. *Proceeding of The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020,* May 14-18, 2020. Kiev, Ukraine. 2020. P.80-84. (*Особистий внесок здобувача*: *деталізована процедура тестування ПЗ з внесенням дефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

57. Одарущенко О.М., Одарущенко О.Б. Концепція і принципи оцінювання і забезпечення надійності та функціональної безпеки програмно-технічних комплексів. //Сьома міжнародна науково-технічна конференція «Проблеми інформатизації», 13-15 листопада 2019р.: тези доп. Черкаси-Харків-Баку-Більско-Бяла, 2019. С.5. *(Особистий внесок здобувача: Концепція і принципи оцінювання і забезпечення надійності та функціональної безпечності ПТК).*

58.Одарущенко О.М., Одарущенко О.Б. Метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах// Десята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», 9-19 квітня 2020р.: тези доп. Баку-Харків-Жиліна, 2020. С.20. (*Особистий внесок здобувача*: *метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах).*

59.Odarushchenko O., Kharchenko V., Odarushchenko V. Multi-fragmental availability models of critical infrastructures with variable parameters of system dependability, information & security. *Information and Security. An International Journal*. 2012, Vol. 28, № 2. P. 248 – 265. *(Особистий внесок здобувача*:

багатофрагментні марковські моделі критичних інфраструктур).

60.Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Availability assessment of computer systems described by stiff Markov chains: case study. *Springer.CCIS (412)*. 2013. P. 112 – 135. *(Особистий внесок здобувача: структурна схема надійності відмовостійкості системи, система диференційних рівнянь).* (Видання входить до міжнародної наукометричної бази Scopus).

Праці, які додатково відображають наукові результати дисертації:

61. Одарущенко О.Н., Харченко В.С., Поночовный Ю.Л., Одарущенко Е.Б., Бутенко В.О., Харыбин А.В. Системы и технологии высокой готовности. Харьков, 2013. 273с. (*Особистий внесок здобувача*: *моделювання та оцінка комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ).*

62. Одарущенко О.Н., Поночовный Ю.Л., Одарущенко Е.Б., Бутенко В.О., Харыбин А.В. Системы и технологии высокой готовности. Харьков, 2013. 96 с. *(Особистий внесок здобувача*: *практичні заняття змоделювання та оцінки комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ).*

63. Комп’ютерна програма «MSMC-Method selector for Markov chains»: Свідоцтво про реєстрацію авторського права на твір №57120. - Дата реєстрації 05.10.2014. *(Особистий внесок здобувача*: *алгоритм рішення марковських ланцюгів).*

64. Гарантоздатність програмно-технічних комплексів критичного призначення /Ю. Алексеєв, Б. Конорев, В. Скляр, О. Одарущенко, В. Харченко, Г. Чертков// СОУ-Н НКАУ 0060:2010. Настанова національного космічного агенства України. *(Особистий внесок здобувача*: *поняття про інформаційно-технічний стан,, дефекти та уразливості, що призводять до порушення працездатності).*

65.Харченко В.С., Андрейченко Д.К., Антощук С.Г., Дрозд М.А., Одарущенко О.Н., Бульба Е.Н., Стрюк А.Ю., Ивасюк А.О. Зеленая ИТ-

инженерия. В 2-х томах. Том 1. Принципы, компоненты, модели. Харьков, 2014. 594с. *(Особистий внесок здобувача*: *опис методів контроля відмов обладнання, опис функційного тестування, аналіз процесів валідації FPGA систем).*

66. Харченко В.С., Скляр В.В.. Одарущенко О.М., Одарущенко О.Б. Університетсько-індустріальна кооперація. Модельно-орієнтований підхід. Практичне керівництво та приклади. Харків, 2017. 363 с. *(Особистий внесок здобувача*: *опис створення spin-off компанії із задачами забезпечення та оцінювання безпеки ІКС).*

67. Барсов В.І., Одарущенко О.М., Краснобаєв В.А., Тиртишніков О.І., Барсова З.В. Основи побудови АСУ. Полтава, 2012. 400с. *(Особистий внесок здобувача: загальна характеристика процесу побудови автоматизованих систем управління).*

68. Харченко В.С., Одарущенко О.Н., Иванченко О.В. Принципы анализа и управления безопасностью критических инфраструктур. *Вісник Хмельницького національного університету*. 2010. Вип.5. С. 218-221. *(Особистий внесок здобувача*: *принципи забезпечення безпеки).*

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АК	апаратні компоненти
АГ	атрибути готовності
АБ	атрибути безвідмовності
АФБ	атрибути функційної безпечності
АІБ	атрибути інформаційної безпеки
АГз	атрибути гарантоздатності
АЗ ПЗ	аварійний та попереджувальний захист
АСУ ТП	автоматизована система управління технологічними процесами
ASIC	Application-Specific Integrated Circuit
ББМ	базова багатофрагмента марковська модель
ЖЦ	життєвий цикл
ПК	програмні компоненти
ПЗ	програмне забезпечення
ПвК	програмовані компоненти
МК	множина компонент
МНПЗ	модель надійності програмних засобів
МПЗ	множина змінних параметрів
ММ	марковська модель
МВ	множина відмов
МД	множина дефектів
МЗП	множина змінних параметрів

МС	множина станів
МА	множина атрибутів
НіФБ	надійність і функційна безпечність
БФМ	багатофрагментна марківська модель
ОФМ	однофрагментна марківська модель
СДР/ЖСДР	система диференційних рівнянь/жорстка система диференційних рівнянь
ССН	структурна схема надійності
СДПП	самодіагностовна програмовна платформа
ТККВ	технічний комплекс критичного використання
SW	Software
SRGM	Software Reliability Growth Model
SIL	Safety Integrity Level
ПЛК/БПЛК	програмовний логічний контролер / безпечний програмовний логічний контролер
ПТК	програмно-технічний комплекс
ПЛІС	програмовна логічна інтегральна схема
PFH	Probability of failure per hour
PFD_{avg}	Probability of failure on demand (average)
ІКС	інформаційно-керуюча система
I&C	Instrumentation and Control System
ІС	інформаційний стан
ТС	технічний стан
ІТС	інформаційно-технічний стан

ДФ	фізичні дефекти апаратних засобів
ДППЗ	проєктні дефекти програмних засобів
ДПА	проєктні дефекти апаратних засобів
ДВ	дефекти взаємодії
ДВФ	дефекти взаємодії фізичної природи
ДВІ	дефекти взаємодії інформаційні
ЗІВм	змінні інтенсивності відмов
ЗІВн	змінні інтенсивності відновлень
ЗКВн	запас компонент для відновлень
ФБ	функційна безпечність
ФГ	функція готовності
ФВД	фактор вторинних дефектів
FPGA	Field-Programmable Gate Array
FIT	Fault insertion testing
FPICS	FPGA PLC-based safety critical I&C systems
FFCS/ FFCSS	Full FIT Covered Space/ Full FIT Covered Space of Scheme
TFCS	Trivial FIT of Covered Space
IFCS	Implemented FIT Covered Space of Scheme
FITR	Fault Insertion Testing Restrictions
FMECA/SFMECA	Failure Mode Effect and Criticality Analysis/ Software Failure Mode Effect and Criticality Analysis
FMEDA	Failure Mode Effect and Diagnostic Analysis
HW	Hardware

ВСТУП

Обгрунтування вибору теми роботи. В забезпеченні безпеки АЕС, авіаційних і ракетно-космічних комплексів та інших критичних об’єктів важливу роль відіграють інформаційні-керуючі системи (ІКС), ядром яких є програмно-технічні комплекси (ПТК). Вартість відмов апаратних, програмних, програмовних і комунікаційних (мережних) засобів ПТК ІКС АЕС, є надзвичайно високою. Кількість експлуатаційних подій за даними сайту Державного науково-технічного центру з ядерної та радіаційної безпеки в період, які викликані відмовами ІКС в період 2015-2018 рр. становить 46%.

Найважливішою характеристикою ІКС є функційна безпечність, яка відповідно до міжнародних і національних стандартів (IEC61508, IEC26262) визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та/або його наслідки [8, 10]. Для України актуальність нормування, моніторингу, оцінювання та забезпечення функційної безпечності підтверджується наявністю великої кількості аварійно небезпечних об’єктів, перш за все, реакторів АЕС.

Це зумовлює необхідність: по-перше, гарантованого виконання вимог до стійкості до відмов програмних, програмовних, апаратних засобів, збурень різної природи та змін характеристик фізичного та інформаційного середовища; по-друге, забезпечення якості розроблення і точності відтворення реальних потреб використання ПТК ІКС за призначенням; по-третє, мінімізації часових, енергетичних та інших ресурсів, які використовуються.

Сьогоденні процеси модернізації існуючих та розробки перспективних ПТК ґрунтуються на використанні нової елементної бази, сучасних технологіях розробки їх апаратної та програмної компонент. Це, з одного боку, розширює можливості ІКС, призводить до підвищення ефективності технологічних процесів, знижує ресурсємність виробництва, а з іншого боку – призводить, до зростання ризиків, які супроводжують процес підвищення залежності функціональності, надійності і безпеки від якості проектних рішень. Тобто збільшення можливостей

сучасної елементної бази, впровадження індустріальних технологій розробки програмного забезпечення не привело до такого ж прогресу у проектуванні ПТК з необхідним і гарантованим рівнем надійності і безпеки.

Слід зазначити, що такий стан речей склався, не зважаючи на інтенсивні дослідження впродовж останніх десятиліть, які виконувалися в Україні та за її межами, зокрема, за напрямами:

− розвитку теоретичних засад, загальних методів оцінювання та підвищення надійності та функційної безпечності (A. Avizienis, J.-C. Laprie, G. Johnson, B. Randell, E. Zaitseva, Б.Ю. Волочий, Б.М. Конорєв, В.С. Харченко, М.О. Ястребенецький та інші) [7, 44, 63, 84, 96÷ 97, 217÷219, 269÷271, 279, 298];

− розроблення методів і засобів оцінювання та забезпечення надійності програмного забезпечення для різних застосунків (B. Littlewood, P. Popov, A. Romanovsky, S. Russo, L. Strigini, J. Vain, В.В. Ліпаєв, Д.А. Маєвський, В.С. Яковина та інші) [141, 142, 149, 183÷188, 221, 222, 225, 230, 231];

− розроблення й дослідження моделей та методів діагностування і забезпечення стійкості інформаційно-керуючих систем і ПТК до фізичних та проєктних дефектів (T. Anderson, F. Saglietti, K. Trivedi, О.В. Дрозд, В.А. Краснобаєв, Г.Ф. Кривуля, В.М. Опанасенко, О.М. Романкевич, В.О. Романкевич, В.В. Скляр, В.І. Хаханов та інші) [1÷3, 7, 88÷91,64÷66,68, 87, 88, 148, 227, 273];

Але залишається низка нерозв’язаних задач і обмежень існуючих методів і засобів, а саме:

− моделі, які описують надійнісну і безпекову (як інформаційну, так і функціональну) складові, не ураховують реальну розмірність задач оцінювання з огляду на складність індустріальних ІКС і ПТК, змінність параметрів відмов і відновлень;

− у методах оцінювання функційної безпечності, насамперед, аспекти безвідмовності апаратних і програмних засобів розглядаються відокремлено, без спільного кількісного аналізу результатів верифікації;

− методи розроблення й забезпечення відмовостійкості ПТК з використанням програмовних платформ недостатньо ураховують можливості, обмеження і похибки вбудованих засобів контролю і діагностування на рівні електронних проєктів, модулів і каналів тощо.

Таким чином, можливо зробити висновок про існування **протиріччя,** яке полягає у невідповідності між розширенням множини причин порушення працездатності програмно-технічних комплексів інформаційно-керуючих систем атомних станцій, аерокосмічних комплексів та інших індустріальних об'єктів критичного застосування (КЗ) 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***.

Подолати це протиріччя можливо 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 вразливостями програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційну роботу виконано на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут» 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).

Мета і завдання дослідження. Метою дисертаційного дослідження 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.

Досягнення поставленої мети передбачає вирішення таких завдань:

1. Аналіз принципів, методів і засобів оцінювання та забезпечення надійності та функційної безпечності ПТК ІКС критичного застосування;
2. Розвиток методології оцінювання і забезпечення надійності та функційної безпечності ПТК для ІКС критичного застосування;
3. Вдосконалення ймовірнісних моделей надійності програмних засобів з урахуванням вторинних дефектів;
4. Розроблення методу оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю;
5. Розроблення моделей оцінювання надійності та функційної безпечності ПТК на самодіагностованих платформах;

6. Розроблення методів верифікації і валідації програмовних платформ і ПТК на їх основі;

7. Вдосконалення методу забезпечення функційної безпечності ПТК на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності);

8. Розроблення методу оцінювання та забезпечення функційної безпечності при створенні та ліцензуванні модулів і платформ для ІКС на програмовних логічних інтегральних схемах;

9. Розроблення та впровадження інструментальних програмно-апаратних засобів підтримки процесів ліцензування програмовних платформ та ПТК ІКС, забезпечення їх відповідності вимогам національних і міжнародних стандартів.

Об'єкт дослідження – програмно-технічні комплекси інформаційно-керуючих систем критичного застосування, а також процеси забезпечення їх надійності та функційної безпечності на різних етапах життєвого циклу.

Предмет дослідження – принципи, методи і засоби оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів інформаційно-керуючих систем критичного застосування при розробленні, верифікації та використанні за призначенням.

Методи дослідження. При розв'язанні науково-прикладної проблеми було використано наступні методи. При удосконаленні ймовірнісних моделей оцінювання надійності (безвідмовності) програмних засобів було використано методи теорії надійності програмних засобів та математичної статистики. При розробленні методу оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю було використано методи теорії надійності, теорії множин і графів, марковських випадкових процесів з дискретними станами і неперервним часом. При розробленні математичних моделей оцінювання готовності та функційної безпечності ПТК на самодіагностовних платформах було використано методи теорії надійності і технічної діагностики, теорії ймовірностей та марковських випадкових процесів.

При розробленні методів верифікації і валідації програмовних платформ і ПТК на їх основі було використано методи аналізу видів, наслідків і критичності відмов, теорії множин, методи системного аналізу. При розробленні методу забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах було використано теорії надійності і технічної діагностики, теорії множин і графів, марковського аналізу. При розробленні методу оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах було використано методи теорії надійності і технічної діагностики, теорії множин і графів, марковського аналізу, системного аналізу.Оцінка експериментальних даних, отриманих у ході роботи, проводилася на основі методів математичної статистики.

Наукова новизна одержаних результатів обумовлена розробленими методологією, моделями та методами оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного призначення, які надали подальший розвиток відповідному науковому напряму та в межах яких отримані такі нові наукові результати:

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 ПТК 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 програмових 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 проектних, що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності за рахунок 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 самодіагностовних програмовних платформах шляхом

використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною.

Достовірність нових наукових положень і висновків дисертаційної роботи підтверджується:

− збігом з результатами, отриманими з використанням відомих моделей і методів теорії надійності; обґрунтованістю припущень, прийнятих при розробленні моделей і методів, виходячи з досвіду експлуатації ПТК ІКС;

− працездатністю та ефективністю апаратних рішень та інструментальних засобів, отриманих із застосуванням запропонованих методів і моделей, підтвердженою на низці підприємств;

− результатами практичного використання розроблених моделей, методів та інструментальних засобів при створенні, сертифікації та експлуатації ПТК на програмовних платформах та ІКС різного призначення.

Практичне значення одержаних результатів полягає в тому, що розроблені моделі та методи доведено до прикладних інженерних методик та процедур (додаток В), 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, а також обгрунтувати вимоги до них.

Результати досліджень впроваджено на наступних підприємствах (додаток Г):

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 (акт впровадження 17.09.2020);

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) (акт впровадження 16.09.2020);

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 (акт впровадження 28.08.2020);

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 (акт впровадження 29.09.2020);

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 (акт впровадження 23.09.2020);

6. Національному аерокосмічному університеті ім. М.Є. Жуковського «ХАІ» при виконанні 5 науково-дослідних робіт за держазомвленням (акт впровадження 24.08.2020), 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» (акт впровадження 25.09.2020).

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи отримано особисто. Робота [30] і розділи роботи [3] написано без соавторів. В опублікованих із співавторами здобувачеві належить такі результати: [1]-моделювання і оцінка готовності ПТК з урахуванням зміни параметрів процессів відмов та відновлень; [2]-методи визначення параметрів потоків відмов та відновлення ПЗ та величин їх зміни, послідовність розробки і аналіз моделей готовності ІТ-інфраструктур з змінними параметрами; [3]-методи контроля випадкових відмов обладнання, методи виключення систематичних відмов обладнання; [4]-методика оцінювання енергоспоживання ПЛК; [5]-аналіз недоліків IEC 61508, багатофрагментні марковські моделі та розв’язання систем диференційних рівнянь; [6]-багатофрагментна марковська модель; [7]-алгоритм модифікованого експоненційного методу розв’язання систем лінійних алгебраїчних рівнянь; [8]-визначення термінів дефект ПЗ, відмова ПЗ; [9]-визначення термінів дефект ПЗ, відмова ПЗ; [10]-МНПЗ з урахуванням недетермінованого числа вторинних дефектів; [11]- модель інформаційно-технічного стану з урахуванням рівней працездатності, показники гарантоздатності; [12]-марковські моделі з урахуванням прояву вторинних дефектів ПЗ; [13]-модель подій, показники гарантоздатності; [14]-елементи технології модельної розробки апаратного забезпечення з використанням комбінації методів машинного навчання та алгебраїчного підходу; [15]-

визначення параметрів функцій ризику МНПЗ для урахування вторинних дефектів; [16]-список параметрів параметрів, які застосовуються в МНПЗ для урахування вторинних дефектів; [17]- етапи розроблення багатофрагментних марковських моделей; [18]-метод оцінювання надійності ПЗ з урахуванням прояву вторинних дефектів; [19]-інструментальні засоби функціонального покриття для електронних проектів ПЛІС в ході виконання їх функціонального тестування; [20]-модель функціонального покриття для електронних проєктів ПЛІС);[21]-марковські моделі оцінювання готовності комп'ютерних систем; [22]-структурна схема надійності відмовостійкості системи, система диференційних рівнянь; [23]-алгоритм обрання інструментальних засобів; [24]-однофрагментні та багатофрагментні моделі оцінювання надійності комп'ютерних систем; [25]-базова марковська модель відмов ІКС, структурна модель системи контроля та діагностики на основі самодіагностовних програмовних платформ; [26]-однофрагмента та багатофрагментна марковські моделі оцінювання надійності двохканальної комп'ютеризованої системи; [27]-постановка завдання розроблення моделей математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів; [28]-структурні схеми систем нормальної експлуатаціїта аварійного захисту, дерева відмов, багатофрагментні моделі з урахуванням помилок засобів контролю; [29]-модифікована МНПЗ Джелінські-Моранди; [31]-математичні моделі готовності критичних інфраструктур з змінними параметрами; [32]-структурна схема надійності, багатофрагмента марковська модель; [33]-процедура тестування з внесенням дефектів; [34]-етапи оцінювання готовності ПТК; [35]-оптимальна FIT – процедура, алгоритм та приклад виконання процедури; [36]-багатофрагментна марковська модель, індустріальний приклад; [37]-результати аналізу недоліків стандарту IEC 61508, структурна схема надійності та марковська модель системи аварійного захисту; [38]-етапи виконання HW FIT процедури; [39]-основні етапи реалізації процедури тестування АК з внесенням мультидефектів; [40]-індустріальний приклад виконання процедури тестування з внесення

мультидефекту; [41]-етапи автоматизації техніки FMEDA;. [42]- процедура обрання інструментальних засобів для оцінювання надійності ПТК; [43]-визначення FIT –здатності, SW та HW процедури з внесенням дефектів; [44]-процедура SW FMEA; [45]-модель оцінювання надійності відновлюваних управлючих систем з урахуванням засобів контролю; [46]-методика оцінка надійності обчислювальних систем;[47]-визначення надійності як критерія якості програмного забезпечення; [48]-багатофрагментна модель для дубльованої архітектури ПТК; [49]-модифікація МНПЗ Джелинського-Моранди; [50]-приклад формування кореляційної залежності; [51]-визначеннння інформаційно-технічного стану, елементи методології; [52]-перелік параметрів оцінювання надійності ПЗ з урахуванням вторинних дефектів; [53]-визначення етапів метода оцінювання надійності програмних засобів; [54]-аналіз IEC 61508, перелік недоліків стандарта, підходи до їх усунення; [55]-етапи оцінювання надійности ПТК в контексті 61508; [56]-деталізована процедура тестування ПЗ з внесенням дефектів; [57] - Концепція і принципи оцінювання і забезпечення надійності та функціональної безпеки програмно-технічних комплексів; [58] - метод оцінювання та забезпечення функційної безпеки; [59]- багатофрагментні марковські моделі критичних інфраструктур; [60] – марковські моделі; [61] - моделювання та оцінка комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ; [62]-практичні заняття змоделювання та оцінки комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ; [63] - алгоритм рішення марковських ланцюгів; [64]-поняття про інформаційно-технічний стан, дефекти та уразливості, що призводять до порушення працездатності; [65]-опис методів контроля відмов обладнання, опис функційного тестування, аналіз процесів валідації FPGA систем; [66] - опис створення spin-off компанії із задачами забезпечення та оцінювання безпеки ІКС; [67]-загальна характеристика процесу побудови автоматизованих систем управління; [68]-принципи забезпечення безпеки.

Результати дисертаційної роботи повністю відображено в публікаціях. Всі співавтори згодні із внеском здобувача. Робота не містить плагіату та запозичень. У докторській дисертації не містяться результати кандидатської дисертації.

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи доповідалися та обговорювалися на міжнародних, всеукраїнських та регіональних конференціях: Всеукраїнському науково-технічному семінарі «Критичні комп'ютерні технології та системи» на кафедрі комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ» (м. Харків, 2003÷2019 рр.); DepCos-RELCOMEX 2010: Dependability of Computer Systems - International Conference on Dependability of Computer Systems, Brunow Palace, Poland, 2010; IDT 2013: 7th International Conference on Digital Technologies, Circuits, Systems and Signal Processing, Žilina, Slovak Republic, 2010; ICTERI 2013: 9th International Conference on ICT in Education, Research, and Industrial Applications, Kherson, Ukraine, 2013; 6th International Workshop on the Applications of FPGA in Nuclear Power Plants, Kirovograd, Ukraine, 2013; CrISS 2013: 3rd International Workshop Critical Infrastructure Safety and Security, Sevastopol, Ukraine, 2013; EWDTS 2013: East-West Design&Test Symposium, Ростов-на-Дону, Росія, 2013; МОДС 2013: Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання», Чернігів-Жукин, Україна, 2013; DT 2014: 10th International Conference on Digital Technologies, Zilina, Slovak Republic, 2014; PSAM 12: 12th International Conference on Probabilistic Safety Assessment and Modeling, Hawaii, Honolulu, USA, 2014; ICONE 22: 22nd International Conference on Nuclear Engineering, Prague, Czech Republic, 2014; NPIC and HMIT 2015: 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC, USA, Charlotte, 2015; ICONE 23: 23rd International Conference on Nuclear Engineering, Chiba, Japan, 2015; SMRLO 2016: 2nd International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management, Beer Sheva, Israel, 2016; ICONE 26: 26th International

Conference on Nuclear Engineering, London, United Kingdom, 2018; міжнародна науково-технічна конференція НТК "Гарантоздатні (надійні і безпечні) системи, сервіси і технології (DESSERT – Dependable Systems, Services and Technologies)" (м. Полтава, 2006 р., м. Кіровоград, 2007-2010 рр., м. Севастополь, 2012 р., 2014 р., м. Київ, 2016 р., 2018 р., 2020 р.).

Публікації. За результатами досліджень опубліковано 68 наукових праць, 5 монографій [1-5], з яких одну індексовано у науково-метричній базі Scopus, підручник [67], 2 навчальних посібника [61, 62], настанова Національного космічного агентства України [64], 25 статей у наукових фахових виданнях України та інших держав [6-30], з яких 3 індексовано у науково-метричній базі Scopus, 30 тез доповідей в збірниках матеріалів конференцій [31-60], з яких 12 індексовано у науково-метричній базі Scopus, отримано свідоцтво про реєстрацію авторського права на твір [63].

Структура та обсяг дисертації. Дисертаційна робота складається з анотацій двома мовами, вступу, шести розділів, висновків, списку використаних джерел та додатків, де: додаток А - показники, параметри системні позначення; додаток Б – результати оцінювання готовності ПТК дубльованих архітектур; додаток В – загальна процедура верифікації і валідації; додаток Г – акти впровадження; додаток Д – список опублікованих праць за темою дисертації. Загальний обсяг дисертації становить 429 сторінок; робота містить 112 рисунків (з них 16 на окремих сторінках); 35 таблиць; список використаних джерел, що включає 317 найменувань на 36 сторінках; 4 додатки на 41 сторінці.

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ КРИТИЧНОГО ВИКОРИСТАННЯ. ФОРМУЛЮВАННЯ НАУКОВО-ПРИКЛАДНОЇ ПРОБЛЕМИ ТА МЕТОДИКИ ДОСЛІДЖЕНЬ

1.1 Аналіз причин та наслідків відмов інформаційно-керуючих систем та їх вплив на надійність і функційну безпеку технічних комплексів критичного використання

1.1.1 Аналіз причин відмов авіаційних систем та ракетно-космічної техніки

Зростаюча залежність суспільства від інформаційних технологій (ІТ) проявляється у двох протилежних тенденціях. З однієї сторони, динамічно розширюється набір ІТ-продуктів та послуг, які стали частиною життя, а з іншого, - зростають ризики, що супроводжують процес, який прискорює залежність функціональності, надійності та безпеки аварійно-небезпечних систем, елементів критичної інфраструктури з інтенсивним використанням ІТ від якості проєктних рішень, яки отримані та реалізовані за допомогою цих технологій. Ця залежність та зростання ризиків, пов'язаних з ІТ, проявляється у різних технічних комплексах критичного використання (ТККВ), таких як атомна енергетика, ракетно-космічна та авіаційна техніка [81]. Наблюдається схожість причин окремих систуацій або передумов до них та схожість статистичних даних про відмови, які привели до аварійних ситуацій. Незважаючи на зростаючу безпеку виконання польотів, яка є похідною великої кількості факторів: технічних, організаційних, природних, людських, авіаційниі катастрофи відбуваються. З детальною статистикою щодо аварій воздушних суден можливо ознайомитись на сайті історика авіакатастроф Ронана Хуберта [315]. Цей архів включає дані про 26375 авіаційних аварій.

Найчастіша причина катастроф - людський фактор (35%). Майже чверть припадає на технічні несправності, погодні умови - 6%. Терористична атака або саботаж привели до 5% авіакатастроф (всю класифікацію зробили автори сайту). Аналіз статистики технічних відмов показує, що першочерговою причиною помилок пілота були сбої в роботі бортових на наземних інформаційно-керучих систем. Тобто справедливим є висновок про те, що технічні відмови є фактично домінуючим фактором авіаційних катастроф.

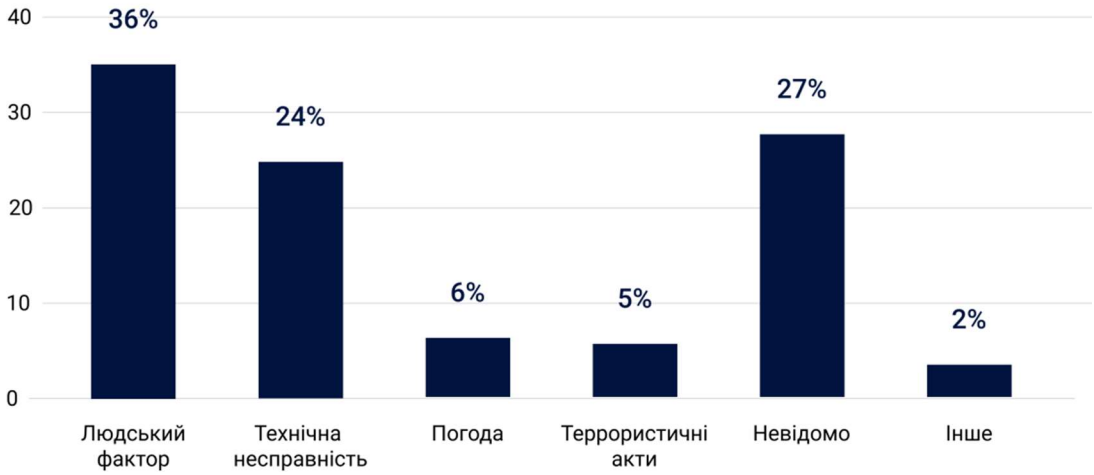


Рис. 1.1 Причини загибелі літаків за даними сайту Bureau of Aircraft Accidents Archives

Аналіз причин аварій і катастроф ракетоносіїв і космічних апаратів показує, що вплив ІКС на безпеку польотів ракетно-космічної техніки (РКТ) змінювався разом з еволюцією цих систем [316]. Основні причини аварій РКТ за період з 1960 по 2000 рр. наведені в таблиці 1.1 Накопичення досвіду, впровадження нових систем керування, вдосконалення процедур підготовки до виконання запусків призвело до зниження відсотка аварійності в 70-80-і рр. Це обумовлено нівелюванням безлічі чинників, які визначали рівень безпеки РКТ на початковому етапі освоєння космосу. Якісний стрибок в еволюції бортових ІКС почався в середині 90-х рр., зумовивши появу нових ризиків. Він характеризувався впровадженням нових інформаційних технологій в аерокосмічній індустрії,

комп'ютеризацією РКТ, подальшою еволюцією бортових ІКС [60].

Нові ризики призвели до збільшення аварійності РКТ. Поява відмов апаратної і програмної частини ІКС фактично показує напрямки еволюції бортових ІКС в той період. Відмови програмного забезпечення разом з відмовами двигунів ділять 3-4 місце серед причин відмов. В середньому через відмови програм припиняється аварією кожен 100-й пуск (в середньому - раз на рік). Слід зазначити, що апаратні засоби відмовляють майже в два рази рідше, ніж ПЗ

Таблиця 1.1

Причини відмов РКТ

Причини аварій	1960 рр.		1970 рр.		1980-90рр.		2000рр.	
	к-сть	%	к-сть	%	к-сть	%	к-сть	%
Відмови і вибухи ракетоносія	136	79	60	66	38	90	31	29
Відмови космічних апаратів (КА)	9	5	9	10	0	0	0	0
Відмови двигунів	6	3	5	5	1	2	10	10
Відмови радіоапаратури (РА)	2	1	2	2	1	2	7	7
Відмови розгінних блоків (РБ)	3	2	1	1	1	2	6	6
Відмови систем живлення та кабельних мереж	2	1	1	1	0	0	9	9
Відмови систем керування	**16**	9	**14**	15	**1**	2,5	**24**	23
Відмови апаратних засобів бортових комп’ютерів (АЗ)	0	0	0	0	0	0	6	6
Відмови програмного забезпечення (ПЗ)бортових комп’ютерів	0	0	0	0	0	0	10	10
Усього	174	100	92	100	42	100	103	100

Дана тенденція збереглася і в останнє десятеріччя, прикладом цього є

невдалий запуск 01 лютого 2011 року ракети-носія «Рокот», в результаті аварії розгонного блоку «Бриз-КМ» (помилка програмного забезпечення) КА «ГЕО-ИК-2» виведено на нерозрахункову орбіту, в результаті чого апарат втрачено. Наступна аварія сталася 17 серпня 2011 року призапускі ракети-носія «Прогрес-М» (помилка програмного забезпечення) [317].

1.1.2 Аналіз причин та наслідків відмов інформаційно-керуючих систем і їх вплив на надійність і функційну безпечність систем промислової автоматизації

В теперішній час у світі наблюдається стала тенденція зростання кількості вироблення електричної енергії, яку генерують атомні електростанції. Так тільки за останнє десятиріччя ця кількість зросла на 30%. За даними, наприклад, компанії Westinghouse станом на 1 вересня 2017 року в світі налічувалась рекордна кількість працюючих атомних реакторів - 477. Потужність АЕС досягла майже 400 гігават. Будуються 56 нових реакторів, заплановані до будівництва 160. У появі власної ядерної енергетики зацікавлені 28 держав.

В забезпеченні безпеки АЕС велику роль відіграє автоматика, а більш конкретно – інформаційно - керуючі системи (ІКС), ядром яких є програмно-технічні комплекси (ПТК) [6].

Вартість відмов апаратних, програмних, програмовних і комунікаційних (мережних) засобів критичних ІКС, є надзвичайно високою. Розподіл причин порушень в роботі АЕС України, які викликані неправильним функціонуванням ІКС (за даними сайту Державного науково-технічного центру з ядерної та радіаційної безпеки http://sstc.com.ua) в період 2015-2018 рр. наведено діаграмою на рис.1.2. Доля порушень ІКС сягає 46%.

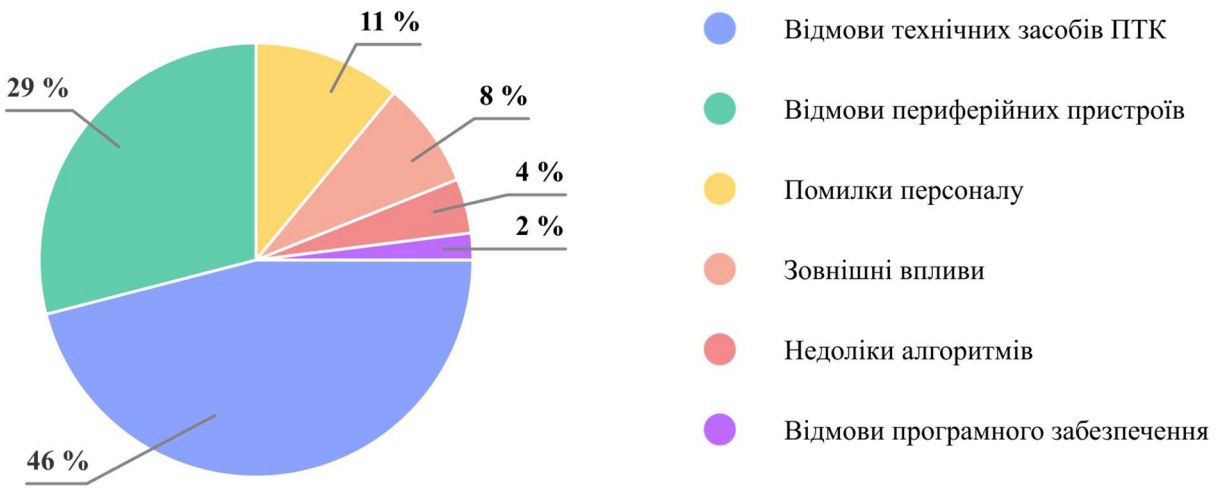


Рис.1.2 Розподіл причин порушень в роботі АЕС України в період 2015-2018 рр.

Найважливішою характеристикою критичних ІКС є функційна безпечність, яка відповідно до міжнародних і національних стандартів (IEC61508 [8], IEC26262 [10], IEC62443 [12]) визначає здатність систем мінімізувати ризики переходу в аварійний (небезпечний) стан та/або його наслідки. Для України актуальність нормування, моніторингу, оцінювання та забезпечення функційної безпечності підтверджується наявністю великої кількості аварійно небезпечних об’єктів, перш за все, АЕС, енергетичних систем і комунікацій, промислових виробництв, авіаційних та ракетно-космічних комплексів та існуючими фактами експлуатаційних подій, які вібуваються на обє’єктах критичної інфраструктури (Таблиця 1.12).

Це зумовлює необхідність: по-перше, гарантованого виконання вимог до стійкості до відмов програмних, програмовних, апаратних засобів, збурень різної природи та змін характеристик фізичного та інформаційного середовища; по-друге, забезпечення якості розроблення і точності відтворення реальних потреб використання ІКС за призначенням; по-третє, мінімізації часових, енергетичних та інших ресурсів, які використовуються.

Таблиця 1.2.

Кількість експлуатаційних подій, які відбулися на енергоблоках АЕС України (2015 – 2018)

Рік	Запоріжська АЕС	Хмельницька АЕС	Южно-Українська АЕС	Рівненська АЕС	Всього	За класифікацією INES - Inernational Nuclear Event Scale
2015	9	2	5	1	17	0
2016	5	1	5	1	12	0
2017	7	2	3	6	18	0
2018	7	7	3	2	19	0

ІКС, що забезпечують на сьогодні функціонування енергоблоків ВВЕР-1000, ВВЕР-440 є спадщиною СРСР та зберігають набір «дефецитів безпеки» [1-3]:

- недостатня надійність технічних засобів;
- незадовільна діагностика технічного та програмного забезпечення;
- неповне задоволення вимог до сейсмостійкості;
- відсутність системінформаційної підтримки персоналу;
- громіздкість (велика кількість шкафів), що потребує великих трудозатрат з обслуговування;
- різноманітність елементної бази та технічних рішень для різних ІКС (в межах одного енергоблоку) тощо.

Набір цих та інших дефецитів безпеки зумовлює необхідність виконання модернізації та заміни ІКС. Сьогоденні процеси модернізації існуючих та розробки перспективних ІКС ґрунтуються на використанні нової елементної бази, сучасних технологіях розробки їх апаратної та програмної компонент. Це з одного боку розширює можливості ІКС, призводить до підвищення ефективності технологічних процесів, знижує ресурсємність виробництва, а з іншого боку призводить до зростання ризиків, які супроводжують процес підвищення

залежності функціональності, надійності і безпеки ІКС від якості проектних рішень. Тобто збільшення можливостей сучасної елементної бази, впровадження індустріальних технологій розробки програмного забезпечення, не привело до такого ж прогресу в області проектування ІУС з необхідним і гарантованим рівнем надійності і безпеки, іншими словами зниження дефіцтиів безпеки одного переліки призводить до виникнення нових.

1.1.3 Аналіз нормативних документів в галузі ІКС ТККВ

На даний момент базовими стандартами з безпеки ІКС є стандарти Міжнародної електротехнічної комісії (МЕК англ. International Electrotechnical Comission - IEC) серії МЕК 61508 «Функційна безпечність електричних, електронних і програмованих систем, важливих для безпеки», який складається із семи частин. До основних особливостей цього стандарту належать наступні:

− використання концепції рівней повноти безпеки (Safety Integrity Levels – SIL). Усього стандарт визначає чотири таких рівня від SIL1 до SIL4. Відповідно до цих рівней обладнання проєктується в залежності від вкладу в безпеку критичного об’єкту кожного елемента обладнання;

− розгляд V-моделі життєвого циклу (ЖЦ) критичної системи та рекомендації щодо методів проектування, тестування для кожного етапу ЖЦ;

− окреме визначення програмного забезпечення, як одного із основних джерел відмов, які мають вплив на безпеку системи;

− формулювання вимог в узагальненому вигляді, що дає підгрунтя для їх застосування при розробленні груп стандартив різних галузей промисловості.

У відповідності до цих особливостей на базі МЕК 61508 розроблено наступні стандарти:

− для атомної енергетики – стандарти МАГАТЕ (Міжнародної агенції з атомної енергії, англ. International Atomic Energy Agency) та стандарти МЕК;

− для космічної галузі - стандарти Європейської кооперації із космічної стандартизації (ECSS - European Cooperation for Space Standardization), зокрема, ECSS-E-10 «Космічна інженерія - Розробка систем», ECSS-E-40A «Космічна інженерія - Розробка програмного забезпечення» та інш.;

− для авіації - стандарти Радіотехнічної комісії з аеронавтіки (RTCA - Radio Technical Commission for Aeronautics), зокрема, DO-178B (1992) «Розгляд програмного забезпечення при сертифікації бортових систем і устаткування»;

− для автомобільної техніки - стандарти Асоціації із на-надійності в автомобільній промисловості (MIRA - Motor Industry Research Association), зокрема, MISRA-C: 2004 «Руководство із використанню мови С в критичних системах»;

− для залізничного транспорту - європейські нормативи, розроблені Європейським комітетом із електротехнічної стандартизації (CENELEC - European Committee for Electrotechnical Standardization), зокрема, EN 50126 «Об'єкти залізничного транспорту. Вимоги та підтвердження надійності, безвідмовності і безпеки».

Крім того, слід зазначити стандарт ISO / IEC 12207: 1995 «Інформаційні технології - Процеси життєвого циклу програмного забезпечення» розроблений об'єднаним технычним комітетом з інформаційних технологій МЕК і Межнародною організацією зі стандартизаціэю із стандартизації (ISO). Зазначений стандарт адаптований в якості державного стандарту України ДСТУ 3918-1999.

Основними розробниками міжнародних стандартів із ІКС АЕС є МАГАТЕ і технічний підкомітет 45А МЕК. Нормативна база України в сфері застосування ядерної енергії, ядерної та радіаційної безпеки має ієрархічну структуру (рис.1.3) і детально описана в роботі [2].

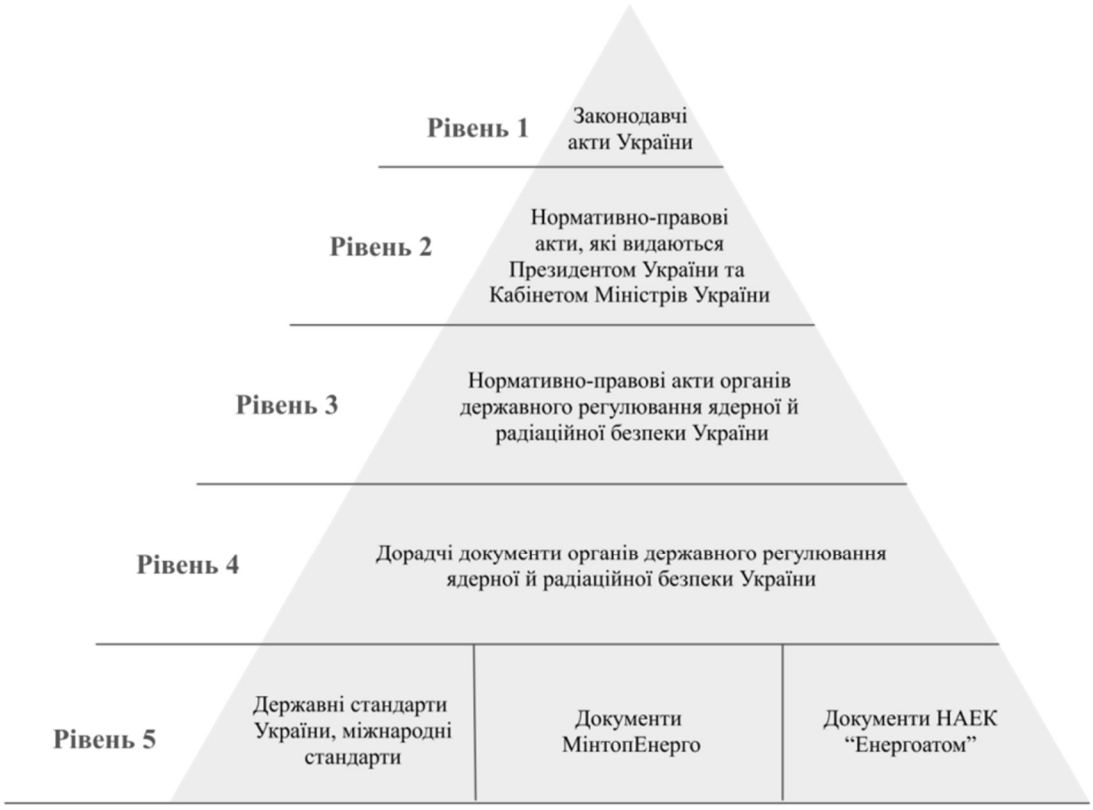


Рис.1.3 Нормативна база України в сфері застосування ядерної енергії, ядерної та радіаційної безпеки

Структура стандартів МАГАТЕ наведена на рис. 1.4. [1]

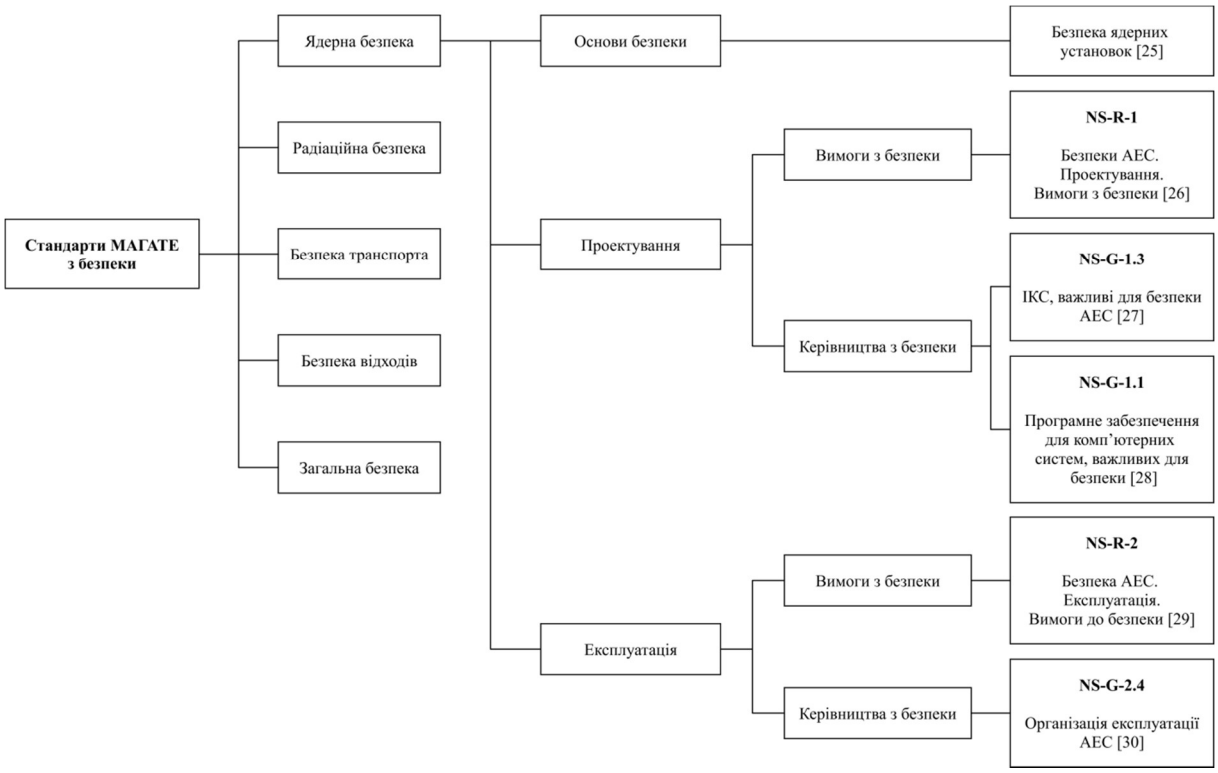


Рис.1.4 Структура стандартів МАГАТЕ з безпеки

Базовими стандартами з функційної безпечності МЕК, які регламентують вимоги до ІКС ТККВ є наступні:

− МЕК 61508 «Функційна безпечність електричних, електронних і програмованих систем, важливих для безпеки»;

− МЕК 61513: 2001 «Атомні електростанції - інформаційні та керуючі системи, важливі для безпеки - Загальні вимоги до АЕС»;

− МЕК 61226: 2005 (2-а редакція) «Атомні електростанції - Інформаційні та керуючі системи, важливі для безпеки - Класифікація»;

− МЕК 60987: 1 989 «Програмовані цифрові комп’ютери, важливі для безпеки атомних електростанцій»;

− МЕК 62138: 2006 (2-я редакція) «Атомні електростанції - Інформаційні та керуючі системи важливі для безпечності - Програмні аспекти комп'ютерних систем, що виконують функції категорії А»;

− МЕК 62138: 2004 «Атомні електростанції - Інформаційні і керуючі системи важливі для безпеки - Програмні аспекти комп'ютерних систем, що виконують функції категорій В та С».

Наступні нормативні документи МАГАТЕ містять вимоги до ІКС АЕС і їх компонентів:

− МАГАТЕ NS-G-1.3 «Інформаційні та керуючі сістеми важливі для безпеки АЕС. Керівництво із безпеки », 2002;

− МАГАТЕ NS-G-1.1 «Програмне забезпечення для комп'ютерних систем, важливих для безпеки АЕС. Керівництво із безпеки », 2000;

− МАГАТЕ TRS № 384 «Верифікація та валідація програмного забезпечення, що відноситься до інформаційних і екруючих систем атомних електростанцій. Технічний звіт».

В Україні з 2000 р діє нормативний документ НП 306.5.02/3.035-2000 «Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій».

Таким чином, вимоги, що пред'являються до ІКС АЕС, спрямовані, в першу чергу, на забезпечення ядерної та радіаційної безпеки.

Наведені множини стандартів встановлюють систему вимог до надійності та функційної безпечності ІКС ПТК, які систематизовано в роботі [18]
та наведено в таблиці 1.3.

Таблиця 1.3

Система вимог до надійності та функційної безпечності ІКС ПТК

Загальні вимоги з ядерної та радіайійної безпеки	Вимога (+)		
	ІКС ПТК	АК	ПК
Класифікація рівня безпеки	+	+	+
Вимоги до складу функцій, що виконуються	+	+	+
Вимоги до дотримання принципу одиничної відмови	+		
Вимоги до дотримання принципу резервування	+		
Вимоги до дотримання принципу різноманітності	+		
Вимоги до структури та елементів ПЗ			+
Вимоги до показників надійності	+	+	
Вимоги до відмов за загальною причиною	+		+
Вимоги до технічного діагностування	+	+	+
Вимоги до якості виконнання функцій:			
− вимоги до точності	+	+	
− вимоги до часових характеристик	+		+
− вимоги до інтерфейсу «людина-машина»	+		
Вимоги до стійкості виконання функцій:			
− вимоги по стійкості до зовнішніх чинників		+	
− вимоги по стійкості до зміни параметрів живлення		+	
− вимоги до електромагнітної сумісності		+	
− вимоги до запобіганню помилкам персоналу	+		
− вимоги до захисту від несанкціанованого доступу	+	+	+
Вимоги до відсутності впливу на інші системи			
− дотримання принципу незалежності	+		

Продовження таблиці 1.3

− вимоги до електромагнітної сумісності (до випромінюваних перешкод)		+	
− вимоги до ізоляції		+	
− вимоги до пожарної безпеки		+	
Процесні вимоги			
− розробка і виконання робочих процедур та інструкцій	+	+	+
− вимоги до випробування	+	+	
− вимоги до верифікації та валідації	+	+	+
− вимоги до кваліфікації обладнання	+	+	+

З урахуванням особливостей ПЗ, вимоги стандартів до нього необхідно аналізувати окремо. Нормативний документ НП 306.5.02/3.035-2000 «Вимоги з ядерної та радіаційної безпеки до інформаційних і керуючих систем, важливих для безпеки атомних станцій» визначає наступну структуру вимог до ПЗ:

− вимоги до ПЗ, як до продукту розроблення (вимоги до структури і елементам ПЗ, вимоги до діагностування, вимоги до забезпечення захисту від відмов, дефектів, помилок;

− вимоги до процесів етапів життєвого цикла (вимоги до етапів розроблення, вимоги до тестування та верифікації).

Вибір профіля вимог залежить від типа ПЗ, яке розроблюється. Профіль типу ПЗ визначається набором класифікаційних ознак, де:

− ознака 1 (категорія безпечності функцій, що виконуються) – відповідно ПЗ категорій А, В, С; ПЗ, яке не виконує функції безпеки;

− ознака 2 (призначення ПЗ) – відповідне системне (загальне), функціональне (прикладне), інструментальне (технологічне).

− ознака 3 (апробованість) – вперше розроблене ПЗ, раніше розроблене ПЗ власної розробки, ПЗ із доступною документацією (комерційне ПЗ), комерційні середовища розробки (англ. Integrated Development Environment IDE).

Таким чином, за результатами аналізу міжнародної і національної нормативної бази щодо оцінювання і забезпечення надійності і функційної

безпечності ІКС ТККВ та їх ПТК встановлено наступне – роозроблення та впровадження рекомендацій вимог нормативних документів, зокрема основного стандарту IEC 61508, дозволило перейти при проектуванні ІКС ТККВ від принципу «проєктуємо настільки добре, наскільки це можливо» до проектування на основі аналізу ризиків та рекомендацій щодо їх зниження. Зважаючи на безумовно позитивні підходи, які стандартом рекомендовано застосовувати при проєктуванні, він не вільний від наступних недоліків:

Недолік 1. Застосування показника PFH (англ. probability of failure per hour) для систем, важливих для безпеки, є недостатньо обґрунтованим за умови їх розроблення з використанням методів резервування, програмно-апаратного автоматичного діагностування та інших і фактично дає змогу оцінити їх надійність та функційну безпечність на початковому інтервалі експлуатації (до першої відмови). Щодо цього показника існує а термінологічна плутанина. За визначенням та фактично – очікувана частотність настання аварій і, таким чином, інтенсивність запиту на виконання відповідної функції безпеки. При цьому стандарт показник називає ймовірністю (probability of failure per hour).

Недолік 2. Результати аналізу стандарту доводять, що він надає перелік рекомендацій для розроблення систем з урахуванням того, що система є програмно-апаратною. Але рекомендацій щодо методів обчислення показників надійності та функційної безпечності систем з комплексним урахуванням надійності програмних та апаратних компонент не містить.

Недолік 3. Частина тверджень IEC 61508-7, наприклад: «... однорідний ланцюг Маркова є простою системою лінійних диференціальних рівнянь з постійними коефіцієнтами. Шляхи аналізу даних моделей, а також ефективні алгоритми їх вирішення були давно проаналізовані і розроблені ...» та частина IEC 61508-6: «... ефективні алгоритми вирішення даних рівнянь давно були розроблені і впроваджені в програмне забезпечення, з цього дослідника необхідно акцентувати увагу на побудову моделі, а не на математичних методах вирішення даних систем рівнянь ...»; «... дослідник також повинен провести перевірку

отриманих результатів за допомогою ручних обчислень ...»; «... в разі застосування програмного продукту в ході дослідження системи, практик повинен мати чітке розуміння, які техніки впроваджені в дане ПЗ і що вони повністю відповідають рішенням даного завдання ...» містять спірну до практичного застосування інформацію.

Таким чином встановлено, що існуюча нормативна база вимагає встановлення всеохоплюючих засобів для забезпечення надійності та функційної безпечності ПТК ІКС КЗ, що потребує виконання аналізу, розроблення нових моделей, методів, технологій оцінювання і забезпечення вказаних властивостей на всіх етапах життєвого циклу систем досліджуваного класу. Важливим є встановлений факт, що існуючі стандарти не дають рекомендацій щодо комплексного оцінювання систем з урахуванням того, що сучасні обчислювальні системи інтегрують апаратні і програмні засоби, які в ході роботи мають взаємний вплив.

На прикладі базового стандарта IEC 61508 доведено, що стандарт (стандарти) не вільні великої кількості недоліків: неточних визначень, методологічних невизначеностей або некорректних рекомендацій тощо.

1.1.4 Аналіз тенеденцій розвитку ІКС ТККВ

Сучасні ІКС ТККВ є цифровими територіально розгалудженими системами. Цифровізація ІКС супроводжується активним впровадження інформаційних технологій в процеси розроки, тестування таких систем. Тенденція цифровізації ІКС ТККВ, надає перелік їх переваг в порівнянні із системами попереднього покоління:

− збільшення продуктивності виконання обчислень, завдяки чому стає можливим підвищити кількість і складність функції управління і складні обчислюва-лення;

− підвищення рівня надійності апаратної компоненти та їх інтеграції, що

сприяє зменшенню кількості цих компонент і зниження числа з'єднань між ними;

− підвищення гнучкості систем при оновленні, оскільки характеристики систем можуть змінюватися модифікацією програмного забезпечення без заміни технічних засобів;

− можливість широкої реалізації підсистем самодіагностики, а також діагностики периферійного обладнання;

− істотне поліпшення інтерфейсу з персоналом завдяки можливості графічного відображення, поліпшення якості пристроїв відображення інформації;

− збільшення швидкості передачі даних по каналах зв'язку завдяки застосуванню оптико-електронних та фіброоптіческой ліній;

− можливість реалізації великої кількості входів і виходів.

Ці переваги викликають істотні зміни в ІКС АЕС, а саме:

− реалізацію розподіленого управління зі структурною і функціональною децентралізацією із застосуванням локальних мереж для обміну інформацією між окремими частинами системи;

− використання замість релейно-контактних логічних схем цифрових логічних схем;

− заміна аналогових пробів на цифрові на пультах керуваня, впровадження цифрових регуляторів, наприкла ПІД-регуляторів;

− периферійне обладнання виконуються як програмно-апаратні компоненти;

− можливість «гарячої» заміни компонент систем (датчиків, модулів обчислювальних платформ т ощо);

− широке впровадження дистанційного керувння (безспсередньо з робочих станцій);

Однак поряд з перевагами цифровізації її впровадення породжує або зберігає ряд недоліків, а саме:

− підвищення складності систем підвищує ймовірність помилки розробників систем, тому процесс розроблення систем стає складним та багатоетапним із використанням спеціалізованих інструментів розробки, які в свою чергу потребують детального вибору та оцінювання з точки зору їх застосування для розробки безпечних або важливих для безпеки систем;

− процеси тестування комп'ютеризованих систем є складними та багатоетапними. Етапи тестування мають бути Ці процеси потребують застосування значної кількості технік, методів і програмно-апаратних інструментів тестування, які потребують постійного розроблення і модернізації;

Наведені тенденції розвитку ІКС забезпечують підвищення кількості функцій що автоматизуються, зростає рівень автоматизації технологічних процесів з одного боку. З іншого боку впровадження нових цифрових та інформаційних технологій породжує нові ризики, які впливають на безпеку систем та відповідно стають актуальним завдання розроблення і впровадження методів, технік та програмно-апаратних засобів розроблення, верифікації і валідації компонент та в цілому ІКС ТККВ.

1.1.3 Узагальнена структура ПТК ІКС

Програмно-технічним комплексом називають сукупність засобів обчислювальної техніки, програмного забезпечення і засобів створення і заповнення машинної інформаційної бази при введенні системи в дію, достатніх для виконання однієї або більше завдань автоматизованих систем (АС) [34].

ПТК утворює центральну частину ІКС (Рис. 1.6). Зазвичай до складу ІКС входить один ПТК, який є головним компонентом системи, який бере участь в реалізації всіх її основних і додаткових функцій. Іноді до складу ІКС може входити кілька ПТК. Для підвищення надійності і функційної безпечності передбачається кілька каналів в одному ПТК і (або) декілька ПТК в одній системі, які одночасно і незалежно беруть участь в реалізації основних функцій,

резервуючи один одного. Кожен ПТК виконаний у вигляді експлуатаційно-автономних складових частин, що з'єднуються електричними або іншими сполучними лініями (наприклад, волоконно-оптичними) і під управлінням власного програмного забезпечення виконує набір таких основних функцій [3]:

- прийом і перетворення в цифрову форму сигналів від периферійних пристроїв;
- обмін інформацією з іншими ПТК;
- обробку прийнятої інформації і вироблення команд управління;
- формування і видачу керуючих сигналів на виконавчі пристрої;
- діагностування стану власного і сполученого устаткування;
- архівування, відображення інформації та в разі необхідності on-line управління.

Узагальнена структура ПТК ІКС АЕС, побудована на основі аналіза структур ПТК [7], розроблених ПАТ НВП «Радій», м. Кропивницький наведена на (Рис.1.4).

Інформаційно-керуюча система (ІКС) - збірне поняття, яке об’єднує за визначенням [6] та узагальнена сруктура якої наведена на (Рис.1.7):

- інформаційна система - система, що призначена для контролю стану і/або функціонування технологічної системи;

- керуюча система - система, що призначенаі для формування і видачі керуючих впливів, що змінюють стан системи і/або функціонування технологічних систем у напрямі, який вимагається.

Автоматизована система управління технологічними процесами (АСУ ТП) – визначається ГОСТ 34.003 як система, що складається з персоналу і комплексу автоматизації його діяльності, що реалізує інформаційну технологію виконання встановлених функцій управління технологічним процесом. Узагальнена структурна схема АСУ ТП наведена на рис.1.6 [1,2,299].

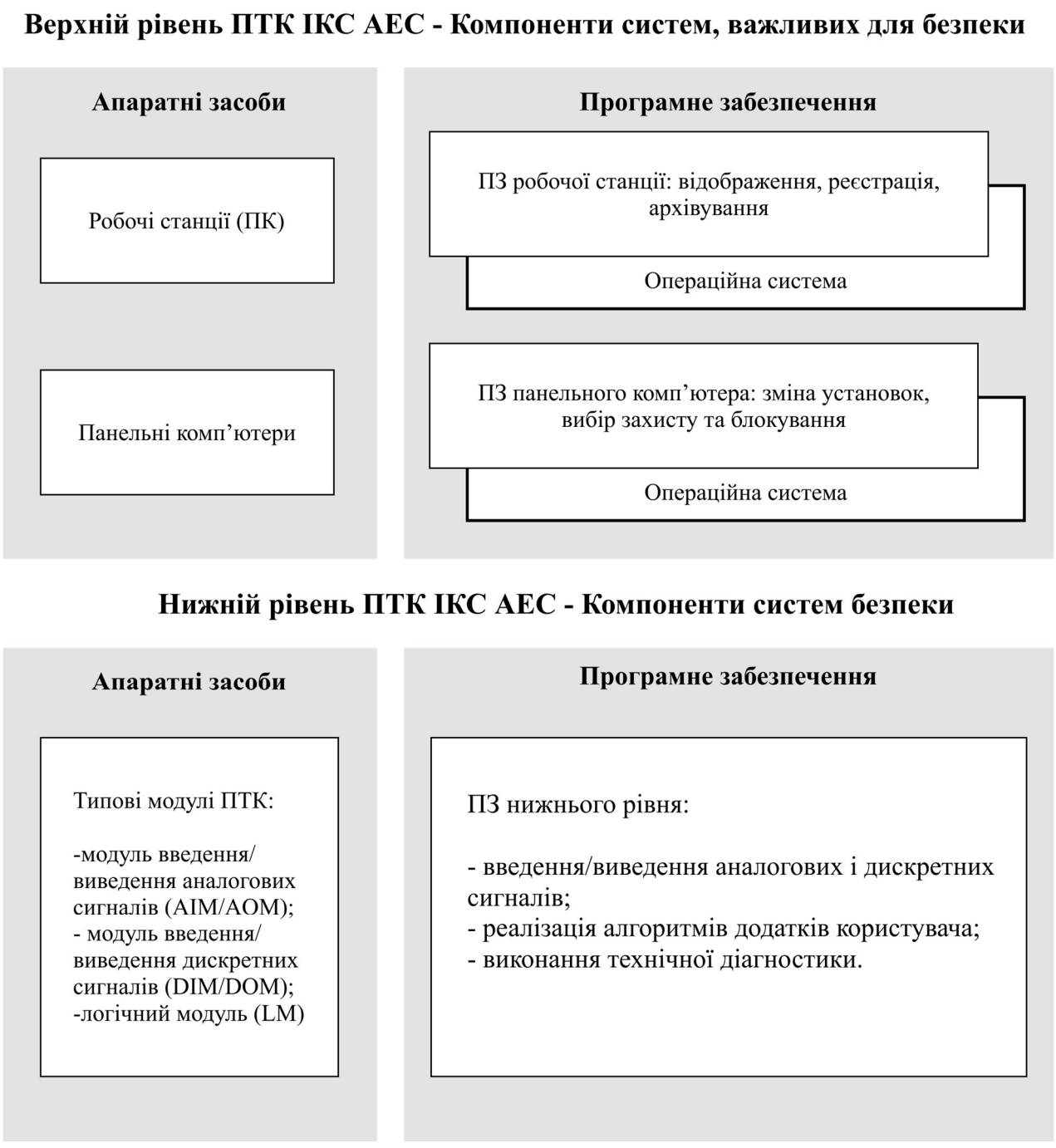


Рис.1.5 Узагальнена структура ПТК ІКС АЕС

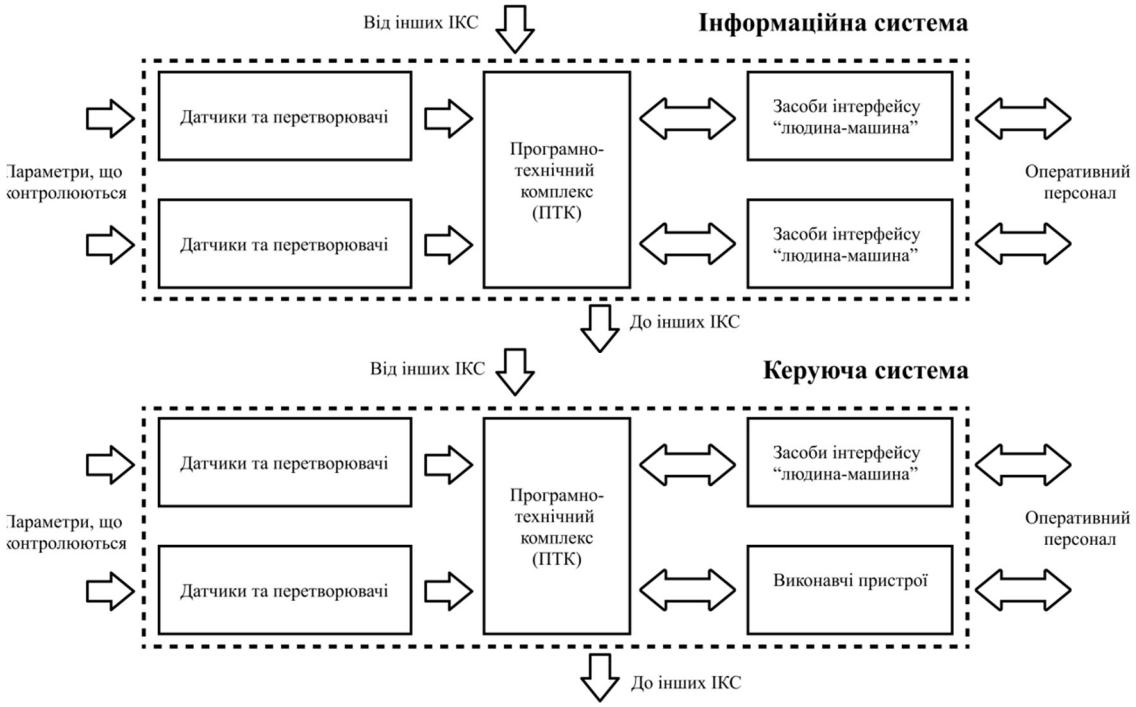


Рис.1.6 Узагальнена структура ІКС АЕС

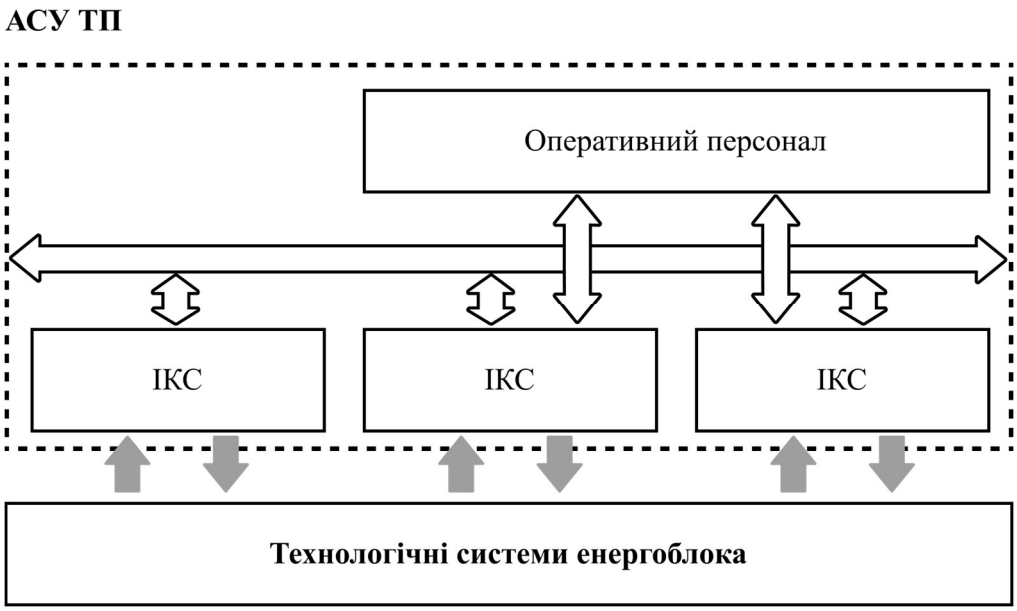


Рис.1.7 Узагальнена структура АСУ ТП АЕС

1.2 Огляд методів і засобів оцінювання надійності і функційної безпечності ІКС критичного використання

1.2.1 Структура науково-методичного апарату оцінювання та забезпечення надійності і функційної безпечності

Дослідження щодо питань оцінювання надійності та забезпечення технічної надійності і функційної безпечності систем досліджуваного класу виконуються провідними вітчизняними та іноземними вченими починаючи з середини минулого століття. Вітчизняні вчені Маліков І.М., Половко А.М., Романов М.А.. Чукреєв П.А., Сорін Я.М., Ушаков І.А., Гнеденко Б.В., Беляєв Ю.К., Соловйов А.Д та інш. сформували радянську школу технічної надійності [45,47 – 57]. Автори розробили основні поняття теорії надійності; поняття надійності елемента, який працює до першої відмови; поняття надійності відновлюваного елемента; поняття надійності системи. Було розроблено методи оцінки показників надійності: за результатами випробувань; перевірки гіпотез про надійність; резервованих систем з та без відновлення. Відомі роботи того періоду іноземних вчених Р. Барлоу та Ф. Прошана також присвячені розробленню основ математичної теорії надійності [46].

Великий вклад в розвиток логіко-ймовірнісного напрямку в теорії надійності, у зв’язку з необхідністю побудови адекватних моделей надійності багатоелементних систем, зробив Рябінін І. А. [58]. Черкесов Г.М. автор оригінальних праць з аналізу надійності систем з часовим резервуванням [59]. Герцбах І.Б. розробив фундаментальні моделі систем з профілактичним обслуговуванням [54, 55].

Важливою особливістю результатів розроблення та застосування методів оцінювання надійності технічних систем того періоду було урахування ними надійнісних характеристик лише апаратного забезпечення.

Розвиток обчислювальної техніки і відповідно зростання кількості сфер її

застосування викликало потребу рішення проблеми надійності програмного забезпечення, яке стало невід'ємної частиною багатьох систем. Рішення цієї проблеми стало предметом теорії надійності програмного забезпечення, як достатньо самостійної науки [141 – 150, 151, 153, 176 – 190, 192 – 225].

Переважно, розвиток цієї теорії грунтується на розробці моделей оцінки надійності програмних засобів (МНПЗ, за аглійською абревіатурою SRGM – Software Reliability Growth Model).

Детальний аналіз наукової та технічної літератури, виконаний Маєвським Д.А. та Колісник М.О. показав, що дослідження питання надійності ПЗ та розробки МНПЗ триває з 1956 року [186 – 188]. Дослідники зібрали і проаналізували сотні наукових статей, монографій та тез конференцій. В результаті було визначено, що за цей час розроблена велика кількість МНПЗ та існує ряд їх основних класифікацій, а саме Хетча, Гоела [154], Фатуєва [191], Благодатських [190], Полоннікова – Нікандрова [155].

Але умовно більшість МНПЗ можливо поділити на: емпірічні (наприклад, моделі прогнозу Холстеда, Мотлі і Брукса); статистичні (наприклад, вимірювальні моделі Нельсона, моделі, що базуються на природі вихідних даних); ймовірнісні (наприклад, експоненційні та Баєсовські моделі). Математичні методи, які використовують МНПЗ значною мірою визначаються їх назвою, а зокрема ними застосовуються математичні методи: теорії ймовірностей та математичної статистики; комбінаторного аналізу; елементи диференційного та інтегрального числення. Незважаючи на значний прогрес розвитку теорії надійності програмного забезпечення практичне застосування МНПЗ обмежується великою кількістю факторів, зокрема: необхідністю доказу відповідності обраної моделі із множини моделей класу програмного забезпечення, надійність якого має бути оцінена; значним обмеженням статистичного матеріалу, щодо результатів функціонування програмного забезпечення (статистика прояву дефектів та інш.); фактичною відсутністю врахування впливу надійності окремих компонент апаратних засобів на кінцевий результат роботи програми.

Огляд базових теорій науково-методичного апарату оцінювання та забезпечення надійності (Рис. 1.7) дозволяє сформулювати деякі висновки. По-перше, математичні методи оцінювання надійності технічних систем розроблялись базуючись на досягненнях математиків в частині розробки методів прикладної математики (теорії ймовірностей, математичної статистики та інш.). По-друге, найбільше практичне застосування на сьогодні знайшли наступні аналітичні методи аналізу і оцінювання надійності технічних систем:

− ймовірнісні методи, які використовують основні теореми теорії ймовірностей та комбінаторного аналізу. Дані методи реалізуються із використанням блок-схем надійності, функціональних схем та фазових діаграм;

− логіко-ймовірнісні методи. Дані методи реалізуються із використанням математичного апарата бінарної алгебри логіки та теорії ймовірностей;

− методи, які базуються на марковських випадкових процесах. Дані методи базуються на використанні понять теорії випадкових процесів, теорії графів, розв’язку рівняння або системи рівнянь Колмогорова-Чепмена.

За умови використання подібних показників в ході оцінювання функційної безпечності складних технічних систем, до яких відносяться ПТК ІКС дані методи можуть бути застосовані і для її оцінювання.

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 не можлива (наприклад, унеможливлено отримання ймовірнісних параметрів надійністної поведінки систем – ймовірностей переходу систем з одного стану в інші., інтенсивності відмов та інш.).

Результати аналізу сучасних базових теорій оцінювання надійності та математичних методів і моделей показав, що вони продовжують отримувати окремий розвиток. Окремо розвивається теорія надійності і відповідно науково-методичний апарат оцінювання надійності і функційної безпечності систем на

основі врахування надійнісних характерстик виключно апаратних компонент. І навпаки, теорія надійності програмного забезпечення, отримує розвиток, як окремий напрямок, з урахуванням надійнісних характеристик виключно програмних складових надійності без урахування того, що сучасні системи є інтегрованими програмно-апаратними системами.

Розвиток набору базових теорій перейшов в практичну площину через розробку і впровадження низки національних, державних та міжнародних стандартів з аналізу, оцінки та забезпечення надійності і функційної безпечності, вимоги яких в розрізі предемету дисертаційних досліджень частково проаналізовано в підрозділі 1.1.3.

Сучасний стан науково-методичного апарату, який частково описано та наведено на рисунку 1.8 значно розширено в ході досліджень і практичної діяльності наукової школи професора Харченка В.С.. Сучасний стан досліджень представниками цієї наукової школи та розроблених базових теорій вітчизняними та закордонними вченими, шляхи їх розвитку та очикуваний ефект за результатами даного дослідження наведено в таблиці 1.4.

1.2.3 Аналіз математичного апарату та обмежень використання існуючих методів та засобів оцінювання надійності і функційної безпечності

Вибір та обгрунтування математичного апарату досліджень має базуватись на результатах аналіза системи. ІКС ТККВ і зокрема їх ПТК є складними (багатокомпонентними) технічними системами.

Кількісному аналізу надійності та функційної безпечності системи передує якісний аналіз, який може бути здійснений дедуктивним (зверху вниз) або індуктивним (знизу вверх) методом. На практиці частіше застосовується ітеративний підхід, коли дедуктивний та індуктивний аналізи доповнюють один одного. Сучасні методи математичного моделювання, що застосовуються для проведення аналізу надійності та безпеки ІКС ТККВ, можливо поділити на три

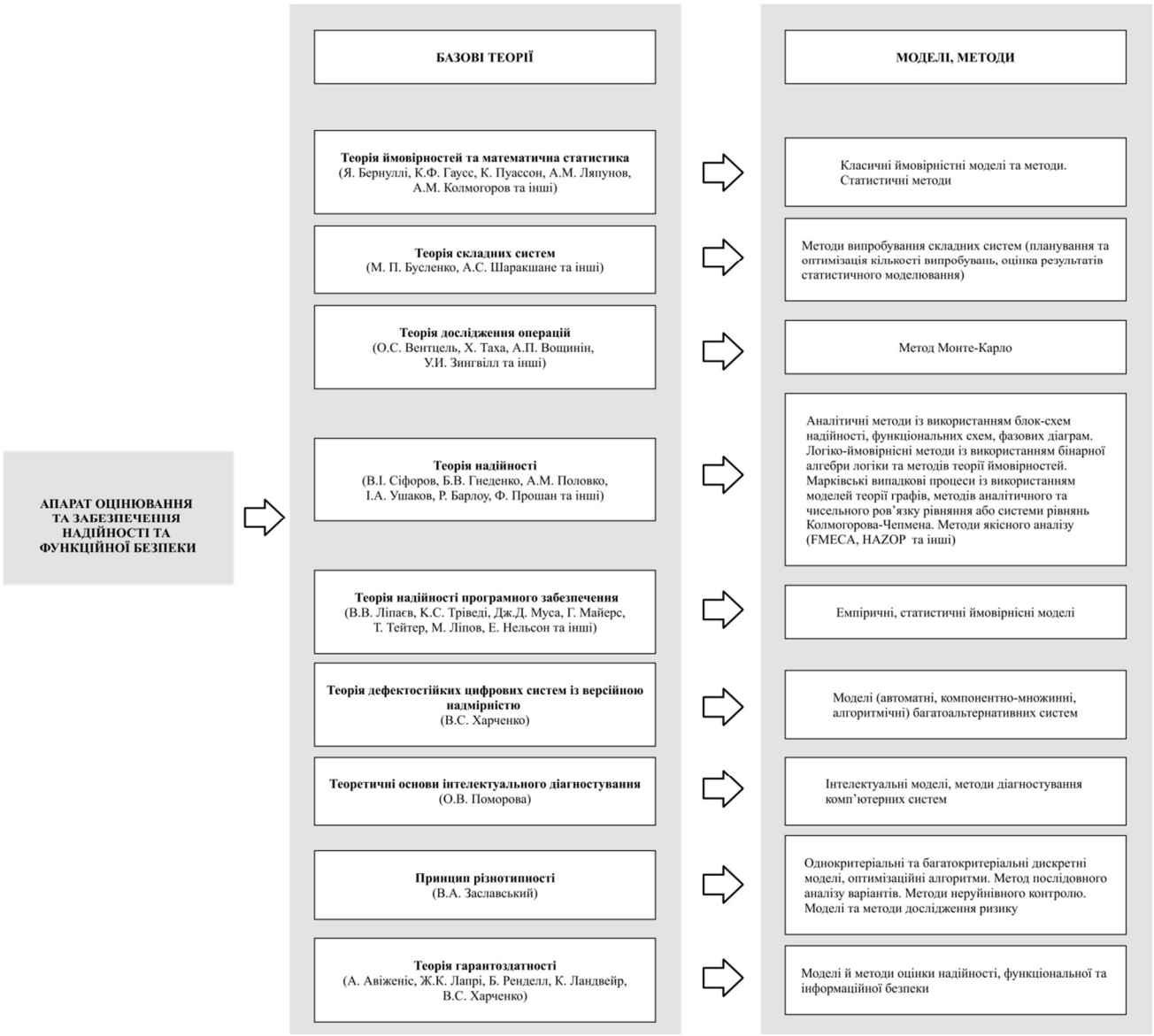


Рис. 1.8 Структура науково-методичного апарату оцінювання та забезпечення надійності і функційної безпечності

Таблиця 1.4.

Сучасний стан досліджень, шляхи розвитку и очикуваний ефект

Сучасний стан досліджень	Шляхи розвитку	Очикуваний стан (ефект)
ДД_ Харченко В.С. Гарантоздатність, багатоверсійні системи, показники гарантоздатності). Теоретичні основи дефектостійких цифрових систем систем (теоертичні основи побудови багатоальтернативних ситем, базові архітектури багатоальтернативних ситем). Врахування АК та ПК, ДФ ДП.	Врахування в ході оцінки та забезпечення НіФБ розширених множин компонент МК, дефектів МД, множини змінних параметрів МЗП.	Моделі та методи оцінювання та забезпечення НіФБ, які враховують розширені множини компонент МК, дефектів МД, множини змінних параметрів МІЗ. Підвищення точності оцінювання НіФБ.
ДД_ Скляр В.В. Методологія і інформаційні технології забезпечення функціональної безпеки інформаційно-керуючих систем	Врахування в ході оцінки та забезпечення НіФБ розширених множин компонент МК, дефектів МД, множини змінних параметрів МЗП, особливостей оцінювання та забезпечення НіФБ за умови не ідеальності засобів контролю та діагностування. Розширення простору станів системи (введення поняття інформаційно-технічного стану (ІТС)).	Моделі та методи оцінювання та забезпечення НіФБ, які враховують розширені множини компонент МК, дефектів МД, множини змінних параметрів МІЗ. Моделі оцінювання НіФБ ПТК на самодіагностованих платформах. Підвищення точності оцінки НіФБ та можливість висунення вимог до засобів контролю та діагностування.
ДД_Поморова О.В. Теоретичні основи інтелектуального діагностування	Інтелектуальні моделі, методи діагностування комп’ютерних систем	Моделі, методи процедури оцінювання НіФБ і процедури верифікації і валідації ПТК та їх компонент, які дозволяють підвищити точність оцінок, сформулювати рекомендації щодо їх архітектурної побудови і визначити рівень повнити безпеки за вимогами державних і міжнародних стандартів

Продовження таблиці 1.4.

ДД_Брежнєв Е.В. Методологія забезпечення безпеки критичних енергетичних інфраструктур	Методи підвищення точності оцінок (інтеграція та уточнення моделей безпеки)	Моделі, методи процедури оцінювання і забезпечення надійності і функційної безпечності ПТК , які дозволяють підвищити точність оцінок за рахунок комплексного урахування впливу на досліджувані властивості надійнісних характеристик апаратних і програмних компонент
КД_Токарєв В.І., Головир В.О. , Герасименко А.Д. , Білий Ю.О. Мультдиверсність для ІКС на ПЛІС.	Врахування в ході оцінки та забезпечення НіФБ розширених множин компонент МК, дефектів МД, множини змінних параметрів МЗП з урахуванням мультдиверсності при проектуванні ПТК на ПЛІС.	Моделі та методи оцінювання та забезпечення НіФБ, які враховують розширені множини компонент МК, дефектів МД, множини змінних параметрів МІЗ з урахуванням мультдиверсності при проектуванні ПТК на ПЛІС і відповідно . підвищення точності оцінювання НіФБ мультидиверсних ПТК.

Продовження таблиці 1.4.

КД_Неткачева Є. І., Орєхова А.А., Бутенко В.О. Формальні методи, інформаційні технології вибору інструментальних засобів для оцінювання готовності ІКС із використанням марківських моделей.	Застосування вибору інструментальних засобів в ході оцінки НіФБ за умови врахування розширених множин компонент МК, дефектів МД, множини змінних параметрів МЗП та особливостей оцінювання та забезпечення НіФБ за умови не ідеальності засобів контролю та діагностування.	Методи оцінювання та забезпечення НіФБ, які враховують розширені множини компонент МК, дефектів МД, множини змінних параметрів МІЗ з урахуванням мультдиверсності при проектуванні ПТК на ПЛІС і відповідно . підвищення точності оцінювання ПТК
КД_Поночовний Ю.Л. , Одарущенко О.Б., Руденко О.А. Дефекти взаємодії, моделювання відмовостійких комп'ютерних систем з урахуванням зміни параметрів потоків відмов та відновлень ПЗ, урахування вторинних дефектів ПЗ.	Врахування розширеної МД, що змінюються в ході реалізації етапів життєвого циклу програмних та апаратних компонент ПТК, врахування вторинних дефектів ПЗ.	Модифіковані моделі і нові методи, які враховують розширену МД, що змінюються в ході реалізації етапів життєвого циклу програмних та апаратних компонент ПТК, врахування вторинних дефектів ПЗ НіФБ. Підвищення адекватності розроблених моделей і методів на основі врахування розширених МД, МК, МЗП, що дозволяє досліджувати обрані показники НіФБ з додаткових сторін і додатковим ступенем деталізації.

Продовження таблиці 1.4.

КД_Дужий В.І., Тарасюк О.М., Гордєєв О.О. Моделі якості і засів-технології для ПЗ.	Реалізація внесення дефектів на різних рівнях апаратної та програмної компонент при проєктуванні та тестуванні ПТК і їх компонент на ПЛІС.	Модифіковані процедури внесення дефектів на різних рівнях апаратних та програмних компонент ПТК на ПЛІС, методи верифікації і валідації ПТК на програмовних самодіагностовних платформах, які дозволяють виконати тестування АК, ПК ПТК для визначення рівня НіФБ за вимогами державних та національних стандартів.
Теорія надійності програмного забезпечення (Ліпаєв В.В., K.S. Trivedi, J.D.Musa, Майерс Г., Тейер Т., Липов М., Нельсон Э.та інш.)	Застосування моделей і методів оцінювання надійності програмних засобів	Модифіковані моделі надійності програмних засобів, процедура оцінювання надійності програмних засобів, які дозволяють одержувати кількісні значення параметрів що характеризують надійність ПК ПТК, які в свою чергу дозволяють розширити перелік МД. МК при оцінюванні НіФБ ПТК

категорії: аналітичні; імітаційні; гібридні [228]. Аналітичні методи можна умовно поділити на дві групи: комбінаторні й просторові. Найбільш відомими методіами є метод діагностування дерева відмов (англ.FTA - Fault-tree analysis) та аналіз за допомогою блок-схем надійності (англ. RBD - reliability-block diagram). Метод діагностування дерева відмов є дедуктивним методом аналізу за допомогою якого визначають та аналізують умови й фактори, які призводять до виникнення небажаної події або сприяють цьому, а також значно впливають на характеристики системи, безпеку, економічність та інші показники. Метод блок-схем надійності дає змогу визначити шляхи сприятливого стану системи по тому, як зв'язані та впливають один на одного її елементи систем та підсистеми. Класифікація методів математичного моделювання, які застосовуються для аналізу надійності та безпеки (безпечності) із трасуванням їх до відповідних державних та міжнародних стандартів наведено в таблиці 1.5.

Застосування методів математичного моделювання в процесі оцінювання надійності та безпеки (безпечності) ІКС характеризується наявністю певних ризиків:

– відхилення точності оцінок – недооцінка або переоцінювання показників, що призводе до помилок в ході прийняття рішень щодо системи, яка розробляється та оцінюється;

– використання надмірних ресурсів – неприйнятні обсяги часового й обчислювального ресурсів [243].

Одними з найбільш поширених просторових методів аналізу є марковський аналіз [38, 39], а також аналіз за допомогою стохастичних мереж Петрі.

Марковський аналіз – це переважно індуктивний метод аналізу, який ґрунтується на теорії марковських процесів (МП) і використовується для оцінювання функціонально складних систем і стратегій технічного обслуговування й ремонту. Аналіз із допомогою стохастичних мереж Петрі є індуктивним методом, що дає змогу гнучко моделювати динамічні дискретні

Таблиця 1.5

Класифікація методів математичного моделювання для аналізу безпеки та надійності ІКС

<table>
<tr><th>Метод</th><th>Підхід</th><th>Приклад</th><th colspan="4">Стандарт (-и)</th></tr>
<tr><td rowspan="4">Анатіличний</td><td rowspan="2">Непросторові моделі (Boolean approach, Non-state space)</td><td>Аналіз діагностування дерева відмов (Fault-tree analysis)</td><td>ДСТУ 2861-94</td><td>ГОСТ Р 27.302</td><td>IEC 61025</td><td>IEC 61508</td></tr>
<tr><td>Аналіз за допомогою блок-схем надійності (reliability-block diagram)</td><td>ДСТУ 2861-94</td><td>ГОСТ 5190.5</td><td>IEC 61078</td><td>IEC 61508</td></tr>
<tr><td rowspan="2">Просторові моделі (state/transition approach, state space)</td><td>Марковський аналіз (Markovian approach)</td><td>ДСТУ 2861-94</td><td>ГОСТ 5190.5</td><td>IEC 61165</td><td>IEC 61508</td></tr>
<tr><td>Аналіз за допомогою стохастичних мереж Петрі (petri nets, place-transition nets)</td><td>ГОСТ 5190.5</td><td>ГОСТ 50779.10</td><td colspan="2">IEC 61508</td></tr>
<tr><td colspan="3">Імітаційний (discrete-event simulation)</td><td>ДСТУ 2861-94</td><td>ГОСТ 50779.10</td><td colspan="2">IEC 61508</td></tr>
<tr><td colspan="3">Гібридний (Hybrid)</td><td colspan="4">IEC 61508</td></tr>
</table>

системи, зберігаючи в допустимих розмірах простір станів моделі й застосовуючи метод Монте-Карло для розрахунку необхідних значень.

Базовою перевагою просторових моделей над комбінаторними є їхня гнучкість у поданні таких важливих особливостей об'єкта, як використання «гарячого» резерву, неповне покриття виявленого дефекту, різні типи відмов, особливості стратегій технічного обслуговування тощо [314].

Імітаційне моделювання – метод, що дає змогу аналізувати безпеку та надійність системи шляхом побудови моделі, максимально близької до оригіналу, яка описує процеси так, як вони проходили б насправді. Перевагою цього підходу є високий ступінь деталізації поведінки системи, і, як наслідок, тривалий час розрахунку необхідних показників, який при реалізації високонавантаженого проекту може становити декілька днів [320]. Необхідно зазначити, що на дослідження аналітичних моделей витрачається значно менше часу порівняно з імітаційними моделями, однак застосування аналітичних моделей, у свою чергу, обмежується складністю систем.

Гібридне моделювання є методом, що дає змогу «ієрархічно» комбінувати непросторові моделі з просторовими, або аналітичні підходи з імітаційними і таким чином використовувати переваги обох підходів [9]. Необхідно зазначити, що на цей час немає стандартизованих вимог до застосування гібридного моделювання.

Аналіз резервованих програмно-апаратних структур ІКС ТККВ та ПТК, що входять до їх складу та особливості їх застосування дозволяють віднести їх до систем, що є самодіагностовними, резервованими та відновлюваними. Найбільш широке використання, із наведених математичних методів моделювання, для оцінювання безпеки (безпечності) та надійності ІКС ТККВ та зокрема їх ПТК зі складною резервованою структурою з урахуванням параметрів відмов і відновлень АЗ і ПЗ, набули методи марковського аналізу, які було обрано базовими для виконання досліджень [80, 169, 235, 237, 249, 250, 255]. Відповідно до шостої частини стандарту IEC 61508 саме базова властивість марковського процесу є допоміжною під час розрахунку показників функційної безпечності [9]. Однак припущення, що зумовлюють застосування теорії марковських випадкових процесів, можуть не відповідати реальному процесу функціонування ІКС. Це потребує додаткових заходів в ході обґрунтування апарату досліджень.

У випадку застосування марковського апарату дослідження ПТК ІКС для оцінювання надійності виконується низка процедур, що включають наступні етапи [240, 241, 245, 246 – 250, 252 – 263, 266, 287].

1. Аналіз архітектури досліджуваного ПТК, його структурної схеми надійності (ССН) з урахуванням різних типів дефектів АЗ і ПЗ, процедур відновлення при відмовах.

2. Визначення підмножин станів системи на основі комбінацій справних і несправних, безпечних і небезпечних станів її елементів, станів відновлення і обслуговування.

3. Визначення кількісних значень початкових параметрів моделі на підставі відомих і розроблених методів, а також прийнятих припущень. Побудова розміченого графа станів і переходів системи.

5. Розробка і дослідження системи диференційних рівнянь (СДР) Колмогорова-Чепмена, отримання кількісних значень ймовірностей перебування системи в кожному з стані. Визначення кількісних значень комплексних показників надійності (наприклад функцій готовності та оперативної готовності). Визначення показників функційної безпечності.

У процесі використання апарату марковського аналізу перед дослідником постають наступні обчислювальні труднощі: зростання простору станів, розрідженість матриці інтенсивностей переходів між станами марковської моделі (ММ) і її жорсткістю [255].

Оскільки однією з головних вимог у процесі оцінювання надійності ПТК ІКС є забезпечення високої точності результатів, необхідно враховувати кожну особливість апарату марковського аналізу на всіх етапах оцінювання надійності та функційної безпечності систем. Ці особливості є наступними.

Збільшення простору станів є наслідком підвищення рівня деталізації марковської моделі функціонування резервованого ПТК, а жорсткість, є властивістю моделі, яка призводить до значних труднощів у разі її числового розв’язання. Жорсткість СДУ виникає за умови великої кількісної різниці між параметрами моделі. Наявність жорсткості вихідної моделі рооявляється в нестійкості отриманого числового розв’язку СДУ і призводе до необхідності зменшення кроку інтегрування, що на значних часових інтервалах дослідження дає неприпустимо високу локальну похибку розв’язання [134].

Наслідком збільшення простору станів є підвищення розрідженості матриці інтенсивностей переходів між станами. Аналіз робіт [149, 212, 221, 226, 230, 231] показав, що з метою економії обчислювального й часового ресурсів у процесі знаходження числових розв’язків необхідно використовувати спеціальні алгоритми для компактного зберігання великих розріджених матриць.

Процес застосування апарату марковського аналізу і його обмежень для оцінювання надійності і функційної безпечності ПТК ІКС можна зобразити у

вигляді шести послідовних фаз (Рис. 1.8): опис модельованої системи, складання простору станів, методологічної, інструментальної й верифікаційної фази, і фази аналізу результатів. Всі етапи мають свої особливості (обмеження), на яких дослідник повинен акцентувати увагу в разі застосування вибраного математичного апарату.

Необхідно зазначити, що, оскільки марковьский аналіз широко подано в нормативних документах, попередження про перелічені обчислювальні складнощі мають бути наведені в їх описовій частині, у якій також наводяться відповідні вимоги й рекомендації щодо проходження проблемних етапів моделювання.

Проаналізуємо детально кожну із фаз процесу застосування апарату марковського моделювання, відповідні типові особливості, а також трасування в стандартах IEC 60300–3–1:2003 «Dependability management. Part 3–1: Application guide – Analysis techniques for dependability – Guide on methodology» [14], IEC 61165:2008 «Application of Markov techniques» [15] і IEC 61508:2010 «Functional safety of electrical/electronic/electronic programmable safety–related systems» [8].

На першій фазі здійснюється: вербальний опис системи, що моделюється; уведення й обґрунтування основних припущень, визначення мети моделювання, а також часового інтервалу дослідження. У таблиці 1.6 наведено найбільш типові особливості цього етапу, а також їх відображення в стандартах.

На другій фазі визначають параметри моделі, базуючись на статистичних даних, отриманих на етапах верифікації й валідації розроблюваної системи, або використовуючи доступні відповідні бази даних. Проводять генерацію простору станів і складання переходів між ними з використанням припущень, прийнятих на попередньому етапі. Типові особливості фази складання простору станів, а також їх трасування в стандартах наведено в таблиці 1.7.

Протягом методологічної фази дослідник здійснює вибір підходу й методу дослідження отриманої ММ. Усі методи дослідження ММ можна поділити на дві групи: прямі підходи і підходи перетворення моделей (або

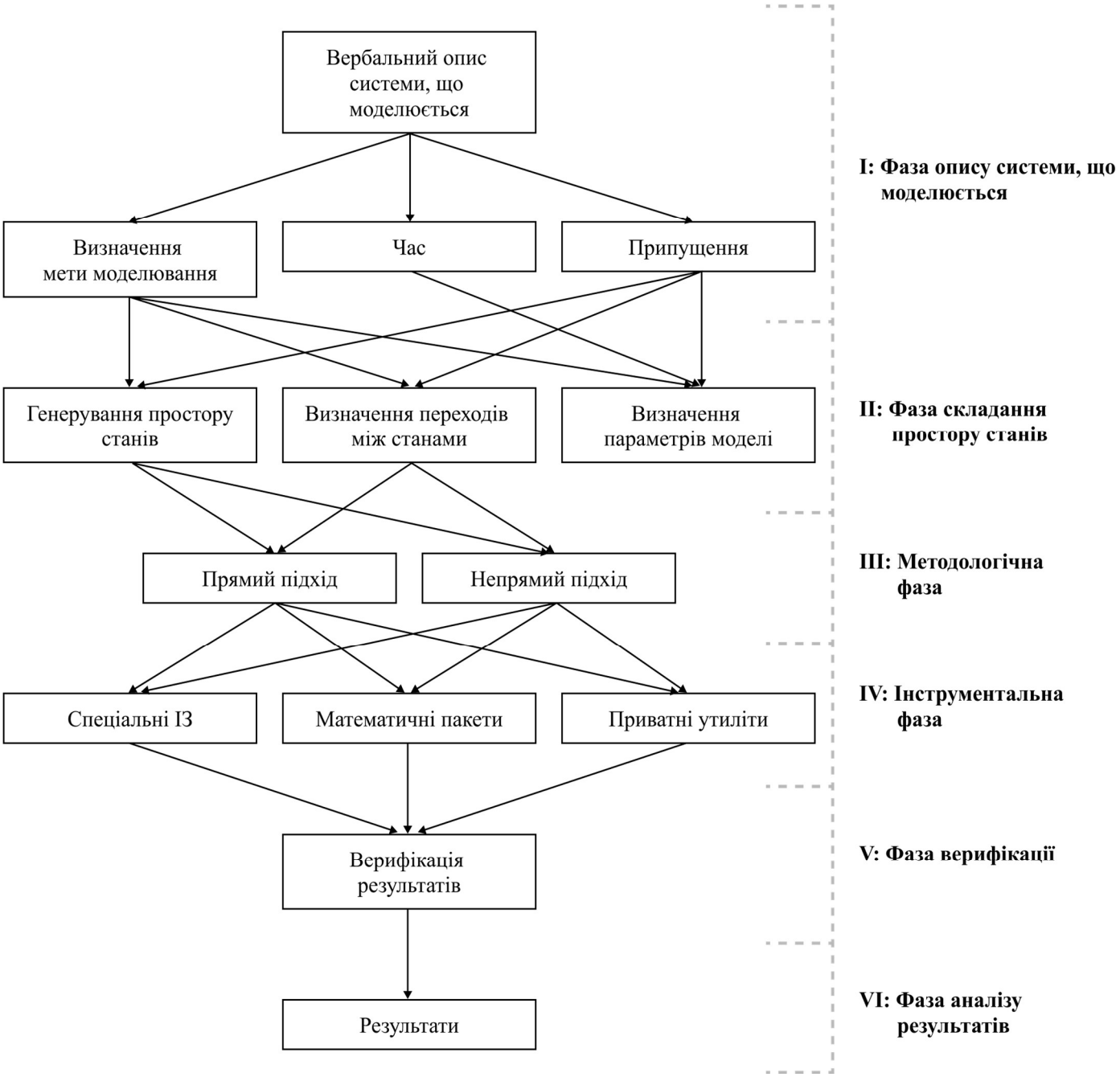


Рис. 1.8 Фази процесу застосування апарату марковського аналізу

*Таблиця 1.*6

Фаза опису системи, що моделюється

№ п/п	Особливість	Опис у стандарті
1	Підтвердження придатності апарату марковського аналізу для досліджуваної системи	**IEC 60300–3–1** “…вибір методу аналізу надійності є індивідуальним і здійснюється спільними зусиллями розробників системи й експертів в області надійності…”
2	Уведення реалістичних припущень, що дає змогу зберегти необхідний рівень абстрактності моделі відносно досліджуваних параметрів	Базові припущення при використанні апарату марковського аналізу подано в стандартах IEC 61165, частина 6 і IEC 61508 – 6, частина B. 5.2

Таблиця 1.7

Фаза складання простору станів

№ п/п	**Особливість**	**Опис у стандарті**
1	Опис повного простору станів моделі, що призводить до експоненціального зростання її розмірності	**IEC 61508–6** “…Базовою проблемою застосування марковських моделей є експоненціальне зростання простору станів з підвищенням рівня деталізації системи…” **IEC 60300–3–1** “…урахування додаткових компонентів системи призводить до експоненційного зростання простору станів моделі й ускладнює її аналіз…”
2	Коректний аналіз статистичних даних із метою визначення параметрів досліджуваної системи	Детальний опис, вимоги й рекомендації щодо проходження цього етапу наведено в IEC 61508, частини 6 і 7

непрямі). Перший вид характеризується застосуванням стійких числових методів для знаходження як стаціонарних, так і перехідних імовірностей, а також використанням спеціальних структур для зберігання великих розріджених матриць. Основою непрямого підходу є ідея перетворення вихідної ММ шляхом дослідження її структури й укрупнення станів, що призводить до зниження жорсткості й розмірності. Проведені раніше дослідження [77, 131, 225, 245, 247, 258] показали: якщо отримана марковська модель є дуже жорсткою, дуже розрідженою, а також має велику розмірність,

то ретельний вибір підходу й методу дослідження є важливим етапом у процесі досягнення точних результатів оцінювання.

Базові складнощі методологічної фази наведено в таблиці 1.8.

Необхідно звернути увагу на певну невідповідність вимог до процесу дослідження ММ, наведених у стандартах IEC 61508 – 6 і IEC 61165 у той час як у стандарті IEC 61508 – 6 стверджується, що дослідник повинен фокусуватися тільки на побудові моделі, а не на наступних етапах (застосування пакетів комп'ютерної математики), у стандарті IEC 61165 акцентується увага на тому, що для дослідження ММ потребується допомога експертів в області прикладної математики.

Протягом інструментальної фази дослідник застосовує вибраний (вибрані) підхід і метод дослідження ММ у певному інструментальному засобі (ІЗ). За останні 30 років було розроблено множину ІЗ, що реалізують кожний із перелічених підходів. Усі ці ІЗ можна поділити на три групи: спеціалізовані ІЗ (λPredict, Möbius, SHARP), комерційні математичні пакети (Maple, Matlab, Mathematica) та ІЗ приватного розроблення (MSMC, ExpMeth, ASNA, MARCA), тобто утиліти, розроблені користувачами для вирішення вузькоспеціалізованих завдань, які пройшли перевірку [254]. Така різноманітність ІЗ є надзвичайно корисною в процесі оцінювання системи, однак може спричинити значні складнощі під час вибору ІЗ, найбільш придатного для розв’язання конкретної задачі з огляду на точність і зручність використання.

Протягом верифікаційної фази дослідник проводить перевірку точності отриманих числових результатів дослідження (таблиця 1.10). Необхідно зазначити, що у наведених стандартах описується класичний ручний метод перевірки результатів. Однак для роботи з великими ММ цей підхід є практично непридатним, тому в процесі перевірки результатів слід використовувати інші підходи або ІЗ.

Таким чином, формування й урахування жорсткості, розрідженості й розмірності ММ відбувається на фазі складання простору станів, методологічній та інструментальній фазах.

Таблиця 1.8

Методологічна фаза

№ п/п	Особливість	Опис у стандарті
1	Вибір методу аналізу за критеріями його застосування, точності й достовірності отриманих результатів	**IEC 61508–7** "…однорідний ланцюг Маркова є простою системою лінійних диференціальних рівнянь зі сталими коефіцієнтами. Шляхи аналізу цих моделей, а також ефективні алгоритми їх розв'язання було давно проаналізовано й розроблено.…"
2	Вибір методу дослідження моделі, що базується на аналізі властивостей жорсткості, розмірності й розрідженості, має значний вплив на процес розв'язання й точність отриманих результатів.	**IEC 61508–6** "…ефективні алгоритми розв'язання цих рівнянь давно було розроблено й впроваджено в ІЗ, тому досліднику необхідно акцентувати увагу на побудові моделі, а не на відповідній математиці…" **IEC 61165** "…розрахункові методи можуть бути досить складними й можуть потребувати застосування спеціальних ІЗ і допомоги експертів в області прикладної математики…"

Таблиця 1.9

Інструментальна фаза

№ п/п	Особливість	Опис у стандарті
1	Вибір ефективного ІЗ відповідно до використовуваного методу розв'язання	**IEC 61508–6** "…у разі застосування програмного продукту в процесі дослідження системи, практик повинен мати чітке розуміння, які техніки впроваджено в ІЗ і що вони повністю відповідають розв'язанню цієї задачі…"
2.	Сумісність із іншими ІЗ з метою перевірки отриманих числових результатів	**IEC 60300–3–1** "…продуктивність ІЗ. Чи є ІЗ зручними для користувача? Чи вони мають спільний інтерфейс з іншими ІЗ для підтримки опції передачі вихідних та отриманих даних для їх повторного використання…"

Таблиця 1.10

Фаза верифікації

№ п/п	Особливість	Опис у стандарті
1	Верифікація результатів досліджень	**IEC 61508–6** "… дослідник також повинен провести перевірку отриманих результатів із допомогою ручних обчислень…" **IEC 60300–3–1** "…перевірка достовірності. Чи ми можемо перевірити результати ручним способом? Якщо ні, то чи є ІЗ зручним для користувача?…"

Таким чином, формування й урахування жорсткості, розрідженості й розмірності ММ відбувається на фазі складання простору станів, методологічній та інструментальній фазах.

Особливості кожної з проаналізованих фаз значно впливають на процеси побудови, аналізу, розв'язання й перевірки отриманих результатів.

Необхідно зазначити, що базові ризики методологічного етапу описано в стандартах не в повному обсязі, що створює додаткові труднощі й неточності в процесі вибору й застосування різних підходів дослідження моделей і відповідних ІЗ. Для вибору підходу й методу дослідження ММ необхідно провести аналіз переваг і недоліків, а також умов застосування прямого підходу дослідження ММ і підходу перетворення ММ.

1.2.4 Засоби оцінювання надійності і функційної безпечності

До прямого підходу дослідження ММ (англ. direct research approach (DR), tolerance approach) належать числові методи (ЧМ) які можуть бути застосовані для отримання як стаціонарних, так і перехідних імовірностей перебування системи в кожному стані протягом певного інтервалу часу. З огляду на розрахунок стаціонарних або перехідних імовірностей, а також з урахуванням жорсткості, прямі ЧМ можна поділити на чотири групи.

а) прямі методи розв'язання систем лінійних алгебраїчних рівнянь (СЛАР). Найбільш поширеними представниками цієї групи є метод Гауса й

алгоритм Грасмана [301]. Також іноземні фахівці часто використовують алгоритм Грасмана – Таксара – Хеймана, який є модифікацією вихідного алгоритму Грасмана [302].

б) прямі методи розв'язання систем диференціальних рівнянь (СДР) Колмогорова – Чепмена. На початковому етапі роботи проводиться розбиття часового інтервалу досліджень $T = [0; t]$ на скінченну множину $\{t_1, t_2, ..., t_i, ... t_n\}$.

Залежно від процесу розв’язання, ці методи можна поділити на два базові типи – явні й неявні ЧМ. У випадку явних методів розв’язок СДР $P(t_i)$ апроксимується відносно значення $P(t_j)$ для $j<i$. Широко відомими прикладами ЧМ цього типу є метод Рунге – Кутта n-го порядку точності й метод Дженсена [134, 301]. Явні методи широко застосовуються для розв’язання нежорстких СДР.

в) прямі методи розв'язання жорстких СДР (ЖСДР) Колмогорова – Чепмена (неявні методи). Для розв’язання жорстких СДР найчастіше рекомендується [303] використання стійких неявних ЧМ, що апроксимують розв’язок СДР $P(t_i)$ відносно $P(t_j)$ для $j \leq i$. Прикладами ЧМ цього класу є неявний метод Рунге – Кутта, TR-BDF2, неявний метод Гіра [134]. Також до методів розв’язання ЖСДР відносять метод Розенброка й експоненціальний.

Необхідно зазначити, що у випадку розв’язання ЖСДР із високою й надвисокою жорсткістю необхідно проводити додаткову перевірку отриманих імовірнісних значень. Більшість методів цієї групи реалізовано у вигляді функцій, вбудованих у широко відомі математичні пакети MATLAB, Mathematica, MathCad і Maple.

г) модифіковані методи розв'язання ЖСДР Колмогорова – Чепмена. Прикладами таких методів є модифікований експоненціальний метод [236] і модифікований метод Дженсена [239], де було впроваджено автоматичний підбір кроку інтегрування з метою збереження стійкості отриманого розв’язку під час дослідження ЖСДР із високою й надвисокою жорсткістю.

ЧМ, що належать до прямого підходу розв’язання, дають можливість знаходити результати із заданою точністю, але для цього дослідник повинен проводити контроль таких типових помилок, як похибки округлення, методу, вихідних даних, скорочення і т. д. Ці методи широко впроваджено у відомих ПКМ, що робить їх доступними для застосування.

Проте у випадку розв’язання великих розріджених марковських моделей застосування цих методів може значно ускладнитися через необхідність уведення й оброблення спеціальних схем зберігання матриці коефіцієнтів СДР. Для розв’зку цієї проблеми застосовують підхід до перетворення марковських моделей.

Основою підходу до перетворення ММ (англ. Indirect Research Approach (IDR), avoidance approach) є вивчення структурних властивостей вихідної ММ із метою вилучення або укрупнення груп станів. Методи, що належать до цього підходу, можна класифікувати таким чином.

а) методи перетворення великих ММ (англ. largeness–avoidance techniques). Базовою ідеєю роботи є початкове уникнення проведення розрахунків над великою ММ. Методи цього класу ґрунтуються на двох принципах роботи й застосовуються як самостійно, так і в групі.

Якщо ММ було сформовано на основі високорівневого формалізму (SAN, PTN) [304], то проводиться аналіз високорівневої структури з метою її укрупнення або скорочення допустимих елементів. Таким чином відбувається значне скорочення простору станів вихідної ММ. У закордонній літературі ці методи називають «model–level lumping technique» [305]. Принцип роботи другої групи методів полягає в дослідженні простору станів уже згенерованої (побудованої) ММ із метою вилучення станів, що мають мізерну ймовірність (менше 10^{-8}), або укрупнення груп станів. У з закордонній літературі ці методи носять назву «state–level lumping technique» [306].

б) методи перетворення жорстких ММ (англ. stiffness–avoidance techniques). Одним із найбільш відомих є метод агрегування-дезагрегування,

розроблений ученими К. С. Тріведі, А. Боббіо і А. Рейбманом [307]. Цей метод базується на визначенні станів, які породжують жорсткість у досліджуваній моделі, їх вилученні, обробленні й укрупненні. Результатом роботи алгоритму є нежорстка ММ зі значно меншим простором станів.

Методи, які базуються на перетвореній моделі, дають змогу знаходити потрібні ймовірнісні значення для ММ, що налічують десятки тисяч станів, у той час, як прямі підходи практично неможливо застосувати для розв'язання задач такої розмірності. Необхідно зазначити, що на цей час проводяться дослідження впливу на точність отриманих результатів укрупнення й скорочення простору станів. У роботі [307] автори наводять інформацію, отриману на основі перевірки правильності розв’язання багатьох ММ, і стверджують, що метод агрегування-дезагрегування дає змогу отримати результати з точністю $\varepsilon=10^{-6}$. Алгоритми, що реалізують ці методи, часто мають високу складність, а це, у свою чергу, безпосередньо впливає на час роботи алгоритму.

Кожний із перелічених підходів було впроваджено у багатьох ІЗ, які можна поділити на три групи: спеціалізовані ІЗ (λPredict, Мебіуса, SHARP), комерційні математичні пакети (Maple, Matlab, Mathematica) та ІЗ приватного розроблення (MSMC, ExpMeth, ASNA, MARCA).

Більшість спеціалізованих ІЗ реалізують прямий підхід дослідження ММ. Такі ІЗ, як SHARP і Möbius, також підтримують опцію використання методу агрегування-дезагрегування (SHARP), підходу укрупнення моделі «model–level lumping technique» та укрупнення станів «state–level lumping technique». Необхідно зазначити, що для роботи з ІЗ Möbius дослідник має апріорно подати модель системи з допомогою високорівневого формалізму SAN, після чого згенерувати її з використанням вбудованого алгоритму. Таким чином, відповідно до вимог, наведених у таблиці 1.5, для роботи з Möbius дослідник повинен мати досвід побудови моделей SAN і розуміти процес генерування моделі. Більшість спеціалізованих ІЗ підтримують опцію генерації електронних звітів, однак мають обмежений функціонал для експортування отриманої ММ

або матриці коефіцієнтів СДР, що значно ускладнює процес перевірки отриманих значень.

Серед комерційних математичних пакетів широко застосовуються методи, що належать до прямого підходу дослідження ММ (DR). Такі пакети комп'ютерної математики (ПКМ), як MATLAB і Mathematica є також середовищами програмування, завдяки чому користувачі мають можливість розробляти й використовувати числові алгоритми власної реалізації, а також обмінюватися ними, а це значно розширює базовий функціонал даних ПКМ. Проте в цьому випадку виникають проблеми щодо якості реалізації цих алгоритмів, а отже, рівня довіри до отриманих результатів.

Стандартні функції ПКМ, що реалізують ЧМ, містять від п'яти до восьми необхідних аргументів, у числі яких – СДР і матриця коефіцієнтів, складання яких при роботі з великими ММ стає практично неможливим. Як і у випадку зі спеціалізованими ІЗ, для ПКМ характерними є проблеми з експортуванням вихідних даних для інших ІЗ.

Алгоритм вибору і застосування комерційних та користувацьких пакетів комп’ютерної математики та експериментальне дослідження цього алгоритму детально розроблено та описано в роботі [318]. Даний алгоритм дозволяє врахувати наведені вище властивості марковських моделей (жорсткість, розрідженість, розмірність), обрати прямий чи непрямий підхід розв’язання системи диференційних рівнянь, обрати інструментальний засіб, одержати результати обчислень із необхідної точністю та виконати аналіз результатів обчислень.

1.3 Обгрунтування і вибір показників надійності та функційної безпечності

Показники надійності ПТК ІКС обираються у відповідності із класифікацією виконуваних системою функцій за часовим режимом (дискретним або неперервним) їх виконання з урахуванням видів та критеріїв відмов.

Такими показниками є одиничні та комплексні показники, що

характеризують наступні властивості обладнання та систем в цілому: безвідмовність; довговічність; ремонтопридатність. Для окремих видів обладнання додатково встановлюється властивість збереженість. Номенклатура показників надійності енергоблоків, систем і обладнання АЕС, до якого відносяться ПТК АЕС наведено в таблиці 1.10 [309]

За умови, коли кількісні значення показників є близькими до одиниці можливо використання показників, які є їх доповненням до одиниці, тобто:
1- $К_г$, 1- $К_{ог}$, 1- $Р_{св}$, 1- $Р_{осв}$, які відповідно мають назву коефіцієнтів неготовності, коефіцієнтів не спрацювання. З огляду на те, що системи досліджуваного класа є резервованими відновлюваними, для таких системє доцільно, для досліджень їх надійності, застосовувати комплексні показники коефіцієнти готовності, оперативної готовності та їх доповнення до одиниці.

Коефіцієнт (функція) готовності - для відновлюваних резервованих систем безперервного функціонування, вихідний ефект від застосування яких пропорційний сумарній тривалості перебування системи в працездатному стані, дорівнює ймовірності того, що об'єкт виявиться в працездатному стані в довільний момент часу, крім запланованих періодів, протягом яких застосування об'єкта за призначенням не передбачається. Часто в іноземній літературі використовується позначення A(t), а його доповнення до одиниці U(t) (функція неготовності).

Коефіцієнт готовності характеризує готовність системи до застосування за призначенням у відношенні її працездатності і відповідно визначає ймовірність її знаходження у працездатному стані у будь-який момент часу, при цому важливо розуміти, що цей момент часу не може бути обраний в часові інтервали, коли застосування системи за призначенням виключається [56].

Показники, що наведено в таблиці 1.11 часто називають стаціонарними. Тобто всі перехідні процеси в системі завершені і вважається, що після приробки значення коефіцієнтів залишаються незмінним, з огляду на це вираз для обчислення стаціонарного коефіцієнта готовності наступний:

Таблиця 1.11

Номенклатура показників надійності

Назва показника	Означення показника	Вид показника
Коефіцієнт технічного використання	$K_{тв}$	Комплексний
Коефіцієнт готовності	$K_г$	
Коефіцієнт оперативної готовності	$K_{ог}$	
Напрацювання на відмову	$T_о$	Безвідмовність
Напрацювання на відмову – «хибне спрацьовування»	$T_х$	
Ймовірність безвідмовної роботи за задане напрацювання	$P(t)$	
Середнє напрацювання на відмову	$T_{ср}$	
Гама-процентне напрацювання до відмови	T_γ	
Ймовірність спрацюваннння на вимогу	$P_{св}$	
Ймовірність оперативного спрацюваннння на вимогу	$P_{осв}$	
Середній час відновлення працездатного стану	$T_в$	Ремонтопридатність
Середня оперативна тривалість планового ремонту	$T_{пр}$	
Середня оперативна трудомісткість планового ремонту	$S_{пр}$	
Середній час заміни	$T_з$	
Середній ресурс	$T_р$	Довговічність
Гама-процентний ресурс	$T_{р\gamma}$	
Призначений ресурс	$T_{пр}$	
Середній термін служби	$T_с$	
Гама-процентний термін служби	$T_{с\gamma}$	
Призначений термін служби	$T_{пс}$	
Середній термін зберігання	$T_с$	Збереженість
Гама-процентний термін зберігання	$T_{с\gamma}$	

$$K_{Г} = \sum_{i:S_i \in MS_{П}} P_{S_i}, \quad (1.1)$$

де P_{S_i} - ймовірність знаходження системи і S_i-му працездатному стані *t,* $MS_{П}$ - множина працездатних станів.

За умови введення поняття інформаційно-технічного стану (ІТС), де під ІТС розуміється сукупність властивостей і ознак як технічного, так і інформаційного характеру, притаманних системі в певний момент часу, множина працездатних станів складається із: $MS_{Птес}$ – підмножини працездатних технічних станів, $MS_{Пinf}$ - підмножини працездатних інформаційних станів.

На практиці більш корисним є оцінювання показників як функцій часу (часто фахівці їх називають динамічними показниками), для того щоб оперативно відслідковувати або прогнозувати значення показників за часом. Тому більш придатним для використання в ході дослідження надійності систем, є вираз для обчислення

$$K_{Г}(t) = \sum_{i:S_i \in MS_p} P_{S_i}(t), \quad (1.2)$$

де $P_{S_i}(t)$ - ймовірність знаходження системи і S_i-му працездатному стані в момент *t*. За умови введення поняття інформаційно-технічного стану (ІТС), множина працездатних станів складається із: , $MS_{Птес}(t)$ – підмножини працездатних технічних станів,
$MS_{Пinf}(t)$- підмножини працездатних інформаційних станів.

Для систем, необхідність у використанні яких, виникає у випадковий момент часу, після якого вимагається безвідмовна робота із достньою тривалістю для реалізації основної функції, застосовується коефіцієнт оперативної готовності.

Коефіцієнт оперативної готовності є ймовірність того, що система опиниться в працездатному стані у випадковий момент часу, крім випадкових

моментів, протягом яких застосування системи за призначенням не планується.

Вираз для обчислення має вигляд:

$$K_{ОГ}(t,\tau) = K_{Г}(t)P(t) + [1 - K_{Г}(t)]P_{B}(\tau)P_{S_i}(t-\tau), \quad (1.3)$$

де $K_{Г}(t)$ – ймовірність застати систему у працездатному стані в будь-який момент часу, $P(t)$ – ймовірність безвідмовної роботи системи за час t, $P_{B}(t)$ – ймовірність відновлення системи за час $\tau<t$, $P_{Si}(t-\tau)$ – ймовірність безвідмовної роботи системи за час $(t-\tau)$, достатнього для виконання покладеної функції.

На сьогодні для стаціонарних процесів достатньо добре виконується співвідношення $T_{o} \gg T_{в}$, тому другим доданком можливо знехтувати. Тому вираз (1.3) можливо записати у вигляді:

$$K_{ОГ}(t,\tau) = \sum_{i:S_i \in MS_p} (P_{S_i}(t) * P_{S_i}(\tau)) \quad (1.4)$$

де $P_{S_i}(\tau)$ - ймовірність того, система буде знаходиться в S_i-му працездатному стані і буде працездатною на протязі часу τ достанього для виконання системою необхідної функції.

Системи, які досліджуються є системами з розвинутими підсистемами контролю та діагностування. Тому для них є доцільним оцінювання властивості достовірності функціонування. В якості показника, що характеризує властивість достовірності функціонування, приймається ймовірність правільної класифікації знаходження системи в працездатних і непрацездатних станах. Вираз для цього паказника має вигляд:

$$D_{ф}(t) = \sum_{i:S_i \in MS_{пр}} P_{Si(ПП)}(t) + \sum_{j:S_j \in MS_{непр}} P_{Sj(НН)}(t), \quad (1.5)$$

де: $MS_{пр}$, - множина працездатних станів; $MS_{непр}$ – множина непрацездатних станів; $P_{Si(ПП)}(t)$ – ймовірність того, що система, яка знаходиться у працездатному стані буде правильно класифікована як працездатна, $P_{Sj(НН)}(t)$ – ймовірність того, що система, яка знаходиться у непразездатному стані буде

класифікована як непрацездатна.

Для випадку, коли відмови можуть бути поділено на небезпечні та безпечні, діагностовані та недіагностовані, доцільним є застосування показника діагностичного покриття (DC, diagnostic coverege):

$$DC = \frac{\sum_{i=1}^{N} \lambda_{DDi}}{\sum_{i=1}^{N} \lambda_{total_i}}, \quad (1.6)$$

де: λ_{DDi} - інтенсивність діагностованих небезпечних відмов *i*-го програмно-апаратного юніта модуля; λ_{totali} є сумою λ_{DDi}, λ_{DUi} – інтенсивності недіагностованих небезпечних відмов *i*-го програмно-апаратного юніту модуля, λ_{SDi} - інтенсивності діагностованих безпечних відмов *i*-го програмно-апаратного юніту модуля, λ_{SUi} - інтенсивності недіагностованих безпечних відмов *i*-го програмно-апаратного юніту модуля, $\sum_{i=1}^{N} \lambda_{DD_i}$ - сумарна інтенсивність діагностованих небезпечних відмов.

Одним із сучасних підходів до забезпечення та оцінювання функційної безпечності ПТК ІКС є підхід, заснований на встановленні рівнів інтегрованості безпеки (Safety Integrity Level - SIL) детально описаний в IEC 61508.

Стандарт IEC 61508 в частині 6 визначає, що для систем, важливих для безпеки, які працюють в режимі з низькою частотою запиту на виконання функції безпеки (що означає можливість виникнення запиту на виконання функції безпеки не частіше одного разу на рік) необхідно оцінювати показник функційної безпечності PFD_{avg} (середнє значення неготовності системи).

PFDavg (англ. Probability of failure on demand, average) - ймовірність неспрацьовування функції безпеки після подачі сигналу на її включення. Вимоги до кількісних значень цього показника наведено в таблиці 1.12.

Таблиця 1.12

Кількісні вимоги до показника функційної безпечності Probability of failure on demand (IEC 61508 ч.6)

Рівень безпеки	Режим роботи з низькою частотою запитів на виконання функції безпеки
SIL	PFDavg
4	$\geq 10^{-5} \ldots < 10^{-4}$
3	$\geq 10^{-4} \ldots < 10^{-3}$
2	$\geq 10^{-3} \ldots < 10^{-2}$
1	$\geq 10^{-2} \ldots < 10^{-1}$

Показник визначається як відношення часу *MDT (T)* (mean down time – час вимушеного простою системи у міжперевірочний період) до *T* (період часу, що враховується [0,T]). Тобто:

$$PFD_{avg} = MDT\ (T)/T, \qquad (1.7)$$

Для практичного застосування показника PFD_{avg} важливо розуміти, що він характеризує неготовність системи забезпечити захист небезпечного процесу (тобто його безпечну зупинку) на протязі встановленого міжперевірочного інтервалу.

Тобто можливо сформулювати висновок про те, що за своєю суттю комплексний показник надійності - коефіцієнт неготовності U(t) та показник функційної безпечності, який застосовується для оцінки рівня неготовності систем важливих для безпеки PFD_{avg} є подібними. Відповідно методи оцінки комплексного показника надійності справедливі та можуть бути застосовані для оцінювання функційної безпечності за цим показником.

Результати аналізу міжнародних стандартів показують, що вони дають перелік рекомендацій для розробки систем з урахуванням того, що системи є програмно-апаратні. Але приклади оцінювання показника PFD_{avg} наводяться

виключно для врахування надійності апаратної компоненти. Жодної рекомендації щодо оцінювання показника з урахуванням надійності (ненадійності) програмної компоненти немає.

Стандарт IEC 61508 в частині 6 визначає, що для систем важливих для безпеки, які працюють в режимі з високою частотою запитів на виконання функції безпеки (що означає можливість виникнення запиту на виконання функції безпеки частіше одного разу на рік) необхідно оцінювати показник функційної безпечності PFH.

PFH - очікувана частотність настання аварій і, таким чином, інтенсивність запиту на виконання відповідної функції безпеки.

За стандартом – середня частота небезпечної відмови системи безпеки для виконання визначеної функції безпеки протягом заданого періоду часу. Можемо бачити деякі протиріччя у визначені даного показника. Назва показника ймовірність (probability), хоча за сенсом він є частотою виникнення небезпечної відмови. В частині 4 стандарту зазначено, що незважаючи на це акронім PFH збережено. Кількісні вимоги до цього показника наведені в таблиці 1.13.

Таблиця 1.13

Кількісні вимоги до показника функційної безпечності Probability of failure per hour (IEC 61508 ч.6)

Рівень безпеки	Режим роботи з високою частотою запитів на виконання функції безпеки
SIL	PFH
4	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-6} \ldots < 10^{-5}$

За вказаним стандартом, для систем які безпосередньо виконують запит на виконання функції безпеки, показник визначається з використанням виразу:

$$F(T) = 1 - R(t), \quad (1.8)$$

Де $R(t) = exp(-\int_0^T \lambda(t)dt)$ - ймовірність безвідмовної роботи системи за визначений інтервал часу Т (основний (експоненційний)закон надійності), *F(T)* – ймовірність відмови відповідно.

За стандартом – PFH є середньою частотою небезпечної відмови системи безпеки для виконання визначеної функції безпеки протягом заданого періоду часу Т. Тобто:

$$PFH(T) = F(T)/T \quad (1.9)$$

Даний показник характеризує швидкість зменшення надійності системи на заданому проміжку часу. Показник базується на обчисленні ймовірності безвідмовної роботи, який, як добре відомо, застосовується для невідновлюваних систем, базуючись на параметрі $T_{ср}$ – середнє напрацювання до відмови (першої). Тому застосування цього показника є доцільним за умови оцінювання функційної безпечності резервованої системи але тільки щодо її окремих компонент в тому числі на рівні одного каналу. Для систем пов'язаних з безпекою рекомендується обчислювати PFH з застосуванням показника U(t) функції неготовності.

1.4 Обгрунтування науково-прикладної проблеми

1.4.1 Протиріччя

Виконаний аналіз причин та наслідків відмов інформаційно-керуючих систем авіаційних систем, ракетно-космічної техніки та систем промислової автоматизації показує, що їх частка досягає майже четвертої частини, тобто 23% для авіаційних та ракетно-космічних комплексів і до 46%, що є майже половиною, для систем промислової автоматизаці і зокрема ПТК ІКС АЕС..

Ця ситуація зберігається незважаючи на те, що модернізація існуючих та розробка нових систем грунтується на використанні нової елементної бази, сучасних, у тому числі, інформаційних технологіях розробки і тестування їх апаратної та програмної компонент, що розширює можливості модернізованих або нових систем з одного боку, а з іншого підвищує ризики залежності рівней надійності та функційної безпечності від якості процесів модернізації та розробки, а тобто від рівня розвинутості процедур, технік та інструментів розробки і тестування.

Тому незважаючи на значний прогрес, продовжує зберігатись значна кількість «дефіцитів» рівня технічного, інформаційного, методичного, інструментального забезпечення процесів модернізації та розробки нових ІКС ТККВ, а саме:

- недостатня надійність апаратного та програмного забезпечення, що модернізується або розроблюється заново;
- недостній рівень діагностики технічного та програмного забезпечення;
- різноманітність технічних рішень для ІКС в межах одного об’єкту автоматизації (наприклад, одного енергоблоку АЕС);
- неврахування в ході розробки систем варіантів взаємного впливу АЗ та ПЗ та розширеного переліку можливих зовнішніх впливів (фізичного та/або інформаційного);
- неврахування в ході системного проектування розширеного переліку причин порушень працездатності ПТК ІКС (дефектів фізичної природи, дефектів проектування, дефектів взаємодії);
- неврахування в ході апріорного оцінювання надійності та функційної безпечності комплексного впливу на ці показники дефектів різної природи та варіантів їх зміни та інш.

Аналіз державної та міжнародної нормативної бази підтверджує відсутність рекомендацій щодо необхідності комплексного підходу при оцінюванні та забезпеченні надійності та функційної безпечності ПТК ІКС,

коли під комплексністю розуміється врахування великої додаткової кількості факторів (розширена множина причин порушень працездатності, взаємний вплив компонент систем та інш).

Досвід роботи з відомими аудиторськими компаніями (наприклад Канадською Exida) підтверджує, що навіть вони проводять аудити та видають сертифікати відповідності систем, застосовуючи методи оцінювання показників функційної безпечності виключно з урахуванням апаратної компоненти. Впевненість, що програмна компонента є надійною спирається виключно на довіру до методів, інструментальних засобів, етапів розробки ПЗ та тестування. Тому проблема комплексного оцінювання і забезпечення надійності і функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного застосування з урахуванням відмов, обумовлених проектними та фізичними дефектами і вразливостей програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень залишається актуальною.

Таким чином, можливо зробити висновок про існування **протиріччя -** у невідповідності між розширенням множини причин порушення працездатності ПТК для ІКС критичного застосування внаслідок фізичних і проектних дефектів їх компонентів, зміною параметрів потоків відмов, відновлень і оновлень, апаратних, програмних і інформаційних ресурсів, ***з одного боку,*** і рівнем розвитку сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпечності ПТК, - ***з іншого боку***.

1.4.2 Проблема

Подолати сформульоване протиріччя можливо шляхом вирішення **актуальної науково-прикладної проблеми** комплексного оцінювання і забезпечення надійності і функційної безпечності ПТК для ІКС критичного застосування з урахуванням відмов, обумовлених проектними, фізичними

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

1.4.3 Завдання досліджень та їх взаємозв’язок з результатами

Метою дисертаційного дослідження є розвиток методологічних основ, розроблення методів і засобів оцінювання та забезпечення надійності та функційної безпечності програмно-технічних комплексів для критичного застосування з урахуванням відмов, обумовлених фізичними та проектними дефектами і вразливостями, а також їх практичне впровадження в інформаційно-керуючих системах критичного застосування для зниження ризиків небезпечних відмов.

Методологія досліджень базується на використанні принципів системного аналізу [69÷70] при постановці і вирішенні завдань дисертаційного дослідження. Що безпосередньо проявляється у:

- визначені етапів вирішення поставлених завдань та логічної послідовності їх виконання;
- виборі адекватного математичного апарату, методів досліджень і їх співвідношення з завданнями окремих етапів досліджень;
- - формальному представленні структури, властивостей та станів ПТК ІКС;
- компонентному представленні ПТК ІКС і дослідженні їх взаємозв'язку в задачах аналізу (оцінювання) та синтезу (забезпечення) надійності і функційної безпечності.

Процес вирішення наукової проблеми декомпозовано на декілька етапів, основними з яких є наступні.

На першому етапі вирішуються завдання 1 та 2 досліджень, а саме, розробляються елементи методології оцінювання і забезпечення надійності та

функційної безпечності ПТК ІКС критичного призначення за рахунок опису їх інформаційно-технічного стану, удосконалення принципів: аналізу інформаційно-технічного стану та варіантів його порушень; визначення змінних параметрів відмов за різними ознаками і відновлень компонентів і систем; комплексування моделей та методів оцінювання апаратних, програмних і програмовних компонент; використання процесно-продуктової диверсності при створенні систем; гнучних стратегій відновлення при відмовах різних компонент, об’єднаних концепцією комплексного оцінювання і забезпечення НіФБ ПТК ІКС критичного призначення, визначається набір моделей, методів та інструментальних засобів для реалізації цих принципів та встановлюються системні зв’язки між ними.

На другому етапі вирішується завдання 3 досліджень, а саме вдосконалюються ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу систем, та різних сценаріїв їх внесення.

Наступний етап доцільно присвячено вирішенню завдання 4 досліджень, а саме розробці методу оцінювання НіФБ ПТК ІКС зі структурно-версійною надмірністю, який 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.

На четвертому етапі необхідно вирішити завдання 5 досліджень, а саме розробити моделі оцінювання НіФБ ПТК ІКС, які будуються на самодіагностованих платформах. Дані моделі враховують помилки контролю та діагностування і змінність параметрів системи, що забезпечує підвищення точності оцінок готовності і функціональної безпеки та надає можливість висунути вимог до засобів рівня глибини контролю та діагностування при проектуванні системи.

П’ятий етап присвячено вирішенню завдання 6 досліджень, а саме

розробленню методів верифікації і валідації програмовних платформ і ПТК на їх основі, які базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов (FMECA/SFMECA) та ін'єктування фізичних і проектних (HWFIT/SWFIT), що забезпечує перевірку виконання вимог стандартів і підвищення функціональної безпеки в ході проектування, тестування системи, сертифікації і ліцензування.

На шостому етапі має бути вирішено завдання 7 досліджень, а саме розроблено метод забезпечення функціональної безпеки програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною.

Заключним етапом має бути розроблення методу, що об'єднує результати виконання попередніх етапів - метод оцінювання та забезпечення функціональної безпеки при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах, який ураховує фізичні та проектні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функціональної безпеки SIL3. Цей результатт має бути рішенням завдання 8 дисертаційних досліджень

При розв'язанні науково-прикладної проблеми доцільно використати наступні методи. При удосконаленні ймовірнісних моделей оцінювання надійності (безвідмовності) програмних засобів було використано методи теорії надійності програмних засобів та математичної статистики. При розробленні методу оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю було використано методи теорії надійності, теорії множин і графів, марковських випадкових процесів з дискретними станами і неперервним часом. При розробленні математичних моделей оцінювання готовності та функційної безпечності ПТК на самодіагностовних платформах було використано методи теорії надійності і

технічної діагностики, теорії ймовірностей та марковських випадкових процесів. При розробленні методів верифікації і валідації програмовних платформ і ПТК на їх основі було використано методи аналізу видів, наслідків і критичності відмов, теорії множин, методи системного аналізу. При розробленні методу забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах було використано теорії надійності і технічної діагностики, теорії множин і графів, марковського аналізу. При розробленні методу оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах було використано методи теорії надійності і технічної діагностики, теорії множин і графів, марковського аналізу, системного аналізу.Оцінка експериментальних даних, отриманих у ході роботи, проводилася на основі методів математичної статистики. Взаємозв’язок завдань досліджень і результатів наведено на рисунку 1.9.

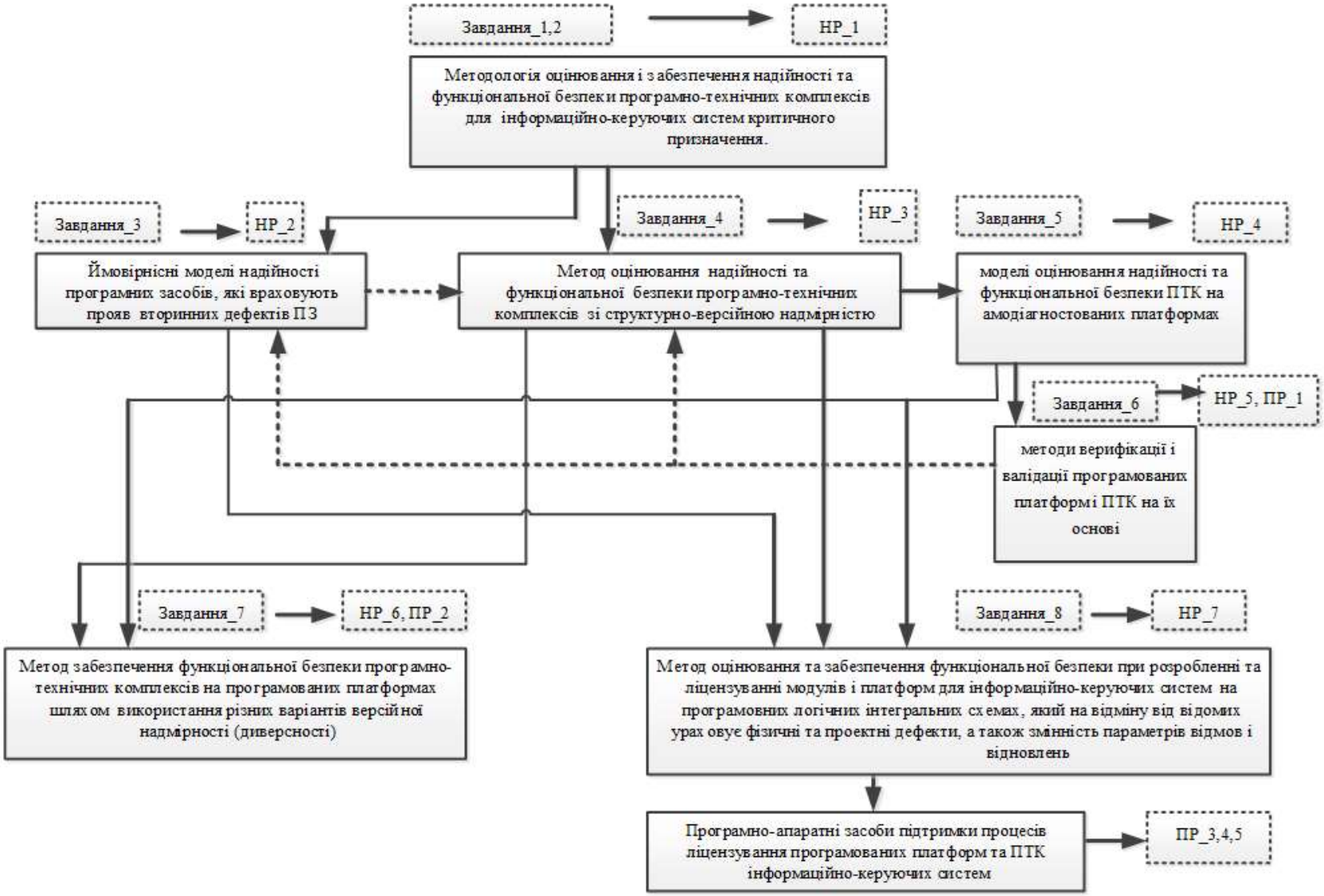


Рис. 1.9 Взаємозв’язок завдань і результатів досліджень

1.5 Висновки за розділом

1. Виконано аналіз причин, наслідків відмов та факторів впливу інформаційно-керуючих систем на надійність та функційну безпечність авіаційних, ракетно-космічних комплексів та систем промислової автоматизації і зокрема на програмно-технічні комплекси інформаційно-керуючих систем АЕС. За результатами аналізу встановлено, що для авіаційних та ракетно-космічних комплексів зберігається значна доля відмов пов'язаних із відмовами їх систем керування. Левова доля відмов таких систем керування виникає в результаті відмов програмного забезпечення. Для систем прмислової автоматизації встановлено, що на сьогодні, найбільш впливовими факторами залишаються: відмови технічних засобів ПТК ІКС; відмови програмного забезпечення; відмови периферійних пристроїв; зовнішні впливи та помилки персоналу. Тому, сучасні ПТК ІКС зберігають набір «дефецитів безпеки», які визначаються: недостатньою надійністю технічних засобів; недостатнім рівнем діагностики апаратного та програмного забезпечення; неповним задоволенням вимог до сейсмостійкості; різноманітністю елементної бази та технічних рішень для різник ІКС (в межах одного енергоблоку) тощо.

2. Виконано аналіз вимог національних та міжнародних нормативних документів до надійності та функційної безпечності ПТК ІКС критичного затсосування. Встановлено, що існуюча нормативна база вимагає встановлення всеохоплюючих засобів для забезпечення надійності та функційної безпечності ПТК ІКС критичного застосування, що потребує виконання аналізу, розроблення нових моделей, методів, технологій оцінювання і забезпечення вказаних властивостей на всіх етапах життєвого циклу систем досліджуваного класу.

Важливим є встановлений факт, що існуючі стандарти не дають рекомендацій щодо комплексного оцінювання систем з урахуванням того, що

сучасні обчислювальні системи інтегрують апаратні і програмні засоби, які в ході роботи мають взаємний вплив. На прикладі базового стандарта IEC 61508 доведено, що стандарт (стандарти) не вільні великої кількості недоліків: неточних визначень, методологічних невизначеностей або некоректних рекомендацій тощо, що потребує розроблення рекомендацій щодо вдосконалення нормативної бази, що надалі позитивно впливатиме на процеси розроблення і тестування систем досліджуваного класу.

3. Виконано аналіз основних тенденцій розвитку інформаційно-керуючих систем технічних комплексів критичного використання. За результатами аналізу встановлено, що сучасні тенденції розвитку ІКС ТККВ забезпечують підвищення кількості функцій що автоматизуються, зростає рівень автоматизації технологічних процесів з одного боку. З іншого боку впровадження нових цифрових та інформаційних технологій породжує нові ризики, які впливають на безпеку систем та відповідно стають актуальними завдання розроблення і впровадження методів, технік та програмно-апаратних засобів розроблення, верифікації і валідації компонент та в цілому ІКС ТККВ.

4. Виконано огляд базових теорій оцінювання та забезпечення надійності та функційної безпечності, що дозволило сформулювати наступні висновки:

− незважаючи на розвиток обчислювальної техніки і відповідно зростання впливу програмного забезпечення на рівень надійності і функційної безпечності цієї техніки продовжує окремий розвиток теорія надійності технічних систем і відповідно науково-методичний апарат оцінювання надійності і функційної безпечності систем на основі врахування надійнісних характерстик виключно апаратних компонент;

− теорія надійності програмного забезпечення, отримує розвиток, як окремий напрямок, з урахуванням надійнісних характеристик виключно програмних складових надійності та функційної безпечності без урахування того, що сучасні системи є інтегрованими програмно-апаратними системами,

тобто на даний час фактичною відсутнє врахування впливу надійності окремих компонент апаратних засобів на кінцевий результат роботи програми і навпаки.

5. Встановлено аналітичний зв’язок між показниками надійності і функційної безпечності, що дозволяє використовувати спільні методи їх оцінювання.

6. Систематизовано математичні методи аналізу надійності та функційної безпечності ПТК ІКС КЗ, а також обґрунтовано застосування апарату марковського аналізу для оцінювання вказаних властивостей. Застосування цього апарату досліджень пов'язано з певними труднощами, такими, як збільшення множини станів марковських моделей, жорсткість і розрідженість матриць коефіцієнтів систем диференційних рівнянь, що описують ці моделі. Оскільки ці складнощі безпосередньо впливають на точність оцінювання показників надійності й функційної безпечності, рекомендації щодо їх подолання необхідно формулювати у відповідних нормативних документах (стандартах).

7. Виконано аналіз математичного апарату та обмежень використання існуючих методів та засобів оцінювання надійності і функційної безпечності ІКС ТККВ. За результатами аналізу для оцінювання надійності і функційної безпечності систем досліджуваного класу – ПТК ІКС ТККВ обрано марковський аналіз. Встановлено, що для досліджуваних систем, застосування теорії марковських випадкових процесів, може супроводжуватись значними обчислювальними труднощами. Ці труднощі викликані специфікою надійнісних параметрів, що окремо описують надійність апаратних і програмних компонент. Далі ці труднощі підсилюються необхідністю комплексного врахування, тобто взаємного впливу апаратних і програмних компонет на надійність і функційну безпечність систем. Як результат отримаєм матрицю коефіцієнтів системи диференційни рівнянь Колмогорова-Чепмена, яка має специфічні властивовсті жорсткості, розрідженості та розмірності. Це потребує додаткових заходів в ході обґрунтування апарату досліджень та обрання інструментальних засобів.

8. Встановлено, що не зважаючи на інтенсивні дослідження за обраної тематикою впродовж останніх десятиліть, які виконувалися в Україні та за її межами, залишається низка нерозв’язаних задач і обмежень існуючих методів і засобів, а саме:

− моделі, які описують надійнісну і безпекову (як інформаційну так і функціональну) складові, не ураховують реальну розмірність задач оцінювання з огляду на складність індустріальних ІКС і їх ПТК, змінність параметрів відмов і відновлень програмно-апаратних засобів;

− у методах оцінювання функційної безпечності, насамперед, аспекти безвідмовності апаратних і програмних засобів розглядаються відокремлено, без спільного комплексного кількісного аналізу результатів і верифікації;

методи розроблення й забезпечення відмовостійкості ПТК з використанням програмовних платформ недостатньо ураховують можливості, обмеження і похибки вбудованих засобів контролю і діагностування на рівні електронних проєктів, модулів і каналів тощо.

9. Обгрунтовано послідовність досліджень, яку декомпозовано на сім етапів, в ході виконання яких послідовно розв’язано часткові завдання, науково-прикладну проблему та отримано сім наукових результатів.

Основні положення розділу викладені у публікаціях автора [80, 87, 123, 141, 231, 232, 234, 240, 247, 248, 255,].

РОЗДІЛ 2. МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНЮВАННЯ І ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ З УРАХУВАННЯМ ПРОЕКТНИХ І ФІЗИЧНИХ ДЕФЕКТІВ. БАЗОВІ ПОНЯТТЯ ТА ПРИНЦИПИ

2.1 Структура методології оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів з урахуванням

2.1.1 Концепція і принципи оцінювання і забезпечення надійності та функційної безпечності ПТК

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 дисертаційній роботі моделей, методів та інструментальних засобів. Базові ідеї досліджень грунтуються на ідеї фон Неймана про створення надійної системи із ненадійних елементів, яка покладена в основу принципа створення електронних обчислювальних машин та мереж [43]. У дисертаційному дослідженні ідея фон Неймана розвивається стосовно складних систем, таких як ПТК ІКС критичного застосування, за рахунок комплексного оцінювання і забезпечення надійності і функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного призначення.

Комплексність базується, по-перше, на розширенні поняття технічного стану (ТС) системи до інформаційно-технічного стану (ІТС), де під ІТС розуміється сукупність властивостей і ознак як технічного, так і інформаційного характеру, притаманних системі в певний момент часу. Застосування поняття ІТС дозволяє врахувати наступні такі властивості системи, як безвідмовність, готовність, функційну безпеку, цілісність.

По-друге комплексність базується на врахуванні:

− множини компонентів: МК={АК, ПК, ПвК} (апаратних (АК), програмних (ПК), програмовних (ПвК);

− множини дефектів: МД={ДФ, ДП, ДВФ, ДВІ} (фізичні дефекти АК – (ДФ), дефекти проєктування (ДП), дефекти взаємодії фізичної природи (ДВФ), дефекти взаємодії інформаційні (ДВІ));

− множини відмов: МВ={ВК, ВН} (відмови критичні (ВК), відмови некритичні (ВН));

− множини змінних параметрів: МЗП={ЗІВм, ЗІВн, ЗКВн} (змінні інтенсивності відмов (ЗІВм - $\Delta\lambda_{дп,}$ $\Delta\lambda_{дв}$), змінні інтенсивності відновлень (ЗІВн - $\Delta\mu_{вп.}$ $\Delta\mu_{дв}$), запас компонент для відновляння (ЗКВн));

− множини властивостей (атрибутів): МА={АБ, АГ, АФБ, АІБ, АГз} (атрибути безпеки (АБ), атрибути готовності (АГ), атрибути функційної безпечності (АФБ), атрибути інформаційної безпеки (АІБ), атрибути гарантоздатності (АГз)).

Таким чином комплексність описується множиною, яка дорівнює декартовому добутку:

$$М = МК \times МД \times МВ \times МЗП \qquad (2.1)$$

Комплексність врахування множин компонент, дефектів та змінність параметрів наглядно ілюстровано у трьохмірному просторі (Рис.2.1).

Сформульована концепція комплексного оцінювання і забезпечення надійності і функційної безпечності ПТК ІКС критичного призначення базується на використанні наступної системи принципів, покладених в основу розроблених моделей і методів:

1) аналізу інформаційно-технічного стану та варіантів його порушення;

2) визначення змінних параметрів відмов за різними ознаками і відновлень компонентів і систем;

3) комплексування моделей та методів оцінювання апаратних, програмних і програмовних компонент;

4) використання процесно-продуктивної диверсності при створенні систем.

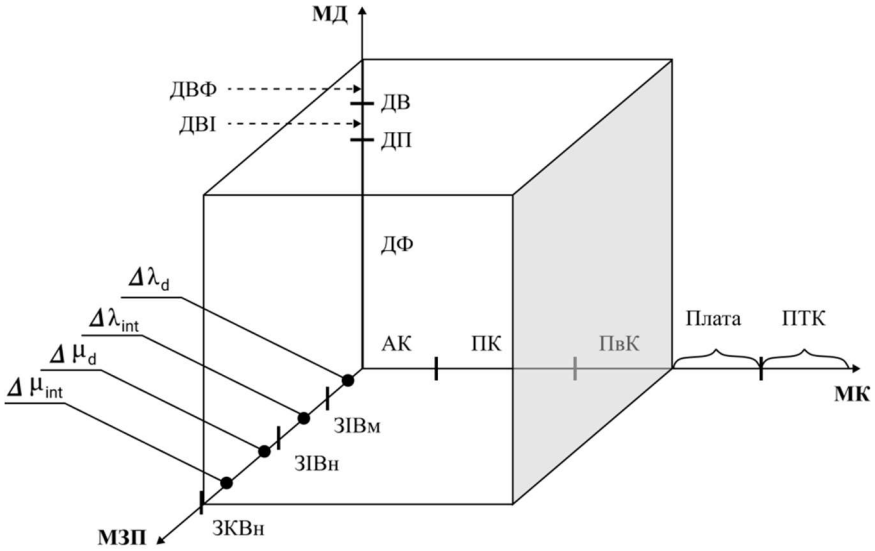


Рис. 2.1 Трьохмірний куб врахування множин компонент, дефектів та змінності параметрів

Запропоновані принципи складають основу для розробки наступних моделей:

1) моделі «система – фізичне та інформаційне середовище» та моделі ІТС;

2) модифікованих ймовірнісних моделей оцінювання надійності програмних засобів (МНПЗ), термін та абревіатура у іноземній технічній літературі - Software reliability growth models (SRGM)) шляхом урахування їх вторинних дефектів;

3) моделей оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю;

4) моделей надійності та функційної безпечності ПТК на самодіагностовних платформах з урахуванням помилок контролю та діагностування.

Розроблені моделі є інструментом множини наступних методів:

1) методу оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю;

2) методу забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності);

3) методів верифікації і валідації програмовних платформ і ПТК на їх основі, які базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов (FMECA/SFMECA) та ін'єктування фізичних і проєктних (HWFIT/SWFIT) дефектів;

4) методу оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для ІКС на програмовних логічних інтегральних схемах, який ураховує фізичні та проєктні дефекти, а також змінність параметрів відмов і відновлень, і гарантує виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3.

Теоретичні результати одержали свого практичного застосування на основі розроблення множини інструментальних засобів:

1) програмно-технічні засоби резервування ІКС на базі перспективної цифрової інформаційно-управляючої платформи RadICS розробки і виробництва ПАТ «НВП «Радій» (м. Кропивницький);

2) програмно-технічні засоби та елементи системи менеджмента якості підтримки процесів ліцензування програмовних платформ та ПТК ІКС ТОВ «НВП «Радікс» (м. Кропивницький);

3) елементи системи менеджмента якості, які реалізують процесно-продуктивний підхід до розробки ПТК ІКС з підвищеними вимогами до надійності та функційної безпечності.

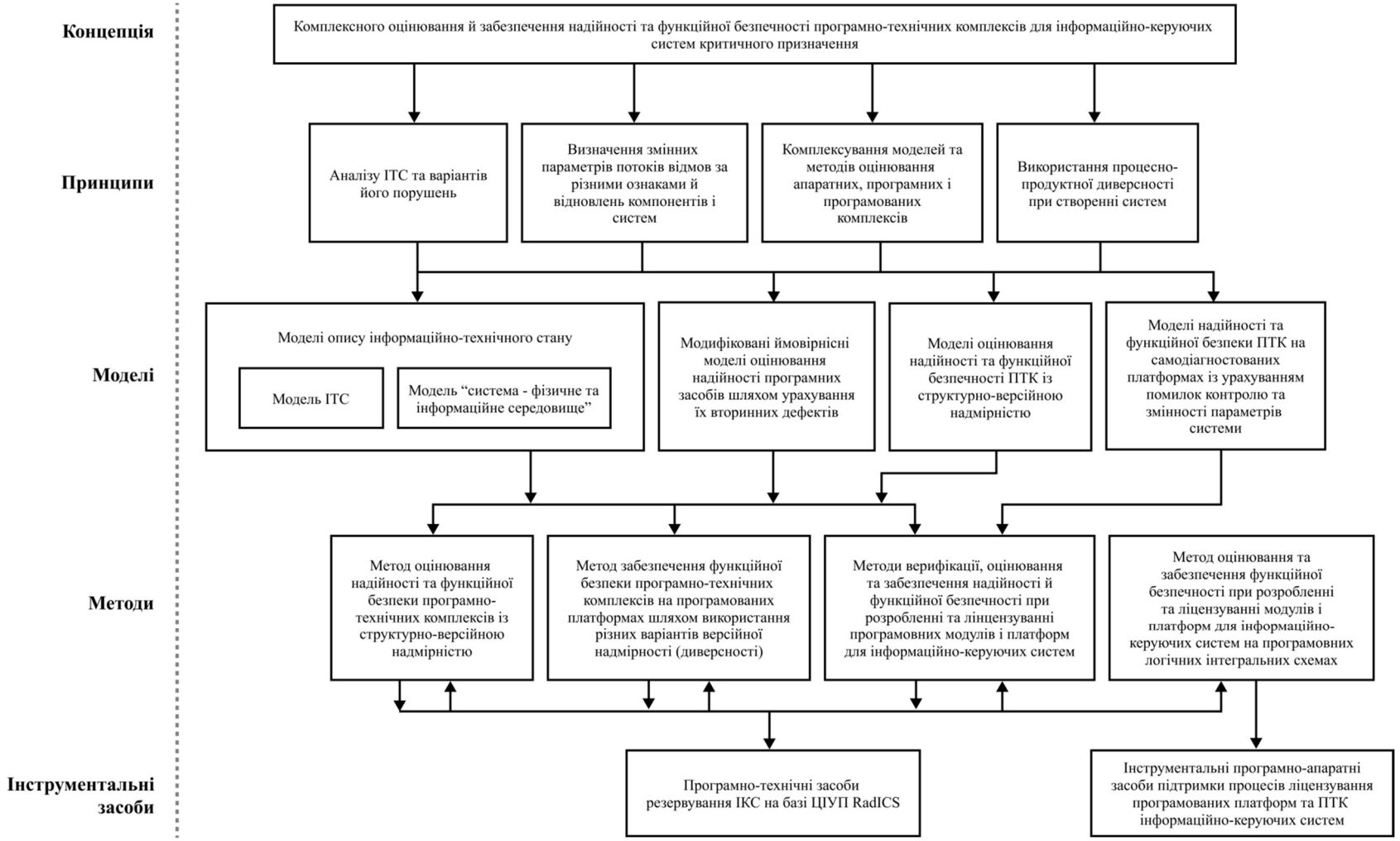


Рис. 2.1 Структура методології оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів з урахуванням проектних і фізичних дефектів

2.1.2 Принцип аналізу інформаційно-технічного стану та варіантів його порушення

Досліджувані системи, програмно-технічні комплекси інформаційно-керуючих систем критичного призначення, функціонують в умовах дії внутрішніх і зовнішніх факторів. Такими факторами є: дефекти різної природи, які можуть виникати на різних етапах розробки та функціонування системи; помилки обслуговуючого персоналу; зовнішні вторгнення, як фізичного так і інформаційного характеру; існуючі вразливості систем, які неминуче існують в системах. Все це призводе, за певних обставин, до відмови у наданні послуг системою із значними втратами. Врахувати представлений розширений перелік факторів для прогнозування надійності та функційної безпечності систем що розробляються можливо за рахунок впровадження ідеї аналізу та дослідження сукупності властивостей, які отримали загальне визначення - інформаційно-технічного стану (ІТС). Тобто з’являється можливість комплексно дослідити надійність та функційну безпечність системи, з урахуванням технічних та інформаційних ознак, які притаманні системи в певний момент часу. До властивостей, які при цьому розглядаються, відносяться наступні: безвідмовність, готовність, функційна безпечність; до числа ознак - множини станів системи: справних (несправних), працездатних (частково працездатних), непрацездатних, безпечних, потенційно небезпечних, небезпечних або критичних з урахуванням того, що переходи між ними можуть здійснюватися внаслідок різних за природою дефектів.

2.1.3 Принцип визначення змінних параметрів відмов за різними ознаками і відновлень компонентів і систем

Однією із основних вимог до моделювання, зокрема марковського, яке

обрано в якості базового метода оцінювання надійності і функційної безпечності, є забезпечення адекватності. У випадку не зняття припущення про не змінність параметрів моделювання систем ця вимога порушується, що призводе до відхилення результуючої функції і відповідно до помилок в оцінюванні шуканих показників. Тому, з метою забезпечення адекватності оцінювання показників надійності і функційної безпечності впроваджена ідея про умовну апроксимацію функцій, що описують параметри моделі, наприклад $\lambda(t)$ – інтенсивність прояву дефекту або $\mu(t)$ – інтенсивність відновлення після прояву, кусково-неперервною функцією. При цьому після зміни станів системи (моделі) відбувається стрибкоподібна зміна величин інтенсивностей λ або μ на певні значення $\Delta\lambda$ або $\Delta\mu$. Слід зазначити, що параметри $\Delta\lambda$ і $\Delta\mu$ можуть бути як постійними величинами і приводити до лінійного характеру зміни відповідних інтенсивностей, так і змінними. В останньому випадку характер зміни інтенсивностей прояви дефектів і відновлення має нелінійний характер. Вид нелінійності можна визначити після дослідження характеру і "ваги" відповідного дефекту.

2.1.4 Принцип комплексування моделей та методів оцінювання апаратних, програмних і програмовних компонент

В основі принципа комплексування лежить ідея використання переваг моделей і методів оцінювання апаратних, програмних і програмовних компонент та послідовного їх поєднання для вирішення завдань оцінювання та забезпечення показників надійності та функційної безпечності ПТК ІКС КЗ.

Наприклад, комплексування для моделей надійності програмних засобів полягає у їх спрямованому поєднанні з метою використання переваг моделей різних класифікаційних ознак при оцінюванні надійності розроблюваного і супроводжуваного програмного забезпечення.

2.1.5 Принцип використання процесно-продуктивної диверсності при створенні систем

Сутність багатоверсійності, як принципа забезпечення надійності, полягає у використанні різних продуктових (програмно-апаратних) та процесних засобів для реалізації ідентичних функцій з метою [319]:

− створення ПТК ІКС, стійких до фізичних та проєктних дефектів, завдяки зниженню ймовірності відмови за загальною причиною через застосування в резервних каналах системи різних програмно-апаратних версій;

− підвищення повноти та достовірності верифікації і валідації програмного забезпечення і ПТК ІКС в цілому завдяки використанню диверсних незалежних процесів і засобів проєктування і тестування та зниження ризиків прояву невиявлених дефектів.

2.2 Моделі опису інформаційно-технічного стану

2.2.1 Модель «система – фізичне та інформаційне середовище»

Обчислювальні системи (до яких можливо віднести ПТК), які здійснюють прийом, зберігання, обробку та видачу інформації, функціонують в умовах дії внутрішніх і зовнішніх факторів, що призводять до порушення їх працездатності і цілісності оброблюваної інформації. Комплекс властивостей системи протистояти цим факторам і забезпечити надання необхідних послуг (виконання функцій), яким можна виправдано довіряти, називають гарантоздатністю [128]. Елементами таксономії гарантоздатності, як відомо з [128, 129], є:

− загрози (уразливості, вторгнення, дефекти, помилки, відмови), які можуть привести до ненадання послуг;

− механізми відмовостійкості (відмовостійкість, стійкость до вторгнень), що забезпечують усунення або зниження ризиків таких загроз;

− первинні властивості гарантоздатності, що характеризують різні аспекти і ступінь стійкості системи до різних типів загроз *і досліджуються в даній роботі* - безвідмовність, готовність, функційна безпечність;

− вторинні властивості, які є похідними від первинних і більш детально характеризують складові гарантоздатності (наприклад, контролепридатність для готовності).

Одним з базових понять, що дозволяє методологічно об'єднати елементи таксономічної схеми гарантоздатності, є поняття інформаційно-технічного стану (ІТС), яке є розширенням поняття технічного стану (ТС).

Вихідна ідея ІТС була сформульована в [309], а його визначення, що розширює стандартне поняття технічного стану, дано в [269]:

Визначення. Інформаційно-технічний стан - це сукупність властивостей і ознак як технічного, так і інформаційного характеру, притаманних системі в певний момент часу.

До властивостей, які повинні при цьому розглядатися, відносяться первинні властивості гарантоздатності (безвідмовність, готовність, функційна безпечність), до числа ознак - множини станів системи (справних - несправних, працездатних - частково працездатних - непрацездатних, безпечних - потенційно небезпечних - небезпечних або критичних) з урахуванням того, що переходи між ними можуть здійснюватися внаслідок:

− виникнення або прояву фізичних дефектів (ДФ) апаратних засобів;

− дефектів проєктування (ДП) програмних (ДПП) і апаратних (ДПА) засобів;

− дефектів взаємодії (ДВ), які викликаються випадковими ненавмисними або навмисними зовнішніми впливами фізичної природи (ДВФ) (механічними, кліматичними, електромагнітними, радіаційними та ін.) Або інформаційними впливами (ДВІ) (помилковими діями персоналу, хакерськими атаками, спамом і т. д.).

Таким чином, модель ІТС, дозволяє розробити моделі і методи оцінювання

надійності і функційної безпечності ПТК з урахуванням впливу зовнішніх і внутрішніх факторів з різним ступенем їх урахування та деталізації. Відповідно до цього отримує розвиток методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного призначення за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушення внаслідок проєктних і фізичних дефектів та дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і забезпечення виконання вимог до відповідних показників.

Уявимо модель станів системи S(t) з урахуванням впливів середовища E(t) (зовнішніх і внутрішніх впливів на систему). Вектор стану системи в момент часу t:

$$S(t) = \{S_0(t), E_{int}(t), E_{ext}(t)\}, \quad (2.1)$$

де $S_0(t)$ - працездатний (і цілісний) стан, в якому система знаходиться при відсутності внутрішніх і зовнішніх впливів і яке характеризується повною відповідністю вимогам до неї, включаючи вимоги за всіма досліджуваними складовими (безвідмовності, надійності, функційної та інформаційної безпеки); $E_{int}(t)$ - вектор внутрішніх впливів, що включає дії, що обумовлені фізичними $E_{int.phs}(t)$ і проектними $E_{int.des}(t)$ дефектами:

$$E_{int}(t) = \{E_{int.phs}(t), E_{int.des}(t)\} \quad (2.2)$$

$E_{ext}(t)$ - вектор зовнішніх впливів, що включає вектори зовнішніх інформаційних $E_{ext.inf}(t)$ і фізичних $E_{ext.phs}(t)$ впливів відповідно, викликають дефекти взаємодії:

$$E_{ext}(t) = \{E_{ext.inf}(t), E_{ext.phs}(t)\} \quad (2.3)$$

$S(t+\Delta t)$ – вектор стану системи в момент $t+\Delta t$:

$$S(t+\Delta t) = \{S_{Eint}(t+\Delta t), S_{Eext}(t+\Delta t)\} \quad (2.4)$$

де $S_{Eint}(t+\Delta t) = \{S_{Ehw}(t+\Delta t), S_{Esw}(t+\Delta t)\}$ – внутрішній стан системи в момент $t+\Delta t$, який характеризується станами його апаратних $S_{Ehw}(t+\Delta t)$ та програмних $S_{Esw}(t+\Delta t)$ засобів; $S_{Eext}(t+\Delta t) = \{S_{Econ}(t+\Delta t), S_{Eitg}(t+\Delta t)\}$ – зовнішній стан системи в момент $t+\Delta t$, який характеризується станом інформаційних ресурсів системи (їх цілісністю) $S_{Eitg}(t+\Delta t)$, і середовища (доступністю до конфіденційних інформаційних ресурсів) $S_{Econ}(t+\Delta t)$.

Реакція системи на внутрішні і зовнішні фізичні впливи проявляється тим, що система формує помилкову вихідну інформацію в даний момент часу або один з наступних моментів часу. Реакція системи на зовнішні інформаційні впливи проявляється тим, що порушується внутрішня інформація, що циркулює або зберігається в системі, або середовище (зовнішня система) отримує несанкціонований доступ до цієї інформації в даний або один з наступних моментів часу.

Припущення 1. Будемо вважати, що інтервал часу Δt малий настільки, що загальний потік внутрішніх і зовнішніх впливів, що характеризується вектором $E(t)$ можливо вважати ординарним. Це не виключає можливість неординарності внутрішніх (вектор $E_{int}(t)$) і зовнішніх (вектор $E_{ext}(t)$) впливів, а також їх складових ($E_{int.phs}(t)$, $E_{int.des}(t)$, $E_{ext.inf}(t)$, $E_{ext.phs}(t)$) в межах інтервалу Δt. Наступний внутрішній або зовнішній вплив може статися в момент часу $\Delta t_+ > \Delta t$.

Припущення 2. При $t = 0$ $E_{int}(0) = Ø$, $E_{ext}(0) = Ø$, $S(0) = S_0(0)$. Таке припущення є загальноприйнятим в теорії надійності і відповідає фізичному змісту і реальній практиці експлуатації систем. У той же час воно може бути доведено як твердження.

Якщо при $t = 0$ $E_{int}(0) = Ø$ або $E_{ext}(0) = Ø$, можна умовно розглянути

поведінку системи на інтервалі часу {t* = 0, t = 0}, де $t^* = t - t_0$, а t_0 - тривалість часу, протягом якого система піддається внутрішнім $E_{int}(t^*)$ або зовнішнім $E_{ext}(t^*)$ впливам. Завжди можна підібрати тривалість інтервалу t_0 таку, щоб:

- або в його початку завжди виконувалося умова $S(t^* = 0) = S_0(t^* = 0)$ і зберігалося далі на всьому інтервалі {t * = 0, t = 0} в умовах впливів;

- або до завершення інтервалу система повністю відновлювалася б при порушенні цієї умови внаслідок впливів в момент часу $t - t_0 < t^* < t$.

Отже, твердження доведено шляхом введення віртуального інтервалу часу $\{t^* = 0, t = 0\}$. Таким чином, можливо записати, що

$$S(t+\Delta t) = S_0(t) \,//\, \{ E_{int}(t), E_{ext}(t) \}, \qquad (2.5)$$

де символом // позначений узагальнений оператор перетворення стану $S_0(t)$ при впливах $E_{int}(t)$, $E_{ext}(t)$ (або скорочено «ОПС»).

Аналогічно справедливо, що

$$S(t) = S_0(t-\Delta t) \,//\, \{ E_{int}(t-\Delta t), E_{ext}(t-\Delta t) \}. \qquad (2.6)$$

2.2.2 Модель інформаційно-технічного стану

З урахуванням (2.4, 2.5, 2.6) отримаємо:

$$S(t+\Delta t) = \{S_0(t) \,//\, \{E_{int.phs}(t), E_{int.des}(t), E_{ext.inf}(t), E_{ext.phs}(t)\}\}. \qquad (2.7)$$

Припущення 3. Будемо вважати внутрішні $E_{int}(t)$ і зовнішні $E_{ext}(t)$ впливи не залежними між собою по моменту часу і характеристикам впливів. Це припущення підтверджується досвідом експлуатації, а також різною природою впливів. При більш детальному розгляді складових впливів можна говорити про можливість в загальному випадку кореляції складових $E_{int.phs}(t)$ та $E_{int.des}(t)$, $E_{int.des}(t)$ та $E_{ext.inf}(t)$, $E_{int.phs}(t)$ та $E_{ext.phs}(t)$.

Виконаємо перетворення

$$S(t+\Delta t) = \{ S_{tec}(t+\Delta t), S_{inf}(t+\Delta t) \}, \quad (2.8)$$

де

$$S_{tec}(t+\Delta t)=\{S_0(t)//\{E_{int.phs}(t),E_{int.des}(t), E_{ext.phs}(t)\}\}, \quad (2.9)$$

$$S_{inf}(t+\Delta t)=\{S_0(t)//E_{ext.inf}(t)\}. \quad (2.10)$$

Стани $S_{tec}(t+\Delta t)$ та $S_{inf}(t+\Delta t)$ будемо називати технічним і інформаційним станами відповідно. Тоді стани $S(t+\Delta t)$ або $S(t)$ будемо називати інформаційно-технічним станом системи.

При $E_{int}(t) = Ø$, $E_{ext}(t) = Ø$ $S(t+\Delta t) = S_0(t)$ і стан $S(t+\Delta t)$ будемо називати справним ІТС, при якому виконуються всі вимоги до системи.

Працездатне (справний або несправний) ІТС має місце, якщо при $E_{int}(0) \neq Ø$ или $E_{ext}(0) \neq Ø$, $S(t+\Delta t) = S_0(t) \vee S'_0(t)$, де $S'_0(t)$ - стан, аналогічний працездатному технічному стану, при якому виконуються також основні вимоги щодо цілісності і конфіденційності інформації.

Непрацездатним ІТС $S_{Н}(t)$ будемо називати стан, при якому не виконується хоча б одна з вимог до працездатності системи в частині всіх досліджуваних властивостей.

2.2.3 Властивості операції перетворення станів

Дослідимо властивості операції перетворення стану //.

Асоціативність. Операція // не має властивість асоціативності, оскільки в загальному випадку $\{S_0(t) // \{E_{int.phs}(t), E_{int.des}(t), E_{ext.inf}(t), E_{ext.phs}(t)\}\} \neq \{\{\{S_0(t) // E_{int.phs}(t)\} // E_{int.des}(t)\} // E_{ext.inf}(t)\} // E_{ext.phs}(t)$.

Комутативність. Очевидно, що ця операція не є комутативною по відношенню до лівої і правої частин, оскільки перетворення $E(t) // S(t)$ позбавлене фізичного змісту. Що стосується властивості коммутативності

операції по впливам, то в окремому випадку такою властивістю можуть володіти пари впливів $E_{int.phs}$ и $E_{ext.phs}$, $E_{int.phs}$ и $E_{int.des}$, $E_{int.des}$ и $E_{ext.phs}$. Вплив $E_{ext.inf}$ є некомутативним з усіма іншими впливами.

Транзитивність. Властивість транзитивності для операції перетворення позбавлене фізичного змісту в силу одиничності розглянутих станів.

Дистрибутивність. Вирази (2.8÷2.10) постулюють властивість дистрибутивності ОПС в частині відносної незалежності цих складових ІТС відповідно до припущень.

2.3 Модель інформаційно-технічного стану з урахуванням рівней працездатності

Модель ІТС описується виразом:

$$S(t) = \{S_{tec}(t), S_{inf}(t)\}, \tag{2.11}$$

де $S_{tec}(t)$, $S_{inf}(t)$ його технічна та інформаційна складові (стани), причому

$$\begin{gathered} S(t) = S(t-\Delta t)//\{E_{int.phs}(t-\Delta t), E_{int.des}(t-\Delta t), \\ E_{ext.inf}(t-\Delta t), E_{ext.phs}(t-\Delta t)\}, \\ S_{tec}(t) = S(t-\Delta t)//\{E_{int.phs}(t-\Delta t), \\ E_{int.des}(t-\Delta t), E_{ext.phs}(t-\Delta t)\}, \\ S_{inf}(t) = S\,(t-\Delta t)\;//\;E_{ext.inf}(t-\Delta t), \end{gathered} \tag{2.12}$$

де E_i $(t-\Delta t)$ – вектори впливів в момент $t-\Delta t$, які викликають дефекти D_i, що належать множині МД; // - оператор перетворення станів при впливах.

Система, виходячи з розглянутої безлічі впливів (дефектів) має в загальному випадку, такі множини станів.

1. Множину справних технічних $MS_{0tec}(t)$, інформаційних $MS_{0inf}(t)$ та

інформаційно-технічних $MS_0(t)$

$$MS_0(t) = MS_{0tec}(t) \cap MS_{0inf}(t), \qquad (2.13)$$

причому потужність множин справних технічних і інформаційних станів може бути прийнята рівною одиниці, тому операція їх перетину в цьому випадку перетворюється в логічне І (з цієї причини символ множини М для таких станів може опускатися). У справному ІТС виконуються всі вимоги до системи, включаючи технічну та інформаційну складові.

2. Множина працездатних технічних $MS_{Ptec}(t)$, інформаційних $MS_{Pinf}(t)$ та інформаційно-технічних $MS_P(t)$ станів, причому

$$MS_P(t) = MS_{Ptec}(t) \cap MS_{Pinf}(t). \qquad (2.14)$$

У працездатному ІТС значення технічних і інформаційних параметрів зберігаються на рівні, що забезпечує виконання заданих функцій відповідно до вимог до системи (включаючи вимоги з інформаційної безпеки).

3. Множина частково працездатних станів:
технічних $MS^i_{чPtec}(t) = \bigcup_i MS^i_{чPtec}(t)$; інформаційних $MS_{чPinf}(t) = \bigcup_j MS^j_{чPinf}(t)$; інформаційно-технічних $MS_{чP}(t) = \bigcup_k MS^k_{чP}(t)$, де ($i = \overline{1, d_{tech}}$, $j = \overline{1, d_{inf}}$, $k = \overline{1, d}$, d - число допустимих рівнів деградації за відповідною складовою), причому в загальному вигляді маємо:

$$MS_{чP}(t) = MS_{чPtec}(t) \bigcup MS_{чPinf}(t). \qquad (2.15)$$

У частково працездатному ІТС система виконує всі життєво важливі функції і не виконує деяку допустиму частину інших функцій або виконує функції з гіршою у порівнянні з працездатним станом якістю. Якщо для системи допускається, що $d > 1$, можна говорити про властивості живучості.

Вид множини $MS^{k}_{ЧР}(t)$ визначається функцією k = f(i,j), яка в частному випадку може представлятися як k = max(i,j).

4. Множина повністю непрацездатних технічних $MS_{ПНtec}(t)$, інформаційних $MS_{ПНinf}(t)$і інформаційно-технічних $MS_{ПН}(t)$ станів, причому

$$MS_{ПН}(t) = MS_{ПНtec}(t) \bigcup MS_{ПНinf}(t). \quad (2.16)$$

Крім того, до складу множини $MS_{ПН}(t)$ входять підмножини:

− непрацездатних, але безпечних технічних $MS_{НРБtec}(t)$, інформаційних $MS_{НРБinf}(t)$ і інформаційно-технічних станів $MS_{НРБ}(t)$;

− небезпечних технічних $MS_{НРОtec}(t)$, інформаційних $MS_{НРОinf}(t)$ і інформаційно-технічних станів $MS_{НРО}(t)$, тобто:

$$MS_{НРБ}(t) = MS_{НРБtec}(t) \cap MS_{НРБinf}(t), \quad (2.17)$$

$$MS_{НРО}(t) = MS_{НРОtec}(t) \bigcup MS_{НРОinf}(t). \quad (2.18)$$

Множина $MS_{НРО}(t)$ розглядається як множина функціонально небезпечних (аварійних) станів, а множини $MS_{Р}(t)$, $MS_{ЧР}(t)$ и $MS_{НРБ}(t)$ об’єднують функціонально безпечні стани (множина $MS_{Б}(t)$):

$$MS_{Б}(t) = MS_{Р}(t) \bigcup MS_{ЧР}(t) \bigcup MS_{НРБ}(t). \quad (2.19)$$

2.3.1 Переходи в просторі інформаційно-технічних станів

В рамках розглянутих понять і моделей слід уточнити події, при яких здійснюються переходи між станами. За аналогією з відомими поняттями несправності, пошкодження і відмови (збою) можуть бути визначені поняття технічних і інформаційних несправностей, пошкоджень і відмов (збоїв), а також уточнені їх різновиди в залежності від типу дефектів, які їх викликають

(множина D), наслідків з точки зору рівня працездатності та ін.

З урахуванням введених множин і моделей, наведених в [308], множина ІТС системи і переходів між ними може бути описано в системі координат «дефекти-стани» (Рис. 2.2).

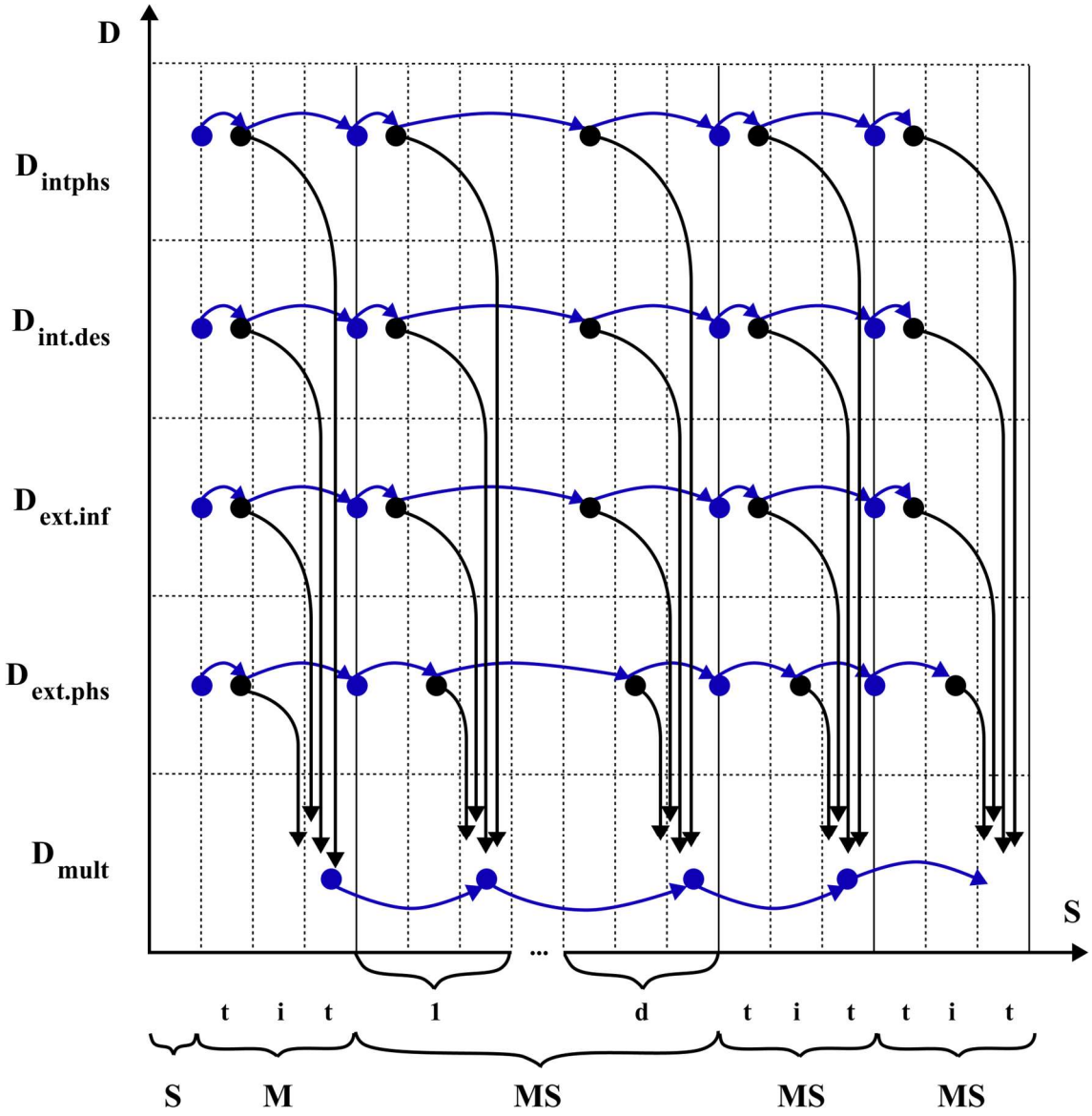


Рис. 2.2 Дефекти, інформаційно-технічні стани і переходи між ними

На рисунку 2.2 використані наступні позначення: D_{mult} – множинні дефекти; $D_{ext.phs}$ – множина зовнішніх фізичних дефектів, які проявляються під впливом $E_{ext.phs}$; $D_{ext.inf.}$ – множинаінформаційних дефектів, які проявляються під впливом $E_{ext.inf}$; $D_{int.des.}$ – множина дефектів проектування, які проявляються під

впливом $E_{int.des}$;. $D_{ext.inf.}$ $D_{int.phs.}$ множина дефектів проектування, які проявляються під впливом $E_{int.phs}$., t –технічна складова ІТС; i – інформаційна складова ІТС; d – рівні деградації).

Переходи між станами s_i та s_j, $i \neq j$, $i,j = \{1,\ldots,cardMS\}$, які належать множині ІТС $MS = S_0 \cup MS_P \cup MS_{ЧС} \cup MS_{НРБ} \cup MS_{НРО}$, описуються матрицею ймовірностей $H = \| P(s_i,s_j) \|$.

Сині стрілки на рис.2.2 демонструють можливі переходи між станами у визначених множинах станів під впливом відповідних типів множин дефектів, а чорні демонструють стани із накопиченими дефектами (мультидефектами).

2.5 Зв’язок між моделями і методами

Запропонована методологія дозволяє реалізувати системний підхід до рішення проблеми комплексного оцінювання і забезпечення надійності і функційної безпечності ПТК для ІКС критичного застосування 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. Це досягається наявністю вертикальних та горизонтальних зв’язків між сутностями методології, а саме: множиною принципів, множиною моделей методів та інструментальних засобів, що їх реалізують на практиці.

Вертикальні зв’язки описано в підрозділі 2.1.1. Горизонтальними зв’язками є наступні:

Модель «система – фізичне та інформаційне середовище» враховує вплив зовнішніх і внутрішніх факторів на досліджувану систему з різним ступенем їх урахування та деталізації, а саме:$E_{int}(t)$ - вектор внутрішніх впливів, який обумовлено фізичними $E_{int.phs}(t)$ і проєктними $E_{int.des}(t)$ дефектами; $E_{ext}(t)$ - вектор зовнішніх впливів, що включає вектори зовнішніх інформаційних $E_{ext.inf}(t)$ і фізичних $E_{ext.phs}(t)$ впливів відповідно. Урахування векторів впливу дозволяє

перейти до моделі інформаційно-технічного стану, яка деталізує рівні працездатності за рахунок розгляду множин станів: справних, працездатних, частково працездатних, повністю непрацездатних для кожної множини станів відповідно технічних; інформаційних та інформаційно-технічних. Дані моделі створюють умови для розроблення або модифікації наступних множин моделей: ймовірнісних моделей оцінювання надійності програмних засобів шляхом урахування їх вторинних дефектів, моделей оцінювання надійності та функційної безпечності ПТК із структурно-версійною надмірністю, моделей надійності та функційної безпеки ПТК на самодіагностовних платформах із урахуванням помилок контролю та змінності параметрів системи.

Модифіковані ймовірнісні моделі оцінювання надійності програмних засобів шляхом урахування їх вторинних дефектів. Дані моделі дають можливість виконати уточнення результатів поведінки ПЗ в умовах внесення вторинних ДППЗ під час розроблення, рефакторинга та тестування програмних проєктів. Визначено множину моделей надійності ПЗ, які дозволяють врахувати зміну їх надійнісних параметрів в часі.

Моделі оцінювання надійності та функційної безпечності ПТК із структурно-версійною надмірністю використовують результати розробки попереднії моделей та розвивають їх в частині врахування комплексного впливу надійнісних параметрів АЗ та ПЗ та надійність та функційну безпечність ПТК.

Моделі надійності та функційної безпечності ПТК на самодіагностовних платформах із урахуванням помилок контролю об’єднують переваги попередніх моделей та підсилюють їх за рахунок врахування помилок засобів вбудованого контролю АЗ та ПЗ компонент ПТК і стана прихованої небезпечної недетектованої відмови.

Комплекс перерахованих математичних моделей дозволив перейти до розробки комплексу взаємопов’язаних математичних методів оцінювання

надійності та функційної безпечності ПТК, взаємозв’язок між якими наведено в п. 2.1.1.

2.6 Висновки за розділом

1. В розділі 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. Методологія базується на розвитку парадигми фон Неймана і гіпотезі про можливість побудови надійних і функційно безпечних систем (ПТК ІКС) із недостатньо надійних програмно-апаратних компонентів, тобто з урахуванням відмов внаслідок їхніх фізичних і проєктних дефектів, а також принципах, які забезпечують її підтвердження.

У рамках методології:

− запропоновано принцип аналізу інформаційно-технічного стану та варіантів його порушення, який відрізняється тим, що оцінювання здійснюється за рахунок впровадження ідеї аналізу та дослідження розширеної сукупності: властивостей (безвідмовності, готовностість, функційної безпечності), зовнішніх та внутрішніх інформаційних та технічних впливів на систему і множин станів, в які переходе система після впливу відповідного типу;

− запропоновано принцип визначення змінних параметрів відмов за різними ознаками і відновлень компонентів і систем, який відрізняється тим, що оцінювання здійснюється за рахунок впровадження ідеї зняття припущення про не змінність надійнісних параметрів АЗ і ПЗ за рахунок умовної апроксимації функцій, що описують параметри моделі, наприклад $\lambda(t)$ –

інтенсивність прояву дефекту або μ(t) – інтенсивність відновлення після прояву, кусково-неперервною функцією. При цьому після зміни станів системи (моделі) відбувається стрибкоподібна зміна величин інтенсивностей λ або μ на певні значення Δλ або Δμ;

− запропоновано принцип комплексування моделей і методів оцінювання апаратних, програмних і програмовних компонент ПТК, який відрізняється тим, що оцінювання здійснюється за рахунок впровадження ідеї послідовного поєднання математичних моделей, використання їх переваг для забезпечення значень показників надійності та функційної безпечності ПТК ІКС КЗ, які вимагаються від системи, що проєктується;

− запропоновано принцип процесно-продуктивної диверсності при створенні систем, який відрізняється тим, що для забезпечення значень показників надійності та функційної безпечності ПТК ІКС КЗ, підвищення повноти та достовірності верифікації і валідації програмного забезпечення і ПТК ІКС в цілому застосовуються диверсні, незалежні процеси і засоби проєктування та тестування.

Обгрунтовно «горизонтальні» та «вертикальні» зв’язки між складовими методології, а саме розробленими математичними моделями та методами. Відзначено, що запропонована методологія базується на основних принципах системного підхода, що дозволяє вирішити проблему комплексного оцінювання і забезпечення надійності і функційної безпечності ПТК для ІКС критичного застосування 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.

2. Запропонований опис «система-фізичне та інформаційне середовище» базується на понятті, що розширює поняття технічного стану системи до інформаційно-технічного і дозволяє розробляти моделі інформаційно-техніого стану. 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.

3. Дано опис властивостей операцій перетворення станів моделі ІТС, а саме: асоціативності; комутативності; транзитивності і дистрибутивності. Це дало змогу дослідити можливості взаємних впливів різної природи на систему, деталізувати множини станів системи, що досліджується, а саме: справних, працездатних, частково працездатних, повністю непрацездатних безпечних і небезпечних. В рамках розглянутих понять і моделей уточнено події, при яких здійснюються переходи між станами. За аналогією з відомими поняттями несправності, пошкодження і відмови (збою) визначені поняття технічних і інформаційних несправностей, пошкоджень і відмов (збоїв), а також уточнені їх різновиди в залежності від типу дефектів, які їх викликають і наслідків з точки зору рівня працездатності.

Основні положення розділу викладені у публікаціях автора [124, 125, 127, 155, 165, 210, 235, 240, 247, 248].

РОЗДІЛ 3 МОДЕЛІ ОЦІНЮВАННЯ ПРОГРАМНИХ ЗАСОБІВ ШЛЯХОМ УРАХУВАННЯ ВТОРИННИХ ДЕФЕКТІВ

3.1 Дослідження відомих моделей надійності програмних засобів

В умовах необхідності оцінювання та забезпечення надійності і функційної безпечності ПТК ІКС КЗ з урахуванням прєктних дефектів компонентів, де часткою проєктних дефектів є ДППЗ систем, що досліджуються, вирішується завдання аналізу, вибору, розроблення та удосконалення моделей надійності програмних засобів (МНПЗ) з урахуванням вторинних ДППЗ.

Розроблення та удосконалення моделей надійності програмних засобів , software reliability growth models SRGM), з урахуванням вторинних дефектів базується на аналізі й виборі з множини базових МНПЗ тих моделей, що дозволяють урахувати прояв вторинних дефектів у ході тестування ПЗ і його експлуатації. Урахування в МНПЗ впливу фактору вторинних дефектів дозволяє більш точно оцінювати надійність ПЗ, що розробляється і таким чином підвищити точність оцінювання показників надійності й функційної безпечності ПТК в цілому.

Подальше дослідження складається з наступних етапів:

− аналізу науково-методичного апарату теорії надійності програмного забезпечення, встановлення розширеного переліку класифікацій МПНЗ за трьома основними класифікаційними ознаками (моделі емпіричні, статистичні, ймовірнісні);

− аналізу припущень, які покладено в основу побудови ймовірнісних МНПЗ з метою встановлення моделей, які дозволяють врахувати фактор прояву вторинних дефектів;розроблення множини сценаріїв внесення вторинних ДППЗ;

− модифікації функцій ризику обраних ймовірнісних МНПЗ у відповідності до розроблених сценаріїв внесення та усунення вторинних дефектів ПЗ;

− розроблення варіантів комплексування МНПЗ;

− розроблення послідовності прогнозування кількості вторинних дефектів за статистичними даними прояву первинних ДППЗ;

− -застосування модифікованих МНПЗ та послідовності прогнозування кількості вторинних дефектів в процесі оцінювання надійності та функційної безпечності ПТК.

Одним із результатів розвитку теорії надійності програмного забезпечення є множини МНПЗ [313], які було розроблено базуючись на різних за природою припущеннях. Різноманітність припущень історично викликано різноманітністю існуючих факторів розроблення ПЗ та умов його застосування. За даними великої кількості джерел МНПЗ прокласифіковано за певними ознаками, прикладами таких класифікацій є наступні.

− Класифікація Хетча [154]. За даною класифікацією пропонується поділ моделей на *прогнозирующие, вимірювальні і оціночні*, де: *прогнозуючі* моделі базуються на вимірі технічних характеристик створюваної програми, а саме: довжини; складності; кількості циклів; кількості помилок на сторінку операторів програми. Прикладом таких МНПЗ є модель Холстеда, Мотлі-Брукса. Тобто ці моделі є емпіричними; *вимірювальні* моделі призначені для вимірювання надійності ПЗ, що працює із заданою зовнішнім середовищем і мають деякі обмеження (припущення), наприклад, програмне забезпечення не модифікується під час періоду вимірювань властивостей надійності, виявлені дефекти не виправляються тощо (типовим прикладом таких моделей є МНПЗ Нельсона, Рамамурті-Бастані); *оціночні* моделі ґрунтуються на серії тестових прогонів і проводяться на етапах тестування ПЗ. У тестовому середовищі визначається ймовірність відмови програми при її виконанні або тестуванні (типовим прикладом такої МНПЗ є модель Муси).

− Класифікація Гоела [154]. За даною класифікацією пропонується поділ моделей за наступними класифікаційними ознаками: моделі без підрахунку дефектів; моделі з підрахунком відмов; моделі із засівом дефектів; моделі з вибором областей вхідних значень. Типовими прикладами МНПЗ за даними класифікаційним ознаками є наступні: моделі без підрахунку дефектів – Джелінського-Моранди, Шика-Уолвертона; моделі з підрахунком відмов – Шумана; моделі із засівом дефектів – Мілса, Бейзина; моделі з вибором областей вхідних значень – Нельсона.

− Класифікація Фатуєва [191]. За даною класифікацією пропонується поділ моделей за наступними класифікаційними ознаками: статичні моделі; динамічні моделі, які поділено на неперервні та дискретні.

− Класифікація Благодатських [190]. Дана класифікація є розширенням класифікації Фатуєва.

− Класифікація Полоннікова-Нікандрова [155]. За даною класифікацією пропонується поділ моделей за наступними класифікаційними ознаками: структура часу; складність ПЗ, розмітка помилок, структура тексту програми, структура простору вхідних даних. Типовими прикладами МНПЗ за даними класифікаційним ознаками є наступні: структура часу – Джелінського-Моранди, проста експоненційна, Шика-Уолвертона, Ліпова, геометрична, Шнайдевінда, Вейбула, Дюена; складність ПЗ – модель Холстеда; розмітка помилок - моделі Мілса, Бейзина, проста еврістична; структура тексту програми – Нельсона, Ла-Падули, регресійна (фірми IBM); структура простору вхідних даних – текстова модель, ентропійна.

Аналіз моделей даних класифікацій дозволив сформувати скорочену класифікацію за наступними ознаками: емпіричні; статистичні; ймовірнісні, що дозволило перейти до обрання МНПЗ, які дозволяють врахувати фактор внесення та прояву вторинних дефектів ПЗ.

Класифікація МНПЗ за трьома ознаками наведена на рисунку 3.1. Показники, за якими оцінюються МНПЗ у відповідності з встановленими

ознаками наступні:

- N_d – кількість залишкових дефектів ПЗ після їх розробки;
- λ_d – інтенсивність прояву програмного дефекту;
- $\lambda(t)$ – функція ризику;
- $P_n(t,\tau_{set})$ – ймовірність безпомилкового виконання програми;
- $P_n(G)$ – ймовірність безпомилкового виконання програми з урахуванням шляхів її виконання, які описує граф G.

	МНПЗ	Показники МНПЗ
Емпіричні	Холстеда	N_d
	Мотлі-Брукса	N_d
	Фірми IBM	N_d
	Іслама-Ломбарді	N_d
	Ліпаєва	λ_d
Статистичні	Міллса	N_d
	Маєрса	N_d
	Коркорена	f_d
	Нельсона	f_d
	Бейзина	N_d
Ймовірністні	Джелінського-Моранди	$\lambda(t)$
	Муси	$P_n(t,\tau_{set})$
	Проста експоненційна	$\lambda(t)$
	Шика-Уолвертона	$\lambda(t)$
	Ліпова	$\lambda(t)$
	Геометричні моделі	$\lambda(t)$
	Шнайдервінда	$P_n(t)$
	Вейбулла	$P_n(G)$

Рис. 3.1 Скорочена класифікація МНПЗ

3.1.1 Розроблення підходу до модифікації функцій ризику та врахування зміни надійності ПЗ за часом

Виконаємо аналіз припущень, недоліків та переваг МНПЗ скороченої класифікації з метою їх практичного застосування. Емпіричні моделі є прогнозуючими і дозволяють отримати оцінки остаточної кількості ДППЗ після розробки ПЗ за їх кількісними параметрами. Зокрема, це абсолютний показник N_d та відносний показник λ_d кількості залишкових дефектів. На практиці, свого часу, широке розповсюдження отримали оцінки (метрики) Холстеда [192], що зв'язують число дефектів у програмі з кількістю операторів n_1 та n_2 операндів:

$$N_d = k_p(\eta_1 log_2 \eta_1 + \eta_2 log_2 \eta_2) log_2(\eta_1 + \eta_2), \quad (3.1)$$

де k_p – коефіцієнт пропорційності.

Статистичні моделі використовують співвідношення, які зв'язують кількість дефектів і відносну частоту їх прояву f_d з кількістю прогонів програм m. Для цього типу МНПЗ кількісні оцінки отримують на основі інтуїтивних припущень з використанням статистичних методів, які базуються на внесенні відомого числа дефектів в програми ($N_{d(in)}$), порівнянні результатів паралельного незалежного тестування програм, аналізі впливу різних типів дефектів на результати тестування. Статистичні моделі орієнтовані на етапи тестування і налагодження ПЗ.

Найбільш простою для реалізації є модель Г. Міллса, яка пов'язує величини N_d та $N_{d(in)}$:

$$N_d = (N_{d1} + N_{d(in)})/N_{d(in)} \quad (3.2)$$

де N_{d1} – кількість виявлених дефектів в ході тестування та $N_{d(in)}$ – відома кількість штучно внесених дефектів.

При цьому передбачається, що N_{d1} не перевищує прогнозованого числа дефектів до початку тестування, що було оцінено, наприклад, метриками М. Холстеда.

Загальним недоліком емпіричних і статистичних МНПЗ є те, що вони не враховують динаміку реального обчислювального процесу та не дозволяють виконати оцінювання надійності ПЗ із урахуванням часу й умов їх функціонування.

Найбільш поширеною є група ймовірнісних моделей, серед яких можна виділити баєсовські, графоймовірнісні, ймовірнісно-лінгвістичні та експоненційні.

Графоймовірнісні моделі базуються на аналізі усіх шляхів граф-схем програм й оцінці ймовірності їх безпомилкового виконання $P_n(G)$ з урахуванням ймовірностей можливих значень умов розгалуження $p(x_i)$ і ймовірностей безпомилкового виконання вершин графа G, які відповідають групам операторів програми.

Ймовірнісно-лінгвістичні моделі розвивають графоймовірнісний підхід та базуються на математичному апарату нечітких множин. Вони дозволяють виконувати оцінку надійності ПЗ залежно від функцій, що визначають супень належності до різних нечітких множин. Використання таких МНПЗ доцільно на етапах налагодження і приймання ПЗ для завдання середніх, оптимістичних і песимістичних рівнів показників надійності та порівняння їх із фактичними.

Баєсовські моделі відповідають на питання, яка ймовірність наявності ДППЗ після того як було усунуто черговий дефект. Моделі даного типу дозволяють проводити порівняльний аналіз якості ПЗ, враховувати вплив на надійність ПЗ деяких суб'єктивних особливостей розробників. Однак ці моделі, як і більшість ймовірнісних, погано пристосовані до оцінювання надійності ПЗ систем, що не обслуговуються.

Цей недолік частково подолано в експоненційних моделях. Основні припущення, на яких базуються ці моделі наступні:

- інтенсивність прояву дефектів пропорційна їх залишковій кількості у ПЗ;
- час до прояву чергового дефекту розподілений експоненційно;
- кожний виявлений дефект усувається, а нові не вносяться.

Тоді ймовірність безвідмовного (безпомилкового) виконання програм на і-му часовому інтервалі обчислюється за формулою:

$$P_a(t_i)=exp(-\lambda_{di} t_i), \tag{3.3}$$

де $\lambda_{di} = K_n[N_d - (i-1)]$ – інтенсивність прояву ДП на i – му інтервалі; K_n – коефіцієнт пропорційності; $t_i \in [\tau_{i-1}, \tau_i]$ (i = 1,2,… кількість виявлених і усунених ДП).

Припущення про експоненційний характер закону розподілу часу до прояву дефекту експериментально підтверджено Дж. Мусою [208÷210]. Вчений запропонував МНПЗ, що дозволяє врахувати різний характер прояву дефектів при тестуванні й застосуванні ПЗ за призначенням:

$$P_p\left(t,\tau_{pp}\right)=\exp\left(-\frac{t}{T_b}\exp\left[-\frac{K_m\tau_{renew}}{N_d\ T_{in}}\right]\right), \tag{3.4}$$

де T_b – початкове значення середньої наробки на відмову (прояву ДП ПЗ); τ_{renew} - тривалість періоду тестування і налагодження (час відновлення (виявлення, діагностика, усунення) після прояву чергового ДП ПЗ); K_m - коефіцієнт, який враховує "ущільнення" часу тестування й налагодження відносно реального часу функціонування системи.

Відповідно, величина інтенсивності прояву ДППЗ, що фіксується на момент початку експлуатації ПЗ обчислюється за допомогою виразу:

$$\lambda_d = \frac{1}{T_{in}} \exp\left(-\frac{K_m \tau_{renew}}{N_d \ T_{in}} \right), \quad (3.5)$$

,

Відповідно до цього модель Муси була модифікована, для можливості зняття припущення про незмінність інтенсивності прояву ДП ПЗ у часі та подальшого врахування зміни надійності ПЗ при оцінюванні надійності й функціональної безпеки ПТК.

З урахуванням припущення про те, що $\Delta\lambda_d$ = const, $\Delta\lambda_d(\tau_{set})$ визначається наступним чином:

$$\Delta\lambda_d = \lambda_{d(0)} - \lambda_{d(1)}, \quad (3.6)$$

де $\lambda_{d(0)}$ - початкове значення інтенсивності, якій відповідають параметри $N_{d(0)}$ і $\tau_{set(0)}$; $\lambda_{d(1)}$ - значення інтенсивності після усунення одного ДП ПЗ, якій відповідають параметри $N_{d(1)} = N_{d(0)} - 1$ и $\tau_{set(1)} = \tau_{set(0)} + \tau_{set(add)}$, где $\tau_{set(0)}$, де $\tau_{set(0)}$ - початкове значення часу налагодження, $\tau_{set(add)}$ - додаткове налагоджувальне час, $\tau_{set(0)}$ для моделі дорівнює τ_{renew}.

Фізичне пояснення суті параметру $\Delta\lambda_d$, який дозволяє врахувати зміну надійності ПЗ за часом гарно ілюструється рис.3.2., за прийнятою умовою, що процеси прояву, усунення ДП ПЗ описують Марковські ланцюги з дискретними станами та неперервним часом. Тобто неперервний змінний параметр потоку прояву ДППЗ можливо описати кусочно-неперервною функцією із постійним $\Delta\lambda_d$ = const або змінним $\Delta\lambda_d$ = var кроком.

Тоді вираз для $\Delta\lambda_d$ набуде вигляду:

$$\Delta\lambda_d = \frac{1}{T_b} \left[\exp\left(-\frac{K_m \tau_{set(0)}}{N_{d(0)} \ T_b} \right) - \exp\left(-\frac{K_m \tau_{set(1)}}{N_{d(1)} \ T_b} \right) \right]. \quad (3.7)$$

.

Очевидно, що в тому випадку, коли час $\tau_{set(add)}$ є величиною постійною, то і величина $\Delta\lambda_d$ також буде постійною. Якщо припустити, що час відновлення (налагодження) після прояву ДП ПЗ буде залежати від "ваги" (складності) програмного дефекту і буде змінюватися, а саме зменшуватися при зниженні складності й збільшуватися при зростанні складності, то величина $\Delta\lambda_d$ буде також змінюватися в бік зменшення або збільшення.

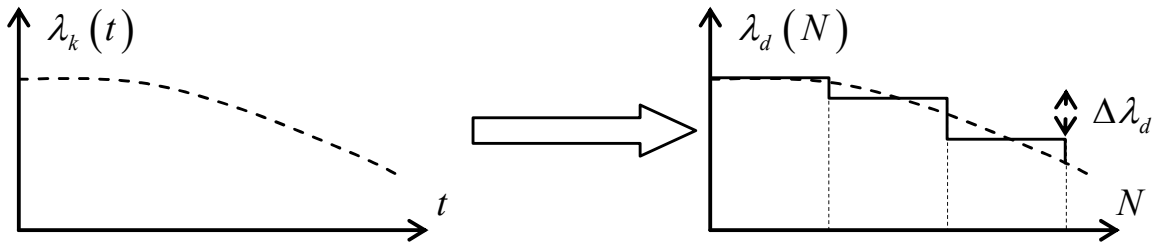


Рис. 3.2 Подання непостійного параметра потоку кусочно-безперервною функцією при утворенні ВМЦ

Подібні міркування застосуємо для оцінювання параметра μ_d – інтенсивності відновлення ПЗ після прояву ДП ПЗ.

Зняття припущення про сталість параметра μ_d робить необхідним рішення задачі оцінки цього параметру, а також обліку його зміни у моделях оцінки надійності й функціональної безпечності ПТК.

У зв'язку з цим можливі різні варіанти зміни цього параметру:

1. Параметр μ_d лінійно зменшується на величину $\Delta\mu_d$. Зменшення може бути пояснено зростанням часу, що витрачається на пошук й усунення чергового ДП ПЗ. У свою чергу це пояснюється зростанням складності виявлення ДП ПЗ після усунення попередніх (менш складних).

2. Параметр μ_d змінюється стрибкоподібно після усунення ДППЗ певного типу. Інтервал зміни параметра заданий від $\mu_{d(min)}$ до $\mu_{d(max)}$, а $\Delta\mu_{d(max)}$ визначається максимально допустимим часом відновлення після прояву ДП ПЗ. У цьому випадку доцільно говорити про зону нечутливості параметру $\mu_{вп}$ до

характеру проявлення дефекту. Потім параметр змінюється на певну величину $\Delta\mu_{вп}$.

Таким чином параметр μ_d (інтенсивність відновлення системи після прояву ДП ПЗ) визначається співвідношенням

$$\mu_d = \frac{1}{T_d}. \tag{3.8}$$

де T_d - середній час необхідний для проведення діагностики, усунення та відновлення роботи системи.

Базуючись на твердженні Дж.Д. Муси [209] про те, що процес відновлення після прояви відмови має пуассоновский розподіл, можна визначити співвідношення для обчислення T_d:

$$T_d = T_{in} \exp\left(\frac{\tau_{new}}{N_{def} \cdot T_{in}}\right). \tag{3.9}$$

де: T_{in} - початкове значення часу відновлення, τ_{renew} - час відновлення (виявлення, діагностика, усунення) після прояву чергового ДП ПЗ. Тоді інтенсивність відновлення після прояву ДП ПЗ і величина її зміни визначаються як:

$$\mu_d = \frac{1}{T_{in}} \exp\left(-\frac{\tau_{вв}}{N_{def} T_{in}}\right). \tag{3.10}$$

$$\Delta\mu_d = \frac{1}{T_{in}}\left(\exp\left(-\frac{\tau_{renew(0)}}{N_{def(0)}\ T_{in}}\right) - \exp\left(-\frac{\tau_{renew(1)}}{N_{def(1)}\ T_{in}}\right)\right). \tag{3.11}$$

Отже, враховуючи, що ймовірнісні моделі дозволяють дослідити

надійність ПЗ відносно часу, вони є найбільш перспективними для врахування фактору внесення вторинних дефектів.

Аналіз джерел [154] дозволяє окреслити підмножину ймовірнісних моделей для подальшого аналізу їх відносно можливості модифікації для врахування фактору внесення та прояву вторинних дефектів ПЗ. До такої підмножини віднесемо наступні МНПЗ: Джелінського-Моранди; Просту експоненційну; Шика-Уолвертона; Муси; Ліпова; Геометрична Моранди (1 та 2); Шнайдевінда; Вейбулла.

3.1.2 Класифікація моделей за ознакою урахування вторинних дефектів

Більшість МНПЗ містить припущення про те, що нові ДП ПЗ не вносяться під час усунення виявлених дефектів в ході тестування або експлуатації ПЗ. Значна частина МНПЗ побудована взагалі без врахування такого припущення.

Для підкреслення необхідності використання під час оцінки надійності й функційної безпечності ПТК припущення про ймовірність внесення нових ДП ПЗ при усуненні виявлених, наведемо дослідження, що було проведене у 1975 році. Під час дослідження професійних програмістів, володіючих мінімум чотирирічним досвідом, попросили налагодити програму з 12 дефектами [309]. У результаті було внесено в середньому 3 і 7,7 нових дефектів (для трьох кращих і трьох найгірших програмістів) враховуючи той факт, що не всі 12 дефектів було виявлено. Таким чином, дефекти ПЗ, які вносяться під час усунення виявлених можливо визначити як *вторинні.*

Із завданням усунення вторинних дефектів зустрічаються фактично більшість груп розробників та тестувальників ПЗ, при цьому питання прогнозування їх кількості, що впливає на тривалість і вартість розробки ПЗ залишається недостатньо дослідженим. Зрозуміло, що актуальність питання виникнення вторинних дефектів ПЗ зростає зі збільшенням вимог до його

складності. Наприклад, більше 30 років тому помилки супроводу ПЗ (вторинні дефекти), становили в середньому 2 – 9% [175], 15-20 років тому їх кількість за деякими даними й оцінками експертів могла складати до 35 - 40% [179, 310].

В останнє десятиріччя, завдяки роботам Д. Маєвського [155, 188, 204], проведені ґрунтовні дослідження, спрямовані на опис фізичної природи вторинних дефектів. Автор, використовуючи концепцію про рівновагу між динамічною інформаційною системою і предметною областю, розробив основи теорії динаміки програмних систем, як нового концептуального підходу до оцінки надійності ПЗ із урахуванням впливу вторинних дефектів. ТДПС відрізняється від існуючої теорії надійності ПЗ тим, що базується на загальній теорії динаміки систем, а не на теорії ймовірностей та розглядає процеси прояву дефектів ПЗ не як випадковий процес, а як результат дії детермінованих потоків дефектів [188].

В теорії ДПС показана і використана аналогія між термодинамічною теорією перенесення й структурними процесами в програмних системах, що дозволяє проводити моделювання їх надійності [187]. Було досліджено роботу і супровід облікової інформаційної системи «Агро-Комплекс» [174], що використовується для автоматизації всіх видів обліку на підприємствах сільського господарства. На основі експериментальних даних зроблено висновок, що сплески прояву дефектів відповідають періодам часу, коли відбувалося значне оновлення структурних параметрів системи. Однією з причин цього відхилення можна вважати внесення дефектів. Крім того, слід врахувати можливість прояву дефектів при взаємодії первинної і оновленої частин ПЗ.

Альтернативним напрямком досліджень у даній області є модифікації існуючих МНПЗ шляхом урахування в моделях параметрів, які характеризують вторинні дефекти. Одним із шляхів такого урахування є модифікація функцій ризику відібраних для цього МНПЗ. Отже розглянемо, яким чином може бути видалено припущення, про безпомилкове усунення виявлених ДППЗ. Множини

припущень обраних ймовірнісних МНПЗ наведено в таблиці 3.1.

Таблиця 3.1

Перелік припущень ймовірнісних МНПЗ та їх функцій ризику

МНПЗ	Перелік припущень для побудови МНПЗ	Функція ризику
Джелінського-Моранди	1.Інтенсивність виявлення $\lambda(t)$ дефектів пропорційна числу дефектів після розроблення і тестування (усунення виявлених). 2.Всі дефекти є рівноймовірними та їх прояв є подією незалежною. 3.Рівень складності дефекту не враховується. 4.Час до прояву наступного дефекту розподілений експоненційно. 5. ПЗ функціонує в умовах максимально наближених до реальних. 6. ***Дефекти усуваються і нові не вносяться.*** 7. $\lambda(t) = const.$	$\lambda(t)=K[N_d - (i-1)]$, t – довільна точка часу між виявленням (i-1)-го та i-го ДППЗ, К - коефіцієнт пропорційності, N_d - залишкове число ДППЗ після розробки і тестування.
Проста експоненційна	1.Інтенсивність виявлення $\lambda(t)$ дефектів пропорційна числу дефектів після розроблення і тестування (усунення виявлених). 2.Всі дефекти рівноймовірні та їх прояв є подією незалежною. 3. Рівень складності дефекту не враховується. 4. Час до прояву наступного дефекту	$\lambda(t)=K[N_d - N(t)]$, *де* $N(t)$ – число виявлених ДППЗ до моменту часу t.

	розподілений експоненційно. 5. ПЗ функціонує в умовах максимально наближених до реальних. 6. ***Дефекти усуваються і нові не вносяться.*** Тобто знято припущення 7 МНПЗ Джелінського – Моранди, після чого функція $\lambda(t)$ вже не є кусочно-неперервною.	
Шика-Уолвертона	1. Всі дефекти рівноймовірні та їх прояв є незалежною подією. 2. Рівень складності дефекту не враховується. 3. ПЗ функціонує в умовах максимально наближених до реальних. 4. ***Дефекти усуваються і нові не вносяться.***	$\lambda(t)=K[N_d - (i-1)]X_i$, X_i – час тестування від t_{i-1} (час виявленя і-1 дефекту ПЗ) до t_i.
Муси	Процес відновлення після відмов має пуассоновским розподіл	$\lambda_{,d}(\tau_{pp}) = \frac{1}{T_b}\exp\left(-\frac{K_m \tau_{pp}}{N_{def} T_b}\right)$
Ліпова	1. Всі дефекти рівноймовірні та їх прояв є незалежною подією. 2. Рівень складності дефекту не враховується. 3. $\lambda(t) = const.$ 4. ПЗ функціонує в умовах максимально наближених до реальних. 5. На i-му інтервалі тестування виявляється f_i, лише n_i із них усуваються.	$\lambda(t)=K(N_d-F_{i-1})$, $F_{i-1}=\sum_{j=1}^{i-1} n_j$ - загальна кількість скорегованих дефектів к моменту часу t_i.
Геометрична Моранди 1	1. Загальна кількість дефектів не обмежена.	$\lambda(t) = DK^{i-1}$, $\lambda(0) = D$, $0<K<1$, $\lambda(0)$ – змінюється в геометричній

	2. Виявлення дефектів не є рівноймовірним.	прогресії (зменшується)
Геометрична Моранди 2	3. Виявлення дефектів – процес незалежний від самих дефектів. 4. ПЗ функціонує в умовах максимально наближених до реальних. 5. $\lambda(t)$ утворює геометричну прогресію та функція між проявами дефектів є постійною.	$\lambda(t)=D\Phi^{i-1}$, число дефектів розподілено за пуассонівським законом із параметром $D\Phi^{i-1}$, $R(0) = D$, $0 < \Phi < 1$.
Геометрична Ліпова		$\lambda(t) = DK^{n_{i-1}}$, $R(0) = D$, $0<K<1$, n_{i-1} - загальне число дефектів, виявлених на всіх інтервалах тестування.
Шнайдевінда	1. Число дефектів на даному інтервалі не залежить від числа дефектів на других інтервалах. 2. Число виявлених дефектів зменшується від одного інтервалу часу до іншого. 3. Всі інтервали часу мають однакову довжину. 4. $\lambda(t)$ виявлення дефектів пропорційна числу дефектів у даний момент часу.	$D = (\alpha/\beta)[1-exp(-\beta)]$, $\Phi = exp(-\beta)$ головний чинник, що враховується – великий вплив на передбачення дефектів прояв більш пізніх ДППЗ
Вейбулла	Характеристики розподілу Вейбулла	$\lambda(t)=(a/b)(t/b)^{a-b}$, де $a>0$, $b>0$ – постійні моделі, $t\geq 0$ – є інтервал часу безвідмовної робот. Ймовірність відмов має функцію розподілу $\lambda(t)=1-exp\{-(t/b)^a\}$.

Одже виконаний аналіз множин МНПЗ, їх класифікацій дозволив сформулювати висновок про те, що найбільш пристосованими до вирішення питання врахування вторинних дефектів ПЗ є ймовірнісні моделі. Аналіз переліку припущень ймовірнісних моделей та їх функцій ризику дозволив визначити перелік моделей, для який є можливим зняти припущення про те, що

ДППЗ усуваються і нові не вносяться. Такими моделями є наступні: Джелінського-Моранди; Проста експоненційна; Шика-Уолвертона; Ліпова; Муси.

3.2 Розроблення моделей надійності програмних засобів з урахуванням вторинних дефектів

3.2.1 Сценарії внесення вторинних дефектів програмних засобів

Спираючись на досвід розроблення, рефакторінга та тестування програмних проектів і базуючись на твердженні про внесення вторинних дефектів в ході реалізації цих процесів, перелік можливих сценаріїв внесення вторинних дефектів є наступним:

$$M_i = \begin{cases} N_d - N_i, \\ N_d - N_i + K_i, \\ N_d - N_i + \Delta N_i, \\ N_d - N_i + K_i + \Delta N_i, \\ N_d - N_i + K_i^*, \\ N_d - N_i + \Delta N_i + K_i^*, \\ N_d - N_i + K_i^* + K_i^B, \\ N_d - N_i + K_i^* + K_i^B + \Delta N_i, \end{cases} \quad (3.12)$$

де, M_i - кількість програмних дефектів після i-го усунення виявлених дефектів ПЗ; N_d – залишкова кількість ДП після розробки ПЗ; N_i - число виявлених дефектів; K_i – кількість дефектів, внесених під час усунення виявлених (вторинні дефекти); ΔN_i - кількість неусунених ДП після їх виявлення; K_i^* - кількість дефектів, внесених в процесі оновлення ПЗ; K_i^B - кількість дефектів взаємодії оновлених і неоновлених програмних модулів. Короткий опис запропонованих сценаріїв наведено в таблиці 3.2.

Таблиця 3.2

Опис сценаріїв внесення вторинних дефектів

№ сценарію	Формальний запис сценарію внесення (усунення ДПЗ)	Опис сценарію внесення (усунення ДПЗ)
1	N_d - N_i	Всі первинні дефекти усуваються і нові не вносяться
2	N_d - N_i + K_i	Всі первинні дефекти усуваються і вносяться вторинні
3	N_d - N_i +ΔN_i	Частину первинних дефектів не усунуто
4	N_d - N_i + K_i +ΔN_i	Частину первинних дефектів не усунуто й внесені вторинні
5	N_d - N_i + K_i^*	Внесені додаткові дефекти в процесі оновлення ПЗ
6	N_d - N_i +ΔN_i+ K_i^*	Частину первинних дефектів не усунуто й внесені вторинні в процесі оновлення ПЗ
7	N_d - N_i + K_i^* +K_i^B	Внесені додаткові дефекти в процесі оновлення ПЗ і виникли додаткові дефекти в процесі взаємодії оновлених компонент ПЗ
8	N_d - N_i + K_i^* +K_i^B+ΔN_i	Частину первинних дефектів не усунуто, внесені вторинні в процесі оновлення ПЗ і виникли додаткові дефекти в процесі взаємодії оновлених компонент ПЗ

Множина сценаріїв спирається на перелік етапів життєвого циклу ПЗ, а саме етапу тестування, в ході якого дефекти виявляються й усуваються; етапу оновлення (рефакторінгу) для додавання нового функціоналу ПЗ або його

оптимізації. Це дає можливість виконати уточнення поведінки ПЗ в умовах відповідного сценарію за рахунок перебору співвідношень параметрів, що сценарій описують. Даний аналіз наведено в таблиці 3.3.

Таблиця 3.3

Розширений аналіз сценарії внесення (усунення) ДППЗ

№ сценарію	Сценарії			процеси			
	Формальний запис сценарію внесення (усунення ДПЗ)	Версії сценарії в	Варіанти співвідношення параметрів	виявлення	усунення	внесення вторинних	неусунення
1	N_d - N_i			+	+	–	–
2	N_d - N_i + K_i	2.1.	$N_i > K_i$	+	+	+	–
		2.2.	$N_i = K_i$	+	+	+	–
		2.3.	$N_i < K_i$	+	+	+	–
3	N_d - N_i +ΔN_i	3.1.	$N_i > \Delta N_i$	+	+	–	+
		3.2.	$N_i = \Delta N_i$	+	+	–	+
		3.3.	$N_i < \Delta N_i$	+	+	–	+
4	N_d - N_i + K_i +ΔN_i	4.1.	$N_i > K_i + \Delta N_i$	+	+	+	+
		4.2.	$N_i = K_i + \Delta N_i$	+	+	+	+
		4.3.	$N_i < K_i + \Delta N_i$	+	+	+	+
5	N_d - N_i + K_i^*	5.1.	$N_i > K_i^*$	+	+	+	–
		5.2.	$N_i = K_i^*$	+	+	+	–
		5.3.	$N_i < K_i^*$	+	+	+	–
6	N_d - N_i + K_i +ΔN_i	6.1.	$N_i > K_i^* + \Delta N_i$	+	+	+	+
		6.2.	$N_i = K_i^* + \Delta N_i$	+	+	+	+
		6.3.	$N_i < K_i^* + \Delta N_i$	+	+	+	+
7	N_d - N_i + K_i^* +K_i^B	7.1.	$N_i > K_i^* + K_i^B$	+	+	+	–
		7.2.	$N_i = K_i^* + K_i^B$	+	+	+	–
		7.3.	$N_i < K_i^* + K_i^B$	+	+	+	–
8	N_d - N_i + K_i^* +K_i^B+ΔN_i	8.1.	$N_i > K_i^* + K_i^B + \Delta N_i$	+	+	+	+
		8.2.	$N_i = K_i^* + K_i^B + \Delta N_i$	+	+	+	+
		8.3.	$N_i < K_i^* + K_i^B + \Delta N_i$	+	+	+	+

3.2.2 Модифікована модель Джелінські-Моранди

Модифікація функції ризику полягає в урахуванні параметру n^{in} - кількості дефектів внесених в процесі усунення виявлених ДП ПЗ. Вираз має вигляд:

$$\lambda(t_i)=K(N_d-i+1+n^{in}) \tag{3.13}$$

Виконаємо деякі перетворення для визначення напрямів оцінювання параметрів моделі (моделей) N_d та n^{in}.

Ймовірність того, що жоден ДП ПЗ не проявиться на проміжку від 0 до визначається виразом:

$$P(t)=\exp\left(-\int_0^t \lambda(t)\,dt\right) \tag{3.14}$$

Тоді розподіл набуде вигляду:

$$P(X_i)=\exp\left(-K\left(N_d-i+1+n^{in}\right)\right)X_i \tag{3.15}$$

а густина ймовірності відмов:

$$q(X_i)=K\left(N_d-i+1+n^{in}\right)\exp\left(-K\left(N_d-i+1+n^{in}\right)\right)X_i \tag{3.16}$$

У відповідності до того, що всі дефекти є рівноймовірними та їх прояв є подією незалежною, функція правдоподібності має вигляд:

$$L(X_1,\ldots,X_n)=\prod_{i=1}^{n+n^{in}} q(X_i) \tag{3.17}$$

Прологарифмуваши вираз (3.8), отримаємо:

$$\ln L=\sum_{i=1}^{n+n^{in}}\left(\ln\left(K\left(B-i+1+n^{in}\right)\right)-K\left(B-i+1+n^{in}\right)X_i\right) \tag{3.18}$$

Знайдемо частинні похідні $\frac{\partial L}{\partial K}$, і $\frac{\partial L}{\partial N_{ДП}}$ прирівняємо їх до нуля та отримаємо систему рівнянь для знаходження оцінки максимальної правдоподібності величин K і N_d:

$$\begin{cases}\dfrac{\partial \ln L}{\partial K}=\displaystyle\sum_{i=1}^{n+n^{in}}\left(\frac{1}{K}-\left(N_d-i+1+n^{in}\right)X_i\right),\\ \dfrac{\partial \ln L}{\partial N_d}=\displaystyle\sum_{i=1}^{n+n^{in}}\left(\frac{1}{BN_d\ i+1+n^{in}}-K\,X_i\right).\end{cases} \tag{3.19}$$

$$\begin{cases}K=\dfrac{n+n^{in}}{\displaystyle\sum_{i=1}^{n+n^{in}}\left(N_d-i+1+n^{in}\right)X_i},\\ \displaystyle\sum_{i=1}^{n+n^{in}}\frac{1}{N_d-i+1+n^{in}}=\frac{\left(n+n^{in}\right)\displaystyle\sum_{i=1}^{n+n^{in}}X_i}{\displaystyle\sum_{i=1}^{n+n^{in}}\left(N_d\ i+1+n^{in}\right)X_i}.\end{cases} \tag{3.20}$$

3.2.3 Модифікована проста експоненційна модель

Виконаємо модифікацію функції ризику простої експоненційної моделі:

$$\lambda(t) = K\left(N_d - N(t) + n^{in}\right) \tag{3.21}$$

Знайдемо похідну обох частин цього рівняння за часом:

$$\frac{d\lambda(t)}{dt} = -K\frac{dN(t)}{dt} \tag{3.22}$$

Враховуючи, що $\lambda(t) = \frac{dN(t)}{dt}$ - число дефектів, виявлених за одиницю часу, отримаємо диференціальне рівняння для $\lambda(t)$:

$$\frac{d\lambda(t)}{dt} + K\,\lambda(t) = 0 \tag{3.23}$$

Враховуючи початкові умови $N(0)=0$ і $\lambda(0)=K(N_d + n^{in})$, маємо розв'язок цього рівняння:

$$\lambda(t) = K\left(N_d + n^{in}\right)\exp(-Kt) \tag{3.24}$$

Введемо означення:

$$a = \ln\left(K\left(N_d + n^{in}\right)\right) \tag{3.25}$$

$$b = -K, \tag{3.26}$$

тоді маємо:

$$\lambda(t) = \exp(a + bt) \tag{3.27}$$

Логарифмуючи обидві частини рівняння (3.27) і переходячи до дискретного часу, отримуємо систему рівнянь:

$$\ln\lambda(t_i) = a + bt_i; \quad i = \overline{1,\ n + n^{in}} \tag{3.28}$$

Систему (3.20) запишемо у векторно-матричному вигляді:

$$AX = C, \text{де } A = \begin{pmatrix} 1 & t_1 \\ 1 & t_2 \\ \dots & \dots \\ 1 & t_{n+n^{in}} \end{pmatrix}, X = \begin{pmatrix} a \\ b \end{pmatrix}, C = \begin{pmatrix} \ln\lambda(t_1) \\ \ln\lambda(t_2) \\ \dots \\ \ln\lambda(t_{n+n^{in}}) \end{pmatrix} \tag{3.29}$$

Використовуючи метод найменших квадратів, приведемо ці рівняння до нормального вигляду: $A^{\mathrm{T}} A X = A^{\mathrm{T}} C$.

$$X = \left(A^{\mathrm{T}} A\right)^{-1} A^{\mathrm{T}} C. \tag{3.30}$$

Виконаємо ряд перетворень для вирішення системи (3.30):

$$A^{\mathrm{T}} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_{n+n^{in}} \end{pmatrix},$$

$$A^{\mathrm{T}} A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_{n+n^{in}} \end{pmatrix} \begin{pmatrix} 1 & t_1 \\ 1 & t_2 \\ \dots & \dots \\ 1 & t_{n+n^{in}} \end{pmatrix} = \begin{pmatrix} n + n^{in} & \sum\limits_{i=1}^{n+n^{in}} t_i \\ \sum\limits_{i=1}^{n+n^{in}} t_i & \sum\limits_{i=1}^{n+n^{in}} t_i^2 \end{pmatrix},$$

$$\det\left(A^{\mathrm{T}}A\right)=\left(n+n^{in}\right)\sum_{i=1}^{n+n^{in}}t_i^{\,2}-\left(\sum_{i=1}^{n+n^{in}}t_i\right)^2,$$

$$\left(A^{\mathrm{T}}A\right)^{-1}=\frac{1}{\det\left(A^{\mathrm{T}}A\right)}\begin{pmatrix}\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2} & -\sum\limits_{i=1}^{n+n^{in}}t_i\\ -\sum\limits_{i=1}^{n+n^{in}}t_i & n+n^{in}\end{pmatrix},$$

$$\left(A^{\mathrm{T}}A\right)^{-1}A^{\mathrm{T}}=\frac{1}{\det\left(A^{\mathrm{T}}A\right)}\begin{pmatrix}\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2} & -\sum\limits_{i=1}^{n+n^{in}}t_i\\ -\sum\limits_{i=1}^{n+n^{in}}t_i & n+n^{in}\end{pmatrix}\begin{pmatrix}1 & 1 & \dots & 1\\ t_1 & t_2 & \dots & t_{n+n^{in}}\end{pmatrix}=$$

$$=\frac{1}{\det\left(A^{\mathrm{T}}A\right)}\begin{pmatrix}\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-t_1\sum\limits_{i=1}^{n+n^{in}}t_i & \sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-t_2\sum\limits_{i=1}^{n+n^{in}}t_i & \dots & \sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-t_{n+n^{in}}\sum\limits_{i=1}^{n+n^{in}}t_i\\ t_1\left(n+n^{in}\right)-\sum\limits_{i=1}^{n+n^{in}}t_i & t_2\left(n+n^{in}\right)-\sum\limits_{i=1}^{n+n^{in}}t_i & \dots & t_{n+n^{in}}\left(n+n^{in}\right)-\sum\limits_{i=1}^{n+n^{in}}t_i\end{pmatrix}.$$

Враховуючи, що $X=\left(A^{\mathrm{T}}A\right)^{-1}A^{\mathrm{T}}C=\begin{pmatrix}a\\ b\end{pmatrix}$, знайдемо a и b.

$$\left(A^{\mathrm{T}}A\right)^{-1}A^{\mathrm{T}}C=\frac{1}{\det\left(A^{\mathrm{T}}A\right)}\times$$

$$\times\begin{pmatrix}\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-t_1\sum\limits_{i=1}^{n+n^{in}}t_i & \sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-t_2\sum\limits_{i=1}^{n+n^{in}}t_i & \dots & \sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-t_{n+n^{in}}\sum\limits_{i=1}^{n+n^{in}}t_i\\ t_1\left(n+n^{in}\right)-\sum\limits_{i=1}^{n+n^{in}}t_i & t_2\left(n+n^{in}\right)-\sum\limits_{i=1}^{n+n^{in}}t_i & \dots & t_{n+n^{in}}\left(n+n^{in}\right)-\sum\limits_{i=1}^{n+n^{in}}t_i\end{pmatrix}\begin{pmatrix}\ln\lambda\left(t_1\right)\\ \ln\lambda\left(t_2\right)\\ \dots\\ \ln\lambda\left(t_{n+n^{in}}\right)\end{pmatrix}. \quad (3.31)$$

$$a=\frac{\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}\sum\limits_{i=1}^{n+n^{in}}\ln\lambda\left(t_1\right)-\sum\limits_{i=1}^{n+n^{in}}t_i\sum\limits_{i=1}^{n+n^{in}}\left(t_i\ln\lambda\left(t_i\right)\right)}{\left(n+n^{in}\right)\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-\left(\sum\limits_{i=1}^{n+n^{in}}t_i\right)^2},$$

,

$$K=-b=\frac{\sum\limits_{i=1}^{n+n^{in}}t_i\cdot\sum\limits_{i=1}^{n+n^{in}}\ln\lambda\left(t_i\right)-\left(n+n^{in}\right)\cdot\sum\limits_{i=1}^{n+n^{in}}\left(t_i\cdot\ln\lambda\left(t_i\right)\right)}{\left(n+n^{in}\right)\cdot\sum\limits_{i=1}^{n+n^{in}}t_i^{\,2}-\left(\sum\limits_{i=1}^{n+n^{in}}t_i\right)^2}$$

. (3.32)

Із (3.17) отримуємо $N_{ДП} = \frac{\exp a}{K} - n^{ВН}$ або

$$N_d = \frac{\exp\left(\frac{\sum_{i=1}^{n+n^{in}} t_i^2 \cdot \sum_{i=1}^{n+n^{in}} \ln\lambda(t_i) - \sum_{i=1}^{n+n^{in}} t_i \sum_{i=1}^{n+n^{in}} \left(t_i \cdot \ln\lambda(t_i)\right)}{\left(n+n^{in}\right)\cdot \sum_{i=1}^{n+n^{in}} t_i^2 - \left(\sum_{i=1}^{n+n^{in}} t_i\right)^2}\right)}{K} - n^{in} \quad (3.33)$$

Подібні перетворення можливо виконати із іншими модифікованими функціями ризику (таблиця 3.4) ймовірнісних моделей для отримання оцінок параметрів $N_{ДП}$ та $n^{вн}$.

Таблиця 3.4

Модифікація функцій ризику ймовірнісних МНПЗ

МНПЗ	Функції ризику	Модифіковані функції ризику
Джелінського-Моранди	$\lambda(t)=K(N_d - (i-1))$	$\lambda(t)=K(N_d-i+1+n^{in})$
Проста експоненційна	$\lambda(t)=K(N_d - N(t))$	$\lambda(t)=K(N_d - N(t)+n^{in})$
Шика-Уолвертона	$\lambda(t)=K(N_d - i+1)X_i$	$\lambda(t)=K(N_d - i+1+n^{in})X_i$
Модель Ліпова	$\lambda(t)=K(N_d - F_{i-1})$	$\lambda(t_i)=K(N_d - F_{i-1}+n^{in})$
Модель Муси	$\lambda(t)=K(N_d - F_{i-1})$	$\lambda(t_i)=K(N_d - F_{i-1}+n^{in})$

3.3 Комплексування моделей надійності програмних засобів з урахуванням вторинних дефектів

Принцип комплексування моделей надійності програмних засобів полягає у їх спрямованому поєднанні з метою використання переваг моделей різних

класифікаційних ознак при оцінюванні надійності розроблюваного і супроводжуваного ПЗ.

Відповідно до цього визначення з метою комплексування моделей можливо використання їх модифікації, в тому числі з урахуванням фактору внесення і прояву вторинних дефектів.

Наведемо приклади комплексування МНПЗ.

Приклад 1. Комплексування МНПЗ запропонованих М. Холстедом [193], Г. Міллсом Дж.Д. Мусою [252]. На рисунку 3.3 зображено схему послідовного поєднання використання МНПЗ різних класифікаційних ознак.

Рис. 3.3 Схема комплексування МНПЗ Холстеда, Міллса, Муси

Зміст даного комплексування наступний:

1. На першому етапі здійснюється апріорна оцінка початкового числа ДП ПЗ, що знаходяться в програмах за допомогою емпіричної моделі оцінки надійності ПЗ М. Холстеда. Застосування цієї моделі дозволяє визначити наступні метричні характеристики програм:

- словник програми

$$\eta = \eta_1 + \eta_2 \tag{3.34}$$

де η_1 і η_2 – число типів відповідно операторів й операндів, що з'являються в даній реалізації програми;

- оцінку довжини програми

$$N = \eta_1 \log_2 \eta_1 + \eta_2 \log_2 \eta_2 ; \tag{3.35}$$

– обсяг програми

$$V = N \log_2 \eta ; \tag{3.36}$$

– залишковий рівень дефектів в програмі (після розробки)

$$N_{def} = \frac{V}{3000}, \tag{3.37}$$

де E_{crit} = 3000 - програмне значення здатності людського мозку, що характеризує його можливості обробляти п'ять "об'єктів", отримане для англійської мови;

– залишковий рівень помилок комплексу програм

$$N_{def\_cp} = \frac{V}{3000} 2 \log_5 \frac{V}{3000}, \tag{3.38}$$

– залишковий рівень суміші розгалуженого і лінійного тексту

$$N_{def\_mix} = \frac{4 + K_r}{3000}, \tag{3.39}$$

де $K_r = V_l / V_p$ - відношення обсягу лінійного тексту до вихідного обсягу програми.

2. На другому етапі здійснюється тестування ПЗ, що полягає в скануванні всіх гілок і сегментів та виявлених при цьому ДП ПЗ. Оцінка числа ДП ПЗ може бути уточнена з використанням статистичної моделі Г.Міллса:

$$N_{def} = \frac{\left(N_{def\_in} + N_{def\_add}\right)}{N_{def\_add}}, \tag{3.40}$$

де N_{def_in} і N_{def_add} - число виявлених власних і спеціально внесених в програму дефектів. При цьому передбачається, що N_{def_in}, не перевищує прогнозованого числа дефектів до початку тестування, визначеного метриками Холстеда.

3. На третьому етапі здійснюється оцінка параметрів λ_d і $\Delta\lambda_d$ для ПЗ, що тестуються на реальному об'єкті з використанням вхідних даних, що імітують реальні умови функціонування у відповідності з виразами (3.5), (3.6) модифікованої моделі Дж .Д. Муси.

Приклад 2. Комплексування МНПЗ запропонованих М. Холстедом, фірмою IBM та Джелінським-Морандо. На рисунку 3.4 зображено схему послідовного поєднання використання МНПЗ різних класифікаційних ознак.

Рис. 3.4 Схема комплексування МНПЗ Холстеда, фірми IBM, Джелінського-Моранди

Зміст даного комплексування наступний:

1.На першому етапі здійснюється апріорна оцінка початкового числа ДП ПЗ, що знаходяться в програмах за допомогою емпіричної моделі оцінки надійності ПЗ М. Холстеда (приклад комплексування МНПЗ №1).

2. На другому етапі здійснюється апріорне оцінювання параметру n^{in} із використанням емпіричної моделі фірми IBM. Значення параметру N_d уточнюється.

$$n^{in} = N_{d_{i-1}} - N_{d_i}, \tag{3.41}$$

де $N_{ДП_i}$ = ЗЧЗ$_i$ = $\alpha\times$ МЧЗ$_i$ + $\gamma\times ММЗ_{i,,}$ ЗЧЗ – загальне число змін, що вносяться у програмні модулі, i – порядковий номер оновлення ПЗ; МЧЗ – модулі чисельних змін модулі (більше 10 змін); ММЗ – модулі із малим числом змін (менше 10 змін), $МЧЗ_i = 0,15\times ММЗ_i + 0,06\times СВМ_i$; $ММЗ_i = 0,9\times НМ_i + 0,15\times СВМ_i$; НМ – нові модулі; СВМ – старі виправлені модулі; Коефіцієнти α і γ показують середню кількість змін внесених на один модуль у відповідних групах МЧЗ та ММЗ (за замовчуванням α = 23, γ = 2).

3. На третьому етапі задіюється модифікована ймовірнісна модель Джелінського-Моранди для оцінки функції ризику $\lambda_d(t)$:

$$\lambda_d(t)=K(N_d - i + 1 + n^{in}) \qquad (3.42)$$

3.4 Послідовність прогнозування кількості вторинних дефектів по статистичним даним

Послідовність прогнозування кількості вторинних дефектів базуючись на статистичних даних (Рис. 3.5) складається з наступних етапів:

Етап 1 – Збір статистичних даних про ДППЗ.

Початкові дані етапу наступні:

− специфікація системних вимог (system requirements specification) - опис системних функцій, опис сценаріїв функціонування, функціональні вимоги, вимоги до інтерфейсів, продуктивності, оточуючого середовища, інформаційної безпеки, надійності;

− специфікація вимог до ПЗ та детальний опис ПЗ (software requirements specification, software detailed design);

Результатами виконання етапу є статистичні дані про ДППЗ на основі аналізу звітів про етапи тестування, а саме звіт про огляди детального дизайну ПЗ, статичний аналіз коду, код-ревью, юніт-тестування, функціональне (поведінкове) тестування, інтеграційне тестування (в тому числі з внесенням

дефектів), валідаційне тестування та інші.

Етап 2 – Побудова залежності числа ДППЗ від часу (кореляційне поле).

Початковими даними етапу є статистичні дані про ДППЗ систематизовані за відношенням до етапу тестування та часом.

Результатами виконання етапу є побудоване кореляційне поле.

Етап 3 – визначення виду лінії регресії та рівняння лінії регресії.

Початковими даними третього єтапу є побудоване кореляційне поле.

У результаті проходження даного етапу отримуємо рівняння лінії регресії.

Етап 4 – Визначення вибіркового коефіцієнту кореляції (перевірка тісноти кореляційного зв’язку)

Початковими даними є статистичні дані про ДППЗ та рівняння лінії регресії.

Результатами виконання етапу є коефіцієнт кореляції.

Етап 5 – Обчислення прогнозованого числа вторинних дефектів на досліджуваних інтервалах часу (n^{in}).

Початковими даними останнього етапу є статистичні дані про ДППЗ, лінія регресії, рівняння лінії регресії та коефіцієнт кореляції.

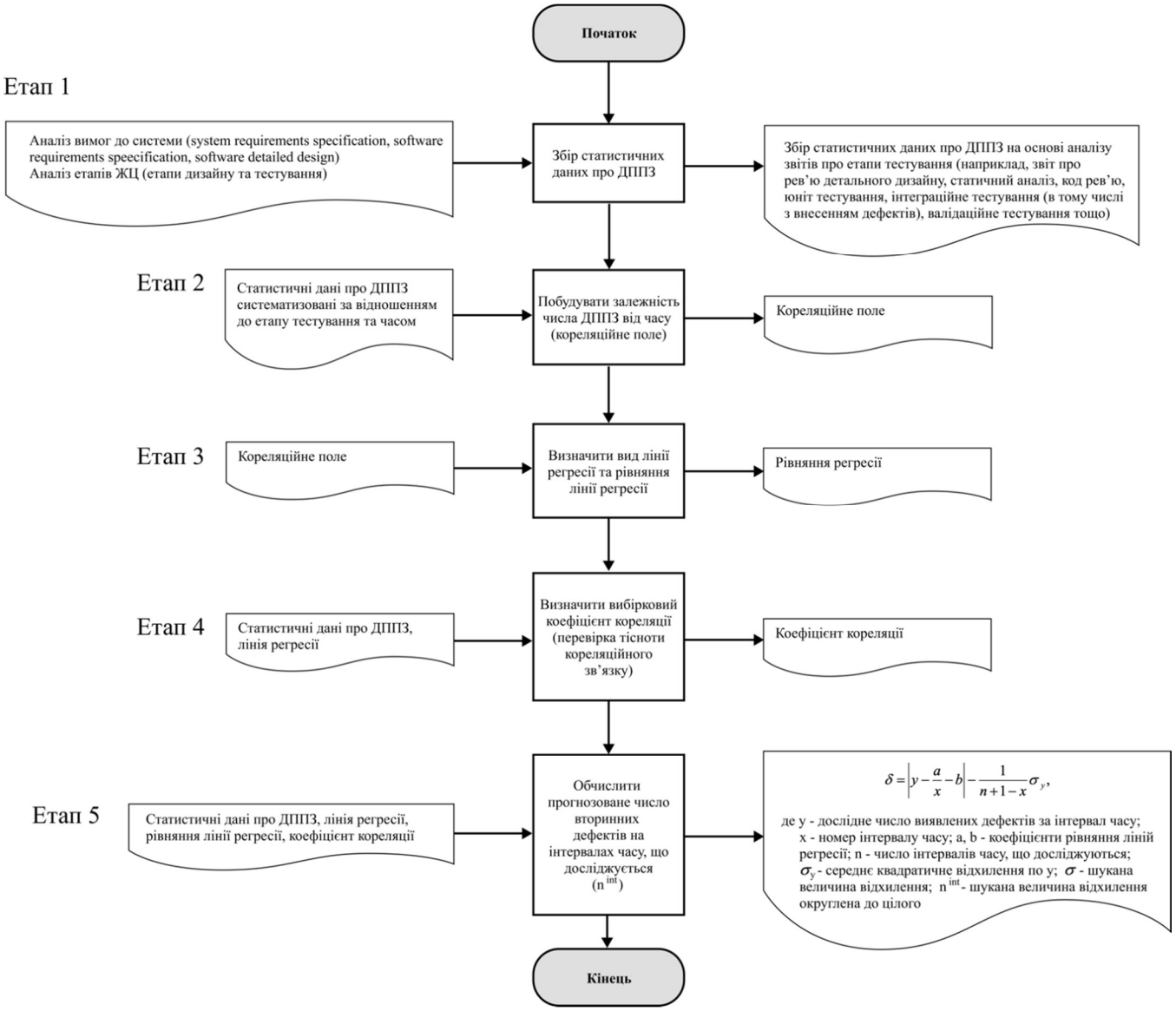


Рис. 3.5 Послідовність прогнозування кількості вторинних дефектів по статистичним даним

Послідовність обчислення прогнозованого числа вторинних дефектів ПЗ наступна:

1. Обчислити модуль різниці між значенням кількості дефектів за певний проміжок часу дефектів і значенням функції регресії в моменти визначення кількості дефектів за проміжок часу.

2. Число вторинних дефектів знаходимо як різницю результату, отриманого при виконанні першого пункту й середнього квадратичного відхилення статистики дефектів в досліджуваний інтервал часу, помноженого на коефіцієнт $\frac{1}{n+1-i}$, де – n число інтервалів тестування (число виявлених дефектів), i- порядковий номер інтервалу (виявленого дефекту). Результат округляється до цілих.

Результатами виконання етапу є n^{in} - шукана величина кількості вторинних дефектів, обчислена за виразом

$$\delta = \left| y - \frac{a}{x} - b \right| - \frac{1}{n+1-x}\sigma_y, \tag{3.43}$$

де y - дослідне число виявлених дефектів за інтервал часу; x – номер інтервалу часу; a, b – коефіцієнти рівняння лінії регресії; n – число інтервалів часу, що досліджуються; σ_y - середнє квадратичне відхилення по y; δ - шукана величина відхилення (n^{in} - шукана величина відхилення округлена до цілого).

3.4.1 Застосування послідовності прогнозування кількості вторинних дефектів по статистичним даним

Застосуємо послідовність прогнозування кількості вторинних дефектів базуючись на статистичних даних з метою отримання їх кількісної оцінки за

результатами функціонального тестування (поведінкового тестування) електронного проекту модуля LM (Logic Module) ЦІКП RadICS.

Розглянемо статистику виявлених ДППЗ для першої релізної версії проєкту. Статистичні дані наведено в таблиці 3.5.

Таблиця 3.5.

Статистика ДППЗ

Місяць	1	2	3	4	5	6	7	8	9	10	11	12
Число ДППЗ	14	12	8	7	7	6	5	4	3	2	1	1

1. Побудуємо кореляційне поле за статистичними даними (Рис.3.6).

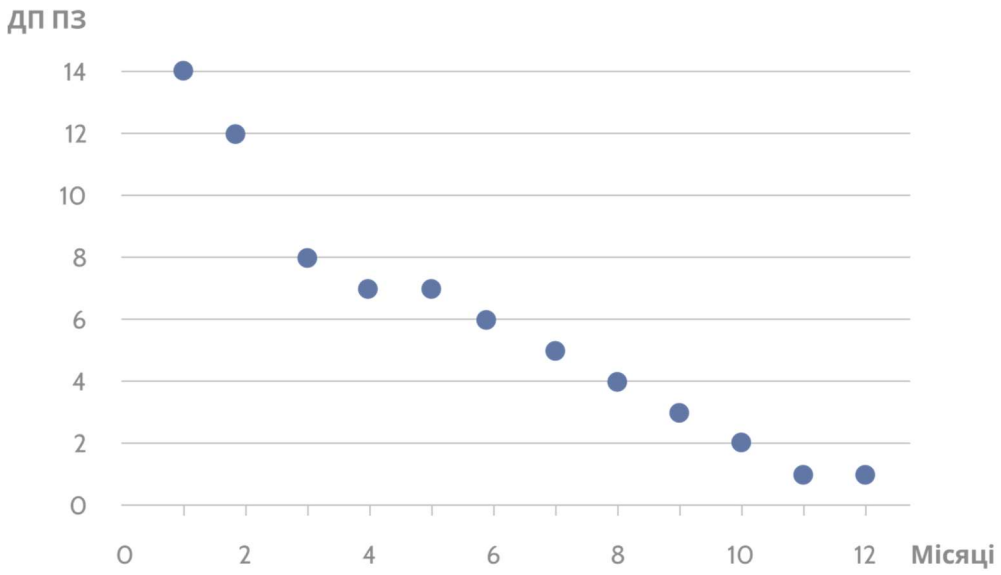


Рис. 3.6 Кореляційне поле статистики дефектів

2. За допомогою метода найменших квадратів знаходимо рівняння лінії регресії. $y = \frac{12,66}{x} + 2,31.$

3. Побудуємо лінію регресії за даними кореляційного поля (Рис.3.7).

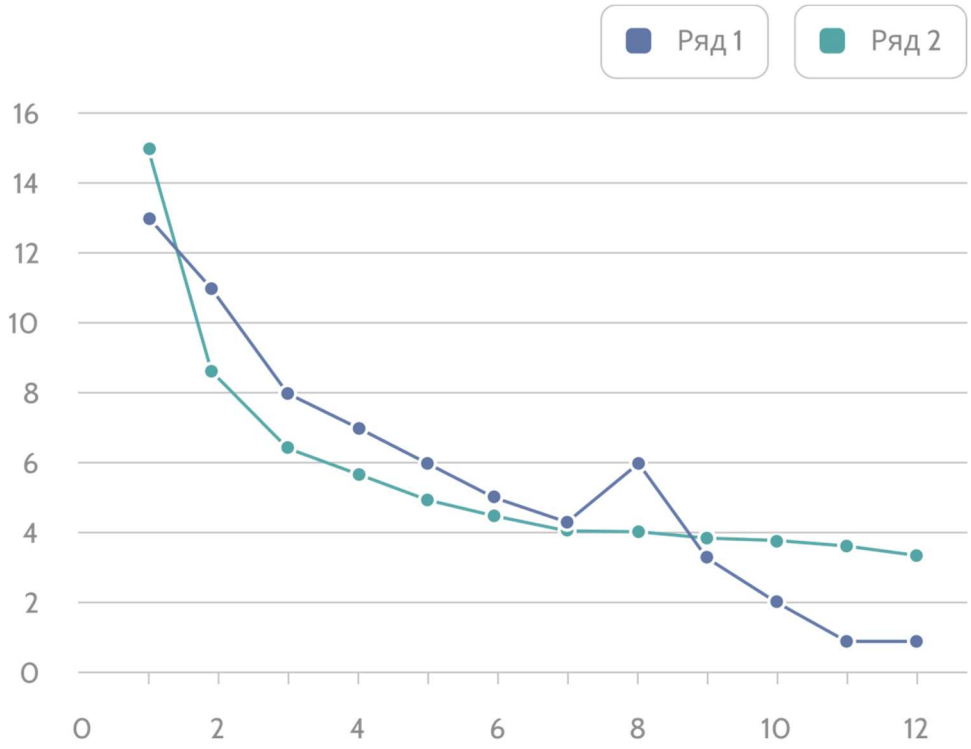


Рис. 3.7 Лінія регресії (ряд 2)

4. Знаходимо значення n^{in} із використанням виразу (3.43),

де y – дослідне число ДП ПЗ за інтервал часу, x – порядковий номер інтервалу часу, a та b – коефіцієнти рівняння лінії регресії $y = a + \frac{b}{x}$ ($a = 2{,}31$, $b = 12{,}66$), n – число інтервалів часу, σ_y – середньоквадратичне відхилення по y, δ – шукана величина.

Таблиця 3.6

Результати розрахунку числа вторинних дефектів

x	y	$a + \frac{b}{x}$	$\left\|y - a - \frac{b}{x}\right\|$	$\left\|y - a - \frac{b}{x}\right\| - \frac{1}{13 - x}\sigma_y$	n^{in}
1	13	14,96916	1,969157	1,667813	2
2	11	8,639352	2,360648	2,031909	2
3	8	6,529417	1,470583	1,10897	1

x	y	$a+\frac{b}{x}$	$\left\|y-a-\frac{b}{x}\right\|$	$\left\|y-a-\frac{b}{x}\right\|-\frac{1}{13-x}\sigma_y$	n^{in}
4	7	5,474449	1,525551	1,123758	1
5	6	4,841469	1,158531	0,706515	1
6	5	4,419482	0,580518	0,063928	
7	4	4,118063	0,118063	–0,48463	
8	6	3,891998	2,108002	1,384776	1
9	3	3,71617	0,71617	–0,18786	
10	2	3,575508	1,575508	0,370132	
11	1	3,460421	2,460421	0,652356	
12	1	3,364514	2,364514	–1,25161	

Результати розрахунку числа вторинних дефектів наведено в таблиці 3.6.

Інтенсивності ДП ПЗ обчислені з використанням МНПЗ Джелінського-Моранди та використано модифіковану функцію ризику цієї моделі з метою врахування вторинних дефектів.

Результати наведено в таблиці 3.7.

Таблиця 3.7.

Результати розрахунку інтенсивності прояву ДППЗ λ_d

Інтервал часу	Виявленні дефекти	Прогнозоване число вторинних дефектів	λ_d без урахування вторинних дефектів	λ_d з урахуванням вторинних дефектів
1	13	2	0,01358	0,013979
2	11	2	0,011183	0,011583
3	8	1	0,009286	0,009486
4	7	1	0,007788	0,007988
5	6	1	0,00649	0,00669
6	5		0,005392	0,005392
7	4		0,004493	0,004493
8	6	1	0,003495	0,003694

Інтервал часу	Виявленні дефекти	Прогнозоване число вторинних дефектів	λ_d без урахування вторинних дефектів	λ_d з урахуванням вторинних дефектів
9	3		0,002596	0,002596
10	2		0,002097	0,002097
11	1		0,001797	0,001797
12	1		0,001598	0,001598
Середня інтенсивність прояву дефектів			0,005816	0,005949
Середня зміна інтенсивності прояву дефектів			0,001089	0,001126

3.5 Висновки за розділом

1. В розділі удосконалено ймовірнісні моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування, рефакторінгу і супроводу, та аналізу різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання кількісних показників. Вибір множини МНПЗ для модифікації з урахуванням прояву вторинних дефектів базується на результатах аналізу науково-методичного апарату теорії надійності програмного забезпечення, в основу якого покладено розгляд встановлення розширеного переліку класифікацій МПНЗ за різними ознаками. Встановлено, що базовими класифікаціями основних МНПЗ є класифікації Хетча, Гоела, Фатуєва-Благодатських, Полоннікова-Нікандрова. Аналіз переліку припущень для побудови МНПЗ та їх функцій ризику дозволив встановити перелік моделей для подальшої модифікації, а саме: Джелінського-Моранди; простої експоненційної; Шика-Уолвертона; моделі Муси, моделі Ліпова.

2. Модифікація моделі Муси дозволила зняти одне з основних припущень про не змінність параметрів моделювання систем досліджуваного класу та реалізувати встановлений принцип визначення змінних параметрів відмов за різними ознаками і відновлень компонентів і систем за рахунок впровадження

ідеї про умовну апроксимацію функцій, що описують параметри моделі, наприклад $\lambda(t)$ – інтенсивність прояву дефекту або $\mu(t)$ – інтенсивність відновлення після прояву, кусково-неперервною функцією. При цьому після зміни станів системи (моделі) відбувається стрибкоподібна зміна величин інтенсивностей λ або μ на певні значення $\Delta\lambda$ або $\Delta\mu$. Модифікація моделі Муси дозволила отримати аналітичні вирази для оцінювання параметрів $\Delta\lambda$ та $\Delta\mu$.

3. Результатом аналіза досвіду розроблення, рефакторінга та тестування програмних проєктів та встановлених фактів внесення вторинних дефектів в ході реалізації цих процесів стало розроблення переліку можливих сценаріїв внесення та усунення вторинних дефектів ПЗ. Кожен сценарій має свій опис, наприклад: всі первинні дефекти усуваються і вносяться вторинні; частину первинних дефектів не усунуто й внесені вторинні; частину первинних дефектів не усунуто й внесені вторинні в процесі оновлення ПЗ; внесені додаткові дефекти в процесі оновлення ПЗ і виникли додаткові дефекти в процесі взаємодії оновлених компонент ПЗ. Дана множина сценаріїв дає можливість виконати уточнення поведінки ПЗ в умовах відповідного сценарію за рахунок перебору співвідношень параметрів, які даний варіант сценарію описують.

3. Одержано модифіковані функції ризиків обраних МНПЗ, а саме: Джелінського-Моранди; простої експоненційної; Шика-Уолвертона; моделі Муси, моделі Ліпова, які враховують можливість внесення вторинних дефектів ПЗ і дозволяють одержувати оцінки інтенсивності прояву ДППЗ з урахуванням означеного фактору.

4. Запропонована послідовність прогнозування кількості вторинних дефектів об’єднала попередні результати і дозволяє отримувати оцінку кількості вторинних дефектів та уточнювати надійнісні параметри ПЗ, зокрема інтенсивність прояву ДП ПЗ. Порівняння результатів обчислення інтенсивності прояву ДППЗ дає висновк про те, що значення означеного параметру параметру уточнюється до 5%.

5. Результатами аналізу основних переваг досліджуваних МНПЗ стали

варіанти їх комплексування для більш точного оцінювання надійності розроблюваного і супроводжуваного ПЗ. До застосування рекомендовано комплексування МНПЗ М. Холстеда, М. Міллса, Дж. Муси та М. Холстеда, фірми IBM, Джелінського-Моранди. Основні положення розділу викладені у публікаціях автора [80, 87, 147, 151, 152, 153, 154, 155, 156, 159, 165, 166, 170, 171, 210, 227, 235].

РОЗДІЛ 4. МОДЕЛІ ТА МЕТОД ОЦІНЮВАННЯ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПРОГРАМНО-ТЕХНІЧНИХ КОМПЛЕКСІВ ЗІ СТРУКТУРНО-ВЕРСІЙНОЮ НАДМІРНІСТЮ

4.1 Принципи розроблення багатофрагментних марковських моделей

4.1.1 Систематизація змінних параметрів

Під час розроблення метода оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю виконано систематизацію змінних параметрів, що враховують відповідні моделі (рисунок 4.1). Для надання методу даної ознаки були проаналізовані основні групи причин прояву множин дефектів.

Перша група причин призводить до прояву ДФ АК, що враховано в моделях параметрами λ_p (інтенсивністю прояву ДФ АК), μ_p (інтенсивністю відновлення після прояву ДФ АК), запасом компонент для відновляння (ЗКВн). До даної групи можуть бути віднесені такі причини як старіння обладнання та обмеження ресурсів на його відновлення.

Друга група причин, а саме старіння ПЗ (software aging), помилки технічного завдання на розробку ПЗ, помилки детального опису ПЗ, нехтування правилами кодування, помилки бібліотечних компонент, що задіяні при розробленні ПЗ, помилки засобів компіляції інтегрованих середовищ розробки (Integrated Development Environment (IDE)) та обмежені ресурси на тестування ПЗ тощо. Дані причини призводять до прояву дефектів проектування ПЗ (ДП ПЗ), що в моделях враховується наступними параметрами: λ_d (інтенсивністю прояву ДП ПЗ) та величиною її зміни $\Delta\lambda_d$ після усунення ДП ПЗ, μ_d інтенсивністю відновлення після прояву ДП ПЗ та величини її зміни $\Delta\mu_d$.

Рис. 4.1 Систематизація змінних параметрів

Третя група призводить до прояву дефектів проектування АК, до них можливо віднести наступні: помилки технічного завдання, помилки детального дизайну АК (HW Design) та помилки його аналізу, обмеження ресурсу на тестування АК окремо та інтегрованих систем (АК+ПК). Для урахування цих дефектів використано параметри: $\lambda_{d(A)}$ інтенсивність прояву ДПА та величина її зміни $\Delta\lambda_{d(A)}$ після усунення ДПА, $\mu_{d(A)}$ інтенсивність відновлення після прояву ДПА та величини її зміни $\Delta\mu_{d(A)}$.

Четверта група причин: навмисні (ненавмисні) впливи фізичної природи – механічні; кліматичні; електромагнитні; радіаційні та інш., призводять до прояву дефектів взаємодії фізичної природи (ДВФ) та враховуються набором параметрів - $\lambda_{int(P)}$ та $\mu_{int(P)}$, де $\lambda_{int(P)}$ – інтенсивність прояву ДВФ, $\mu_{int(P)}$ – інтенсивність відновлення після прояву ДВФ.

Остання п’ята група влючає в себе інформаційні впливи (помилкові дії персоналу, хакерські атаки, спам та інш., призводять до прояву дефектів взаємодії інформаційної природи (ДВІ) та враховуються набором параметрів: $\lambda_{int(I)}$ і $\mu_{int(I)}$.

На рисунках 4.2 – 4.3 представлено розроблені узагальнені моделі зміни параметрів. Процес прояву ДП ПЗ та зміни параметрів λ_d (4.1) і λ_{int} (4.2), де λ_{int}є узагальненим виразом інтенсивності прояву групи дефектів взаємодії (ДВ), зображено на рисунку 4.2.

$$\lambda_d(t_i + 1) = \lambda_d(t_i) - \Delta\lambda_d \quad (4.1)$$

$$\lambda_{int}(t_j + 1) = \lambda_{int}(t_j) - \Delta\lambda_{int} \quad (4.2)$$

Процес впливу прояву дефектів проектування, залежно від вхідних даних $X(t_i)$, та задіяння вразливості, залежно від вхідних даних $A(t_j)$, на зміну вихідного результату $Z_p(t_i) \neq Z_0(t_i)$, $Z_p(t_j) \neq Z_0(t_j)$ наведено на рисунку 4.3. Результатом таких процесів є відхилення одержаних результатів обчислювального процесу від очікуваних.

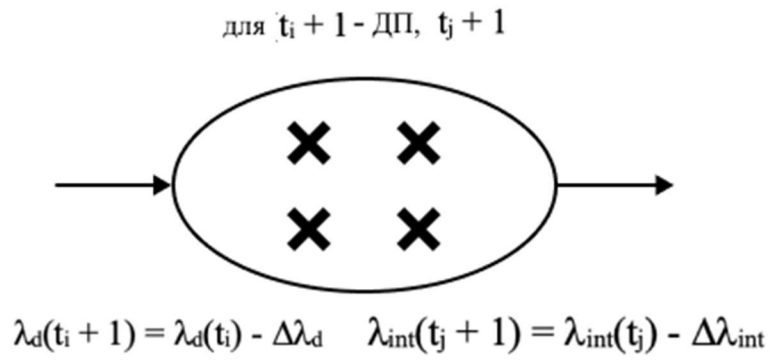


Рис. 4.2 Модель прояву та усунення ДП ПЗ і ДВ

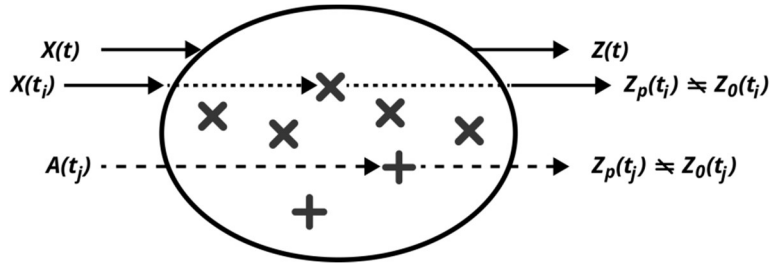


Рис. 4.3 Модель прояву дефектів та вразливостей

4.1.2 Сценарії зміни параметрів в моделях

При побудові марковських ланцюгів виконується умовна апроксимація функції λ(t) або μ(t) кусково-неперервною функцією. При цьому після зміни станів системи відбувається стрибкоподібна зміна величин інтенсивностей λ або μ на певні значення Δλ або Δμ. Слід зазначити, що параметри Δλ і Δμ можуть бути як постійними величинами і приводити до лінійного характеру зміни відповідних інтенсивностей, так і змінними. В останньому випадку характер зміни інтенсивностей прояви дефектів і відновлення має нелінійний характер. Вид нелінійності можна визначити після дослідження характеру і "ваги" відповідного дефекту. З урахуванням того, що надійністні характеристики ПТК досліджуються в

роботі з використанням множин параметрів, що наведено вище, а надійністні параметри ПЗ та їх коефіцієнти в ході моделювання можуть набувати сталих та змінних значень (const & var) - можливі комбінації цих параметрів та коефіцієнтів зведено у таблицю 4.1.

Таблиця 4.1

Комбінації параметрів та коефіцієнтів (λ_d, $\Delta\lambda_d$, μ_d, $\Delta\mu_d$)

№ п/п	λ_d	μ_d	$\Delta\lambda_d$	$\Delta\mu_d$
1	const	const	0	0
2	var	const	const	0
3	var	const	var	0
4	const	var	0	const
5	const	var	0	var
6	var	var	const	const
7	var	var	const	var
8	var	var	var	const
9	var	var	var	var

За допомогою комбінацій наведених в таблиці 4.1 можна описати зміну параметрів потоків відмов і відновлень як АК, так і ПК ПТК. Однак умови розв'язуваної задачі обмежують область моделювання тільки множиною ДП ПЗ. Можливі варіанти зміни інтенсивностей відмов і відновлень ПЗ і величин їх зміни зручно представити у вигляді дерева варіантів (Рисунок 4.4) і поставити йому у відповідність класифікаційну таблицю (Таблиця 4.2). Дерево складено шляхом логічних міркувань і відображає класифікацію можливих варіантів зміни параметрів і відповідні їм типи базових макромоделей оцінки надійності ПТК. У таблиці 4.2 наведені класифікаційні ознаки і поставлені їм у відповідність числові

послідовності. Дані послідовності формалізують відображення множини варіантів розглянутих параметрів в множину базових макромоделей.

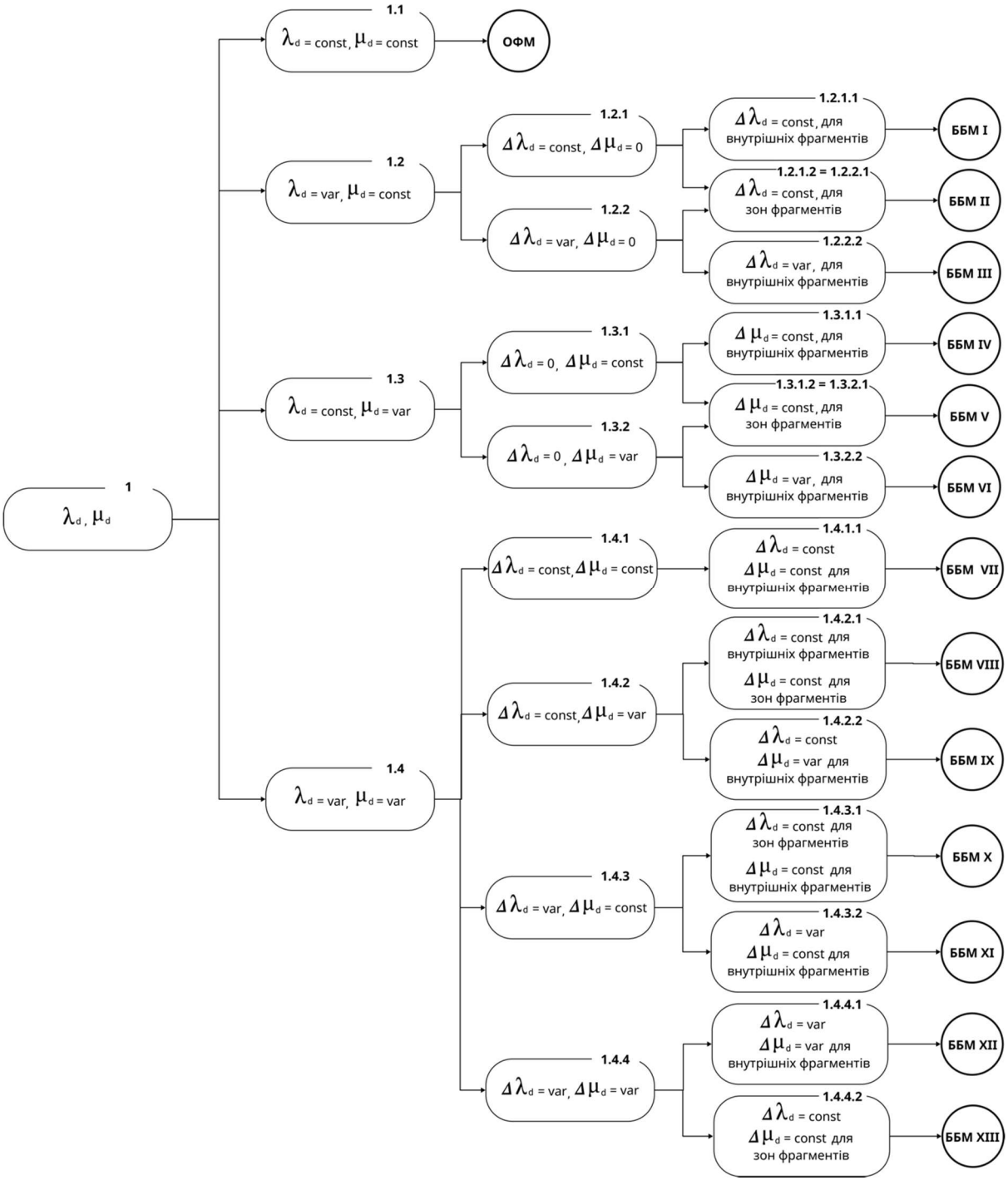


Рис. 4.4 Сценарії зміни надійністних параметрів ПК ПТК

Перша цифра числової послідовності (Таблиця 4.2) визначає множину параметрів, що змінюються $M=\{\lambda_{дп}, \mu_{вп}\}$. Друга числова послідовність визначає сценарій зміни параметрів. Третя числова послідовність визначає сценарій зміни коефіцієнтів $\Delta\lambda_{дп}$ та $\Delta\mu_{вп}$. Четверта (повна) числова послідовність визначає сценарій, який може бути реалізований базовою багатофрагментною макромоделлю (ББМ).

Таблиця 4.2

Класифікаційні ознаки й відповідні числові послідовності

<table>
<tr><td></td><td colspan="4">Ознака класифікації</td></tr>
<tr><td rowspan="20">Числова послідовність</td><td>Множина змінних параметрів</td><td>Сценарій зміни параметрів λ_d та μ_d</td><td>Сценарій зміни коефіцієнтів $\Delta\lambda_d$ та $\Delta\mu_d$</td><td>Сценарій, який реалізовано БММ</td></tr>
<tr><td rowspan="19">1</td><td>1.1</td><td></td><td></td></tr>
<tr><td rowspan="4">1.2</td><td rowspan="2">1.2.1</td><td>1.2.1.1</td></tr>
<tr><td>1.2.1.2</td></tr>
<tr><td rowspan="2">1.2.2</td><td>1.2.2.1</td></tr>
<tr><td>1.2.2.2</td></tr>
<tr><td rowspan="4">1.3</td><td rowspan="2">1.3.1</td><td>1.3.1.1</td></tr>
<tr><td>1.3.1.2</td></tr>
<tr><td rowspan="2">1.3.2</td><td>1.3.2.1</td></tr>
<tr><td>1.3.2.2</td></tr>
<tr><td rowspan="8">1.4</td><td>1.4.1</td><td>1.4.1.1</td></tr>
<tr><td>1.4.2</td><td>1.4.2.1</td></tr>
<tr><td rowspan="2">1.4.3</td><td>1.4.3.1</td></tr>
<tr><td>1.4.3.2</td></tr>
<tr><td rowspan="2">1.4.4</td><td>1.4.4.1</td></tr>
<tr><td>1.4.4.2</td></tr>
</table>

Таким чином маємо множину сценаріїв і відповідно множину ББМ, які покладено в основу розробки багатофрагментих марківських моделей оцінки надійності та функціональної безпеки ПТК.

ББМ №1 (1.2.1.1) – $\Delta\lambda_d$ – величина є не змінною в кожному фрагменті, $\Delta\lambda_{d\,i}$ = const, i ∈1…N, де N – число фрагментів.

ББМ №2 (1.2.1.2 и 1.2.2.1) – $\Delta\lambda_d$ – величина є не змінною в зоні фрагментів, $\Delta\lambda_{d\,i} \in \{\Delta\lambda_{d\,0}, \ldots, \Delta\lambda_{d\,Nz}\}$, где Nz – кількість зон фрагментів.

ББМ №3 (1.2.2.2) – $\Delta\lambda_d$ – величина, яка змінна в кождному фрагменті, $\Delta\lambda_d \in \{\Delta\lambda_{d\,i}, \ldots, \Delta\lambda_{d\,N}\}$.

ББМ №4 (1.3.1.1) – $\Delta\mu_d$ – коефіцієнт є не змінним в кожному фрагменті $\Delta\mu_{d\,i}$= const, i ∈ 1…N.

ББМ №5 (1.3.1.2 и 1.3.2.1) $\Delta\mu_d$ – коефіцієнт є не змінним в зоні фрагментів, $\Delta\mu_{d\,i} \in \{\Delta\mu_{d\,0}, \ldots, \Delta\mu_{d\,Nz}\}$.

ББМ №6 (1.3.2.2) – $\Delta\mu_d$ – коефіцієнт, який є змінним в кождному фрагменті, $\Delta\mu_d \in \{\Delta\mu_{d\,i}, \ldots, \Delta\mu_{d\,N}\}$.

ББМ №7 (1.4.1.1) – модель враховує зміну двох параметрів λ_d та μ_d. Коефіцієнти $\Delta\lambda_d$ и $\Delta\mu_d$ є не змінним в кожному фрагменті, де $\Delta\lambda_{d\,i}$ = const, $\Delta\mu_{d\,i}$ = const, i ∈ 1…N.

ББМ №8 (1.4.2.1) – модель враховує зміну двох параметрів λ_d та μ_d. Коефіцієнт $\Delta\lambda_d$ є незмінним в кожному фрагменті, $\Delta\lambda_{d\,i}$ = const. Коефіцієнт $\Delta\mu_d$ є незмінним в зоні фрагментів, $\Delta\mu_{d\,i} \in \{\Delta\mu_{d\,0}, \ldots, \Delta\mu_{d\,Nz}\}$.

ББМ №9 (1.4.2.2) – модель враховує зміну двох параметрів λ_d та μ_d. Коефіцієнт $\Delta\lambda_d$ є незмінним в кожному фрагменті, $\Delta\lambda_{d\,i}$ = const. Коефіцієнт $\Delta\mu_d$ є змінним в кожному фрагменті, $\Delta\mu_{вп} \in \{\Delta\mu_{вп\,i}, \ldots, \Delta\mu_{вп\,N}\}$.

ББМ №10 (1.4.3.1) – модель враховує зміну двох параметрів λ_d та μ_d. Коефіцієнт $\Delta\mu_d$ є незмінним в кожному фрагменті, $\Delta\mu_{d\,i}$ = const. Коефіцієнт $\Delta\lambda_d$ є незмінним в зоні фрагментів, $\Delta\lambda_{d\,i} \in \{\Delta\lambda_{d\,0}, \ldots, \Delta\lambda_{d\,Nz}\}$.

ББМ №11 (1.4.3.2) – модель враховує зміну двох параметрів λ_d та μ_d. Коефіцієнт $\Delta\mu_d$ є незмінним в кожному фрагменті, $\Delta\mu_{d\,i}$ = const. Коефіцієнт $\Delta\lambda_d$ є змінним в кожному фрагменті, $\Delta\lambda_d \in \{\Delta\lambda_{d\,i}, \ldots, \Delta\lambda_{d\,N}\}$.

ББМ №12 (1.4.4.1) – модель враховує зміну двох параметрів λ_d та μ_d.

Коефіцієнти $\Delta\mu_d$ и $\Delta\lambda_d$ є змінними в кожному фрагменті.

ББМ №13 (1.4.4.2) – модель враховує зміну двох параметрів λ_d та μ_d. Коефіцієнти $\Delta\mu_d$ и $\Delta\lambda_d$ є змінними в зоні фрагментів.

Базові макромоделі, атрибути яких представлені в розділі, дозволяють виконати моделювання різних варіантів зміни інтенсивностей відмов і відновлень ПЗ ПТК. При цьому слід зазначити, що практичну цінність мають ті моделі, які дозволяють апріорно передбачити надійність системи. Як показали дослідження, це ББМ 1, ББМ 4, БММ 7, в яких моделюється лінійна зміна параметрів λ_d, μ_d, $\Delta\lambda_d$ і $\Delta\mu_d$. Решта ББМ, безумовно, становлять інтерес в наукових дослідженнях, проте на даний момент не існує методів апріорного визначення динаміки зміни параметрів, які визначають ББМ. При цьому окрему увагу заслуговує ББМ 12 (λ_d = var, μ_d = var, $\Delta\lambda_d$ = var, $\Delta\mu_d$ = var), яка дозволяє апостериорно провести оцінювання готовності ПТК за результатами тестування і експлуатації систем. У порівнянні зі статистичними методами апостеріорної оцінки надійності, результати застосування ББМ 12 дозволять підтвердити достовірність і адекватність багатофрагментного моделювання.

Виходячи з перерахованих міркувань, далі будуть розглянуті ББМ 1, 7 і 12 (ББМ 4 по структурі аналогічна ББМ 1 і відрізняється змінюваним параметром μ_d).

Моделювання процесу функціонування ПТК в рамках параметрів ББМ №1, 2, 4, 5, 7 досить легко реалізується за допомогою математичного апарату марківських випадкових процесів з безперервним часом і дискретними станами. Внаслідок обліку зміни параметрів λ_d та μ_d на величину коефіцієнтів $\Delta\lambda_d$ та $\Delta\mu_d$ розмірність завдання значно зростає, тому ефективність моделювання знажується, що призводить до необхідності застосування спеціальних чисельних методів [239].

4.1.3 Систематизація багатофрагментних моделей

Визначені множини дефектів та параметри, які їх кількісно описують, базові архітектури побудови ПТК ІКС дозволили перейти до систематизації та класифікації багатофрагментних марковських моделей (БММ), які є одними із основних інструментів розроблених методів. Визначено, що основними ознаками багатофрагментних моделей є:

1. обрана архітектура ПТК (MooN), яку може бути доповнено апаратною або програмною диверсністю [151];
2. вихідні параметри (λ, μ);
3. комбінації змінних параметрів;
4. варіанти зміни вихідних параметрів (параметри в моделі можуть бути або змінними або незмінними – var, const);
5. варіанти зміни коефіцієнтів Δλ, Δμ (var, const);
6. можливий сценарій зміни параметрів Δλ, Δμ для внутрішніх фрагментів багатофрагментної моделі.

Прикладами топологічних структур БММ є:

- лінійні (у випадку врахування зміни одного параметру, наприклад λ_d або μ_d) (Рисунок. 4.5);
- двомірні лінійні (Рисунок 4.6 а) або деревоподібні (Рисунок 4.6 б) (у випадку врахування зміни двох параметрів, наприклад λ_d, μ_d).

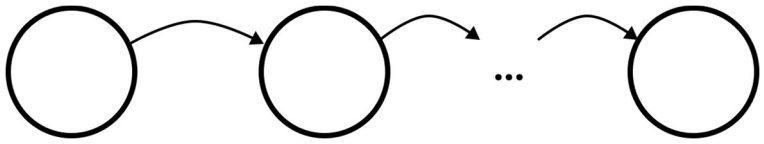


Рис. 4.5 Лінійна структура БММ

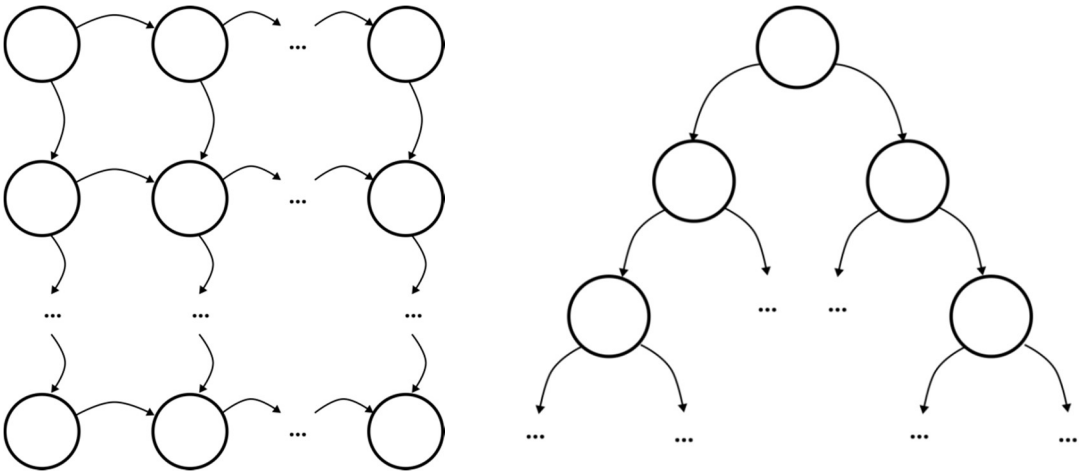


Рис. 4.6 а) лінійна двомірна структура БММ, б) деревоподібна структура БММ

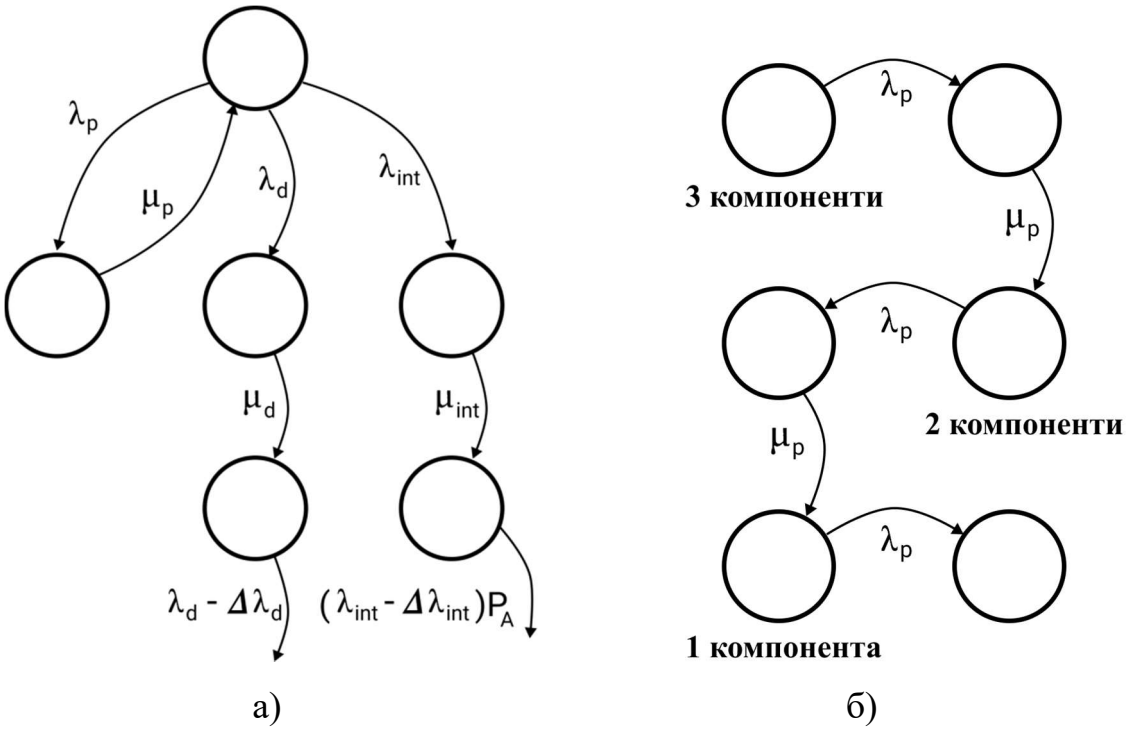


Рис. 4.7 а) деревоподбна структура з урахуванням розширеної множини параметрів, б) лінійна структура з урахуванням N $ЗКВ_н$ запасу компонентів для відновлення

Класифікацю БММ наведено на Рисунку 4.8.

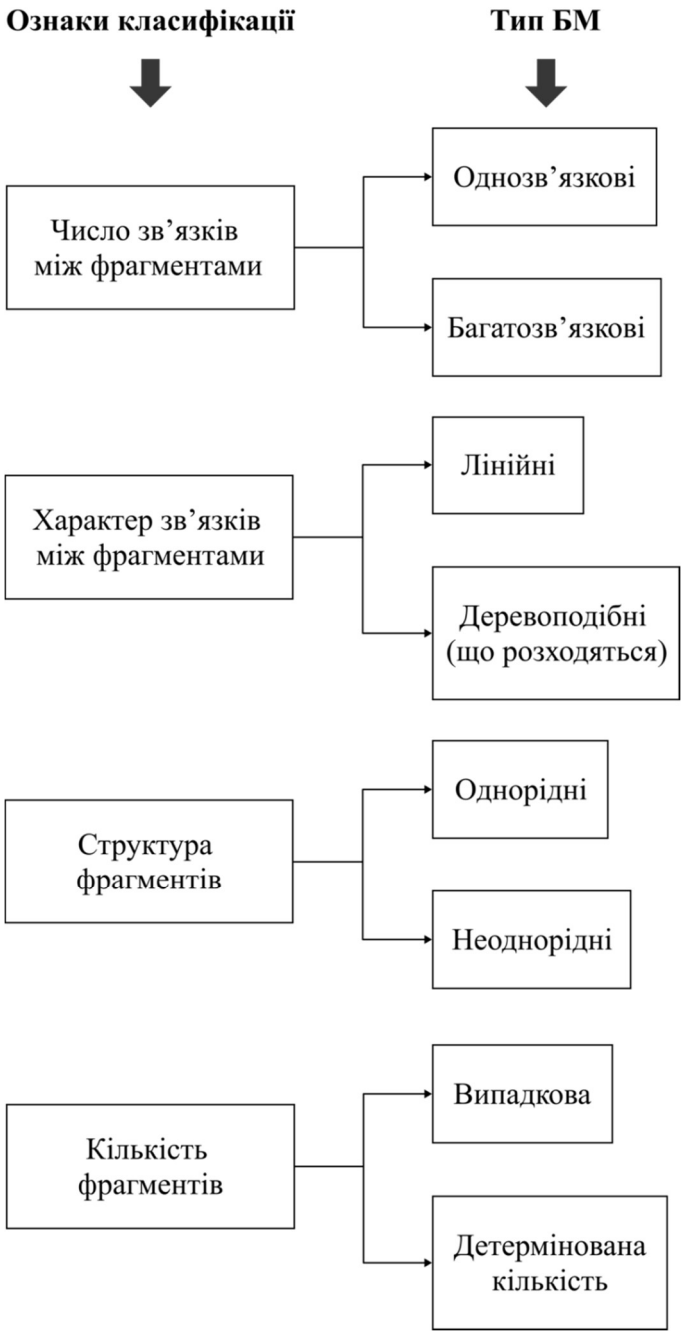


Рис. 4.8 Класифікація багатофрагментних марковських моделей

4.2. Базові відмовостійкі структури зі структурно-версійною надмірністю

Програмно-технічний комплекс (ПТК) за визначенням є сукупністю технічних засобів, що поставляються комплектно з програмним забезпеченням, необхідним сервісним обладнанням та експлуатаційною документацією, що утворює центральну частину інформаційно-керуючої системи. Ядром сучасних ПТК є програмовані логічні контролери (ПЛК). ПЛК за призначенням і галузями застосування можливо поділити на ПЛК загального призначення та безпечні (БПЛК). БПЛК є складною програмно-апаратною системою, яка використовується для забезпечення задач безпеки та критичного керування в системах автоматизації критичних виробництв (зокрема вироблення електричної енергії на АЕС). БПЛК, як правило, є невід'ємною частиною safety instrumented systems (SIS) та використовуються для виявлення потенційно небезпечних ситуацій технологічного процесу. У випадку виникнення даної ситуації, SIS запрограмована на автоматичне вживання заходів, що мають на меті перевести процес до безпечного стану. Існує важливе питання щодо різниці між БПЛК і ПЛК загального призначення, які успішно використовуються роками? А саме, чому не слід використовувати звичайний ПЛК у важливих технологічних виробництвах для контролю та безпеки ?

Уільям М. Гобл визначає [311], що БПЛК є системами, які спеціально розроблюються для досягнення двох важливих цілей:

- забезпечення надійного функціонування за рахунок застосування надмірності, на випадок, якщо запобігти відмові неможливо;

- відмова має впливати на технологічний процес передбачуваним (безпечним) способом.

Для досягнення означених цілей БПЛК розробляються із

використанням великої кількості спеціальних підходів (проектних рішень) . Прикладом таких проектних рішень є:

- самодіагностування на рівні апаратної одиниці модуля (юніта) та апаратного модуля в цілому;
- самодіагностування компонент, які не входять до апаратних одиниць модулів (юнітів);
- контроль цілісності даних при передачі між компонентами системи, захищені операції читання та запис та інш.;
- самодіагностування компонент програмних бібліотек та програмного забезпечення в цілому та інш. (це дозволяє забезпечити надійність програмної компоненти ПЛК).

За твердженням автора [76] БПЛК є детермінованими системами, які мають забезпечувати реакцію на подію на протязі визначеного інтервалу часу за будь-яких обставин (час реакції - Response time). Це теж є однією з ключових ознак БПЛК. Тобто БПЛК є системами жорсткого реального часу, в яких:

- запізнення реакції системи на прийом сигналу, його обробку і видачу керуючої дії є неприпустимим;
- порушення часу реакції є критичною відмовою з неприпустимою ціною.

Для забезпечення надійності функціонування ІКС застосовуються спеціальні методи структурного резервування апаратних засобів і версійного резервування програмних засобів. Спосіб резервування вибирають таким, щоб забезпечити для кожної функції прийнятний баланс між ймовірністю відмов типу «неспрацьовування» і «помилкове спрацьовування».

З метою мінімізації впливу всіх або частини помилок, які можуть виникати на стадіях розробки і впровадження ІКС, а також проявлятися як загальна причина одночасної відмови декількох резервних частин,

застосовується принцип різноманітності. Дотримання цього принципу забезпечується, наприклад, застосуванням в складі однієї системи двох ПТК, кожен з яких здатен виконувати функції безпеки незалежно і в повному обсязі, але досягаючи встановленої мети різними способами і (або) фізично відрізняючись один від одного.

Проаналізуємо базові архітектури побудови ПТК та приклади таких систем виробництва ПАТ НВП «Радій» (м. Кропивницький).

Наведемо набір типових схем резервування, які є базовими для побудови відмовостійких структур (архітектур) зі структурно-версійною надмірністю. Де під структурою (архітектурою*)* ПТК (Architecture) будемо розуміти ряд спеціальних проектних рішень, які специфікують конфігурацію елементів апаратної компоненти ПТК і його програмного забезпечення, що дозволяють наділити систему якостями підвищуючими її надійність і функційну безпеку [75].

Типові схеми резервування, які застосовуються для побудови архітектури ПТК наведено на рисунку 4.9.

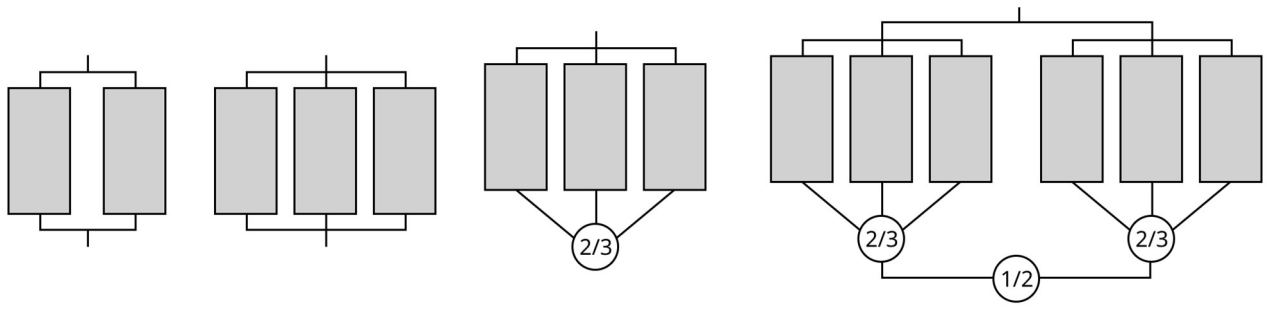


Рис. 4.9 Типові схеми резервування:

а) – дублювання; б) – потроєння; в) – мажоритарне резервування «2 з 3»; г) – два компоненти з резервуванням «1 з 2», де кожний комплект має резервування «2 з 3»

Застосуємо наступну систему означень для архітектури ПТК $S^{x3}{}_{x1x2}$

де S (ознака архітектури системи), x1 – кількість апаратних каналів ПТК, x2 – кількість версій ПЗ ПТК, x3 – ознака наявності програмно-апаратних засобів реконфігурування ПТК (наприклад, переключення в одноканальний режим для дубльованих комплексів, або двоканальний для мажоритарно-резервованих).

Далі наведено базові архітектури побудови ПТК, а саме:

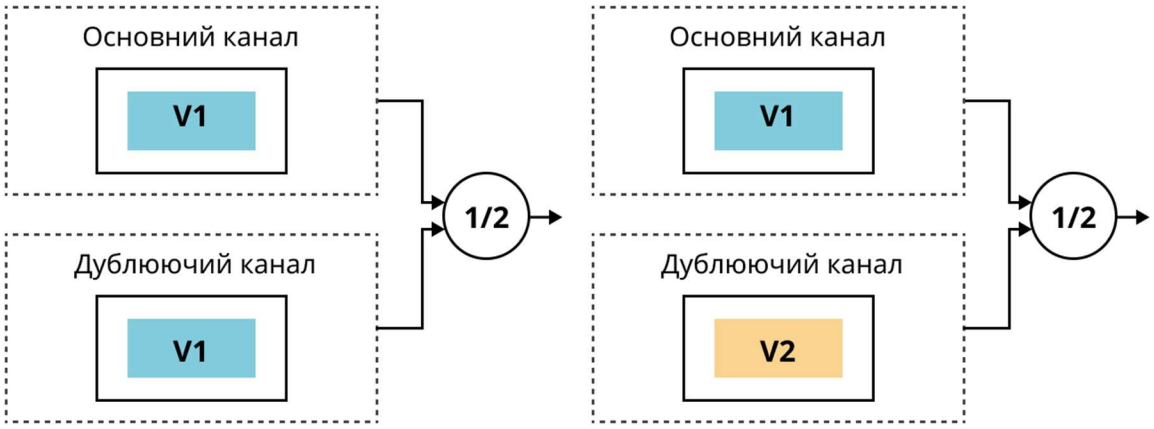
- дубльована одноверсійна ПТК S_{21} (1oo2D) (Рисунок 4.10, а);

- дубльована двоверсійна ПТК S_{22} (1oo2D) з версійною програмною надмірністю (Рисунок 4.10, б);

- одноверсійна мажоритарна ПТК S_{31}(1oo3D) (Рисунок 4.11, а);

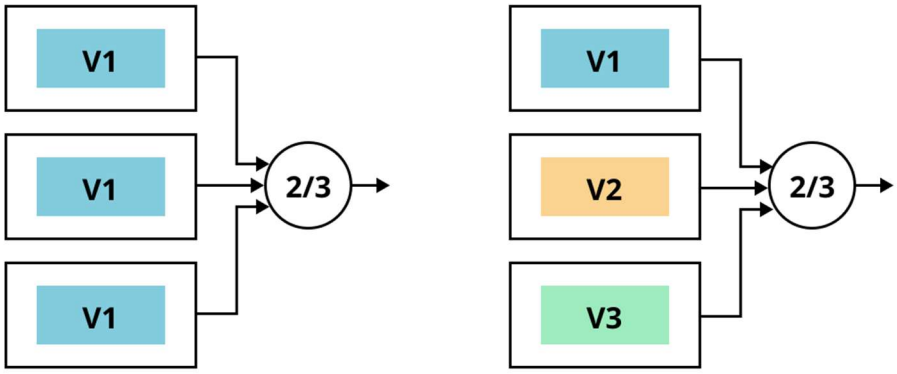
- багатоверсійна мажоритарна ПТК S_{33} (1oo3D) з версійною програмною надмірністю (Рисунок 4.11, б).

-



а) б)

Рис. 4.10 а) Архітектура дубльованого одноверсійного ПТК S_{21} (1oo2D), б) Архітектура дубльованого двоверсійного ПТК S_{22} (1oo2D) з версійною програмною надмірністю.



а) б)

Рис. 4.11 а) Архітектура одноверсійного мажоритарного ПТК S_{31}(1oo3D), б) Архітектура багатоверсійного мажоритарного ПТК S_{33} (1oo3D) з версійною програмною надмірністю.

Звісно, що наведена множина базових архітектур не є вичерпною та спираючись на неї можливо здійснити архітектурну побудову ПТК, які розробляються та поставляються в якості поставочних комплектів на АЕС. Проаналізуємо приклади архітектурної побудови ПТК виробництва ТОВ НВП «Радій» та ТОВ НВП «Радікс» (м. Кропивницький). Прикладом такого ПТК є комплекс аварійного та попереджувального захисту (ПТК АЗ ПЗ). ПТК АЗ-ПЗ призначений для застосування в якості технічної бази при створенні нових і реконструкції діючих систем аварійного та попереджувального захисту реактора типу ВВЕР на енергоблоках АЕС України.

До складу комплекту входять:

- три ідентичних шафи формування сигналів, які утворюють три незалежні канали захисту та взаємно резервують один одного;

- кросова вихідна шафа, яка формує вихідні сигнали комплекту на основі даних отриманих від шаф формування сигналів;

- робоча станція, яка здійснює архівування, відображення і реєстрацію даних;

- автоматизоване робоче місце оператора, призначене для

відображення контрольованих параметрів, станів дискретних входів і виходів, а також причин, що викликали спрацьовування захистів.

Загальним для двох комплектів є автоматизоване робоче місце технолога, на якому можуть здійснюватися перевірка працездатності ПТК АЗ-ПЗ, а також зміна і запис уставок спрацьовування захисту. Таким чином, ПТК розроблений на основі «жорсткої логіки» з реалізацією трьох рівнів формування вихідних сигналів на основі мажоритарної логіки «два з трьох». На рисунку 4.12 представлена двоканальна архітектура ПТК АЗ-ПЗ з реалізацією логіки «M-oo-N» в кожному каналі [312].

Необхідно відзначити, що даний комплекс використовує дві функціонально ідентичні версії ПЗ (V1, V2). Дана архітектура побудови ПТК є однією з базових [269] поширених для побудови ІКС АЕС. На даний момент ПТК АЗ-ПЗ успішно експлуатується на блоках №1 та №3 Запорізької АЕС (3 комплекти), блоці №3 і №4 Рівненської АЕС (3 комплекти), блоці №1 та №3 Южно-Української АЕС (2 комплекти) . На рисунку 4.13 наведено приклад архітектури ПТК з двохксакадною схемою резервування перший каскад 1/2, другий каскад 2/3.

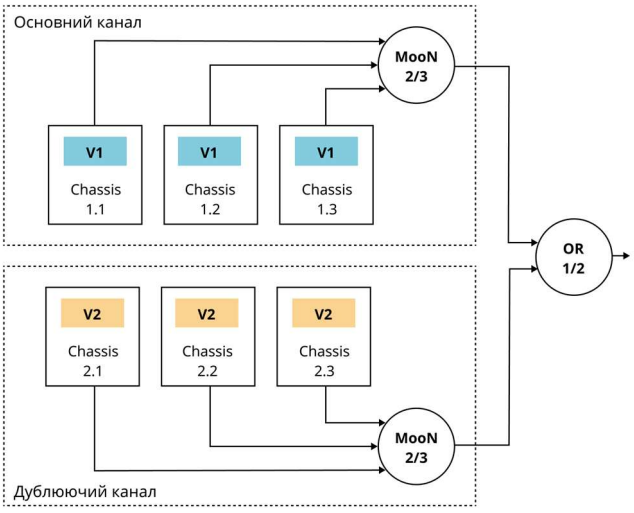


Рис. 4.12 Архітектура двоканального ПТК АЗ ПЗ з двокаскадною схемою голосування (перший каскад 2/3, другий каскад 1/2)

Наступним прикладом архітектурної побудови ПТК є система аварійного захисту управляючої системи безпеки АЗ-УСБ (RTS-ESFAS - Reactor Trip System - Emergency Safety Features Actuation System) енергоблоків АЕС з реакторами PWR (Pressurized Water Reactor), які широко експлуатуються на АЕС США. Дана архітектура є трьокаскадною, де перший каскад містить чотири ідентичні канали прийому інформації від польової мережі датчиків та апаратури контролю нейтронного потоку (АКНП); другий каскад (Рисунок 4.14) представлено двома каналами, що обробляють інформацію від каналів першого касакаду за логікою «2oo4» та третій релейний каскад обробляє інформацію від каналів другого каскаду за логікою «2oo3».

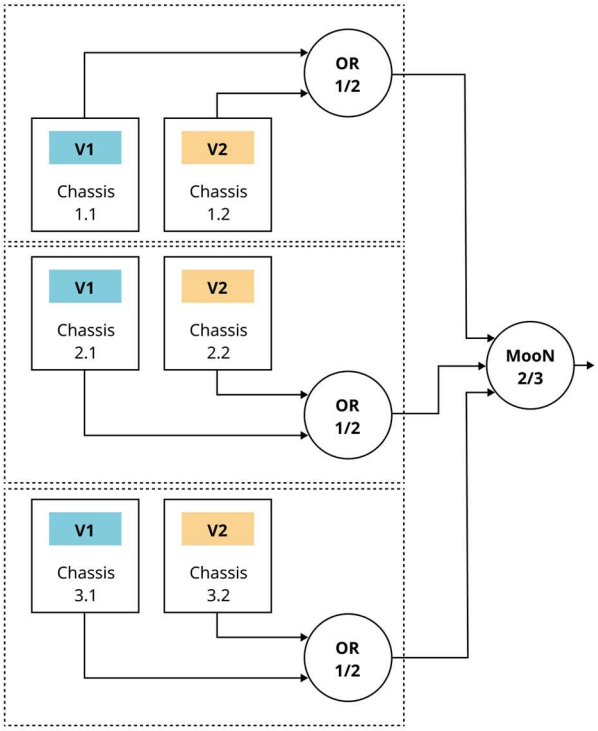


Рис. 4.13 Архітектура двоканального ПТК АЗ ПЗ з двокаскадною схемою голосування (перший каскад 1/2, другий каскад 2/3)

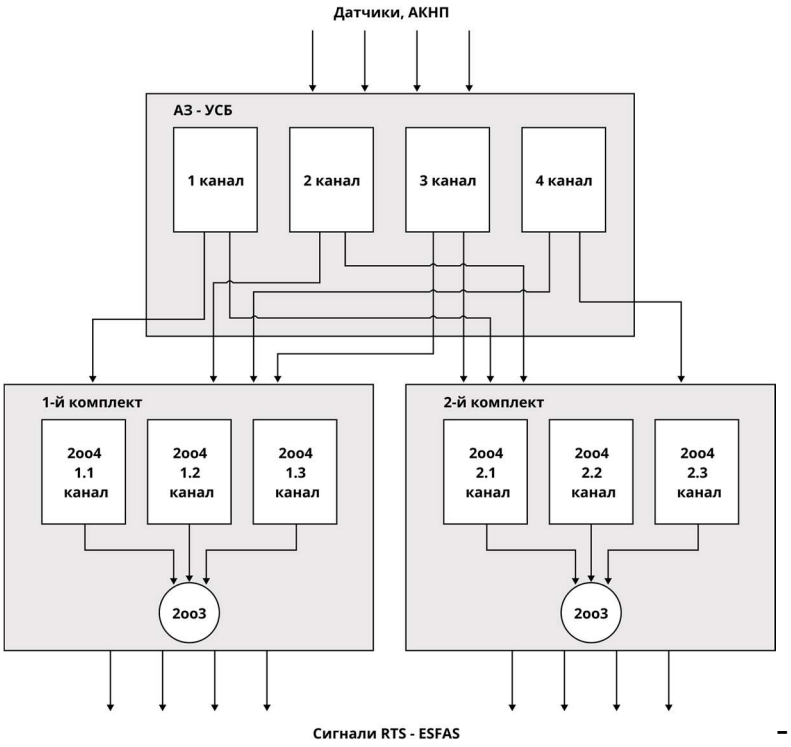


Рис. 4.14 Архітектура ПТК АЗ УСБ із двокаскадною системою голосування (перший каскад 2oo4, другий каскад 2oo3)

4.3 Розроблення і дослідження моделей готовності ПТК побудованих за дубльованою та мажоритарною архітектурами

4.3.1 Багатофрагмента марковська модель готовності дубльованих одноверсійних ПТК

Спираючись на зміст попередніх підрозділів та методику розробки багатофрагментних марковських моделей (БММ) [240] виконано розробку БММ готовності дубльованого одноверсійного ПТК S_{21}. Структура такої системи наведена на рис.4.10а., та структурну схему надійності (ССН) наведено на рисунку 4.15.

Рис. 4.15 ССН дубльованого одноверсійного ПТК $S_{21.}$

Вигляд ССН визначається множиною надійнісних параметрів, які враховуються, послідовністю можливих відмов та відновлень каналів за апаратною компонентою та проявами дефектів проектування програмних засобів враховуючи, що кожний канал керується абсолютно ідентичнм ПЗ та наявністю або відсутністю засобів реконфігурування з двохканального в одноканальний режими роботи. Відповідно до цього на Рисунку 4.15 наведено ССН ПТК, в якого засоби реконфігурування відсутні та відмова апаратної компоненти одного з двох каналів або прояв ДПП переводить ПТК з архітектурою S_{21} у непрацездатний стан.

Множина параметрів, які враховують прояв фізичних і проектних дефектів:

$$M\pi = \{ \lambda_p, \mu_p, \lambda_d, \Delta\lambda_{d,} \mu_d \}, \quad (4.3)$$

де: λ_p – інтенсивність прояву фізичного дефекту (дефекту АК); μ_p - інтенсивність відновлення АК після прояву фізичного дефекту; λ_d - інтенсивність прояву дефекту проектування ПЗ; $\Delta\lambda_d$ – коефіцієнт зміни інтенсивності прояву дефекту ПЗ; μ_d – інтенсивність відновлення ПЗ.

Далі обираємо сценарій зміни параметрів і відповідно ББМ №1 (1.2.1.1) відповідно до якої $\Delta\lambda_d$ є сталою величиною у кожному фрагменті, $\Delta\lambda_{di}$ = const, i $\in$1…N, де N – кількість фрагментів. Граф, який описує функціонування S_{21} без врахування зміни параметрів є однофрагментним (рисунок 4.16), адже всі інтенсивності, які визначають процеси переходів між станами, є сталими величинами.

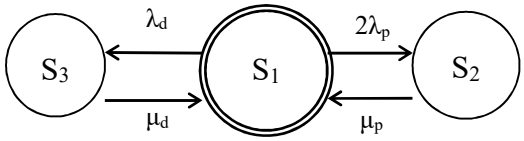


Рис. 4.16 Однофрагментний граф функціонування S_{21}

Даний граф складається з трьох станів, а саме:

- S_1 – початковий стан системи (канали працездатні);
- S_2 – система не працездатна (проявився фізичний дефект одного з каналів);
- S_3 – система не працездатна (проявився дефект проектування ПЗ).

Відповідно до обраного сценарію (1.2.1.1) отримаєм макрограф ББМ №1 зображений на рисунку 4.17.

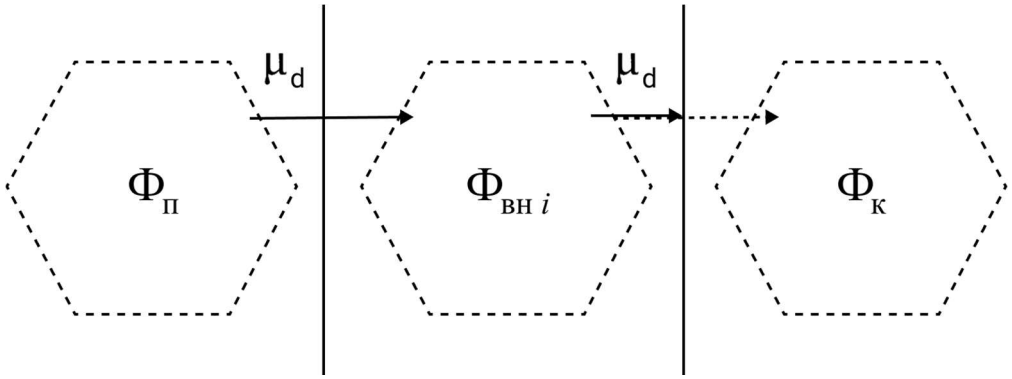


Рис. 4.17 Макрограф ББМ №1 S_{21}

Макрограф зображений на рисунку 4.17 складається з початкового ($Ф_п$), і-х внутрішніх ($Ф_{внi}$) та кінцевого ($Ф_к$) фрагментів. На рисунку 4.18 наведено багатофрагментну марківську модель готовності дубльованого одноверсійного ПТК S_{21}.

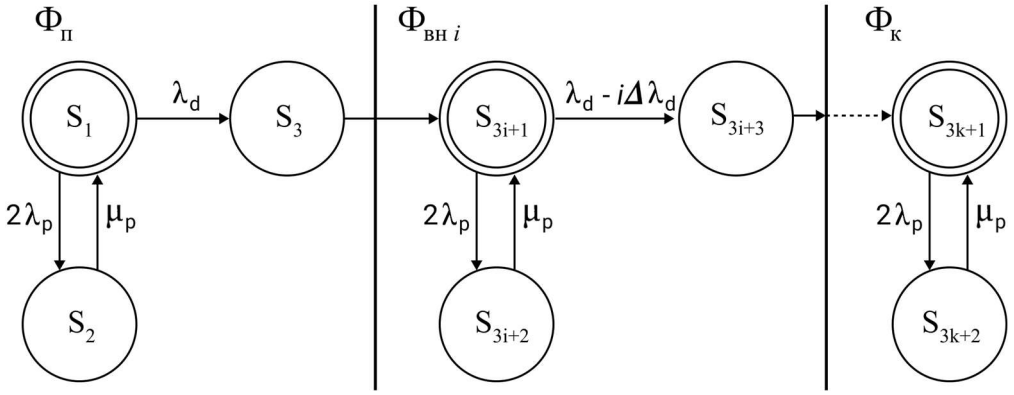


Рис. 4.18 БММ№1 S_{21}

БММ включає в себе наступну множину станів:

- $MS_p=\{S_1,S_4,..S_{3i+1},\ldots,S_{3n+1}\}$ – множина працездатних станів;

- $MS_{нп}=\{S_2,S_5,\ldots,S_{3i+2},\ldots,S_{3n+2}\}$ – множина непрацездатних станів (відмова одного із апаратних каналів);

- $SF_3=\{S_3,S_6,\ldots,S_{3i+3},\ldots,S_{3n+3}\}$ - множина непрацездатних станів (відмова програмної компоненти).

Логіка функціонування системи наступна. Реалізується схема простого поканального порівняння. Відмова АК одного з двох каналів приводить до відмови всієї системи. У початковий момент часу система реалізує всі функції й знаходиться в стані S_1. У випадковий момент часу виявляються ДП ПЗ або возникають ДФ АК. При прояві ДФ АК система переходить у стан S_2 з інтенсивністю 2 λ_p. Далі з інтенсивністю μ_p система відновлюється. При прояві ДП ПЗ система переходить у стан S_3 з інтенсивністю λ_d і з інтенсивністю μ_d відновлюється і система переходе у другий фрагмент (стан S_4). У відповідності до прийнятих припущень, після кожної події, пов'язаної з проявом ДП ПЗ, величина інтенсивності λ_d зменшується на постійну величину $\Delta\lambda_d$. Параметри μ_d, залишається постійним, а параметр $\Delta\lambda_d$ обчислюється за виразом:

$$\Delta\lambda_d = \lambda_{d(o)} - \lambda_{d(1),} \qquad (4.4)$$

де $\lambda_{d(o)}$ – початкове значенні інтенсивності прояву ДП ПЗ, $\lambda_{d(1)}$ - інтенсивності прояву ДП ПЗ після усунення одного програмного дефекту.

Число дефектів визначається за наступним виразом:

$$N_ф = N_{дп\ пз} + 1. \tag{4.5}$$

Система веде себе аналогічно у всіх внутрішніх фрагментах. У кінцевому фрагменті усі ДП ПЗ усунено й порушення функціонування системи може бути викликано лише ДФ АК.

Аналізуючи граф нескладно одержати СДР Колмогорова-Чепмена:

$Ф_п$- описують рівняння:

$$dP_1 / dt = -(2\lambda_p + \lambda_d)P_1(t) + \mu_p P_2(t),$$
$$dP_2 / dt = -\mu_p P_2(t) + 2\lambda_p P_1(t),$$
$$dP_3 / dt = -\mu_d P_3(t) + \lambda_d P_1(t);$$

$Ф_{внi}$ – описують рівняння:

$$dP_{3i+1} / dt = -\left(\lambda_d - i\Delta\lambda_d + 2\lambda_p\right)P_{3i+1}(t) + \mu_d P_{3i}(t) + \mu_p P_{3i+2}(t),$$
$$dP_{3i+2} / dt = -\mu_p P_{3i+2}(t) + 2\lambda_p P_{3i+1}(t),$$
$$dP_{3i+3} / dt = -\mu_d P_{3i+3}(t) + \left(\lambda_d - i\Delta\lambda_d\right)P_{3i+1}(t); \tag{4.6}$$

$Ф_к$ – описують рівняння:

$$dP_{3k+1} / dt = -2\lambda_p P_{3k+1}(t) + \mu_d P_{3k}(t) + \mu_p P_{3k+2}(t),$$
$$dP_{3k+2} / dt = -\mu_p P_{3k+2}(t) + 2\lambda_p P_{3k+1}(t);$$

Початковими умовами розв'язку СДР є:

$$t = 0,\ P_1(0) = 1,\ P_i(0) = 0,\ i = 2,...,3k+2.$$

Функція готовності визначається як сума ймовірностей знаходження системи в працездатних станах $MS_p = \{S_1, S_4, \ldots, S_{3n+1}\}$.

$$A_{\Gamma}(t) = \sum_{i=0}^{k} P_{3i+1}(t) \tag{4.7}$$

Функція оперативної готовності визначається як:

$$A_{O\Gamma}(t,\tau) = \sum_{i=0}^{k} \left[P_{3i+1}(t) P_{БР\,3i+1}(\tau) \right], \tag{4.8}$$

де $P_{БР\ 3i+1}(\tau)$ – ймовірність безвідмовної роботи системи за час τ, якого достатньо для фиконання функції безпеки.

Розробимо БММ ПТК S^{p}_{21}, який має засоби реконфігурування для порівняння впливу цього фактору на складність отриманої моделі. ССН зображено на рисунку 4.19.

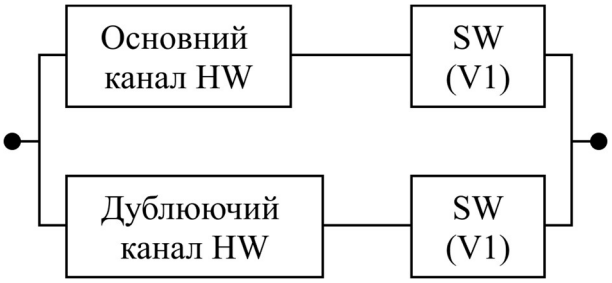


Рис. 4.19 Структурна схема надійності дубльованого одноверсійного ПТК S^{p}_{21}. із засобами реконфігурування каналів.

З урахуванням того, що використовується сценарій (1.2.1.1) базовий є ідентичним до зображеного на рисунку 4.17, марковська модель для початкового фрагменту (ОФМ) наведена на рисунку 4.20.

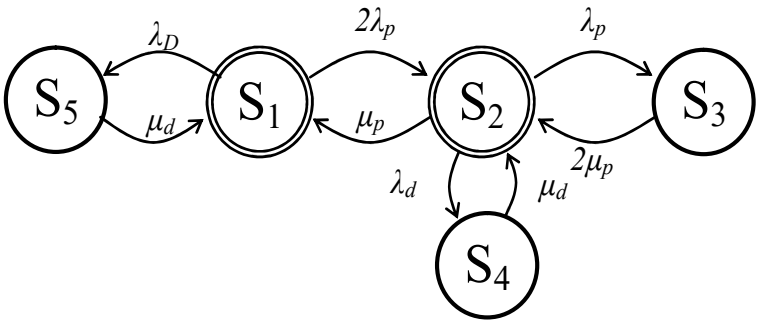


Рис. 4.20 Однофрагментний граф функціонування S^p_{21} із засобами реконфігурування каналів

Логіка функціонування ПТК наступна. В початковий момент часу система працездатна і знаходиться у стані S_1. У випадкові моменти часу система може перейти до станів S_2 (прояв фізичного дефекту одного з каналів та реконфігурування в одноканальний режим – стан працездатний) або S_5 прояв ДППЗ (стан непрацездатний). Відповідно зі стану S_2 система може перейти у стан S_3 (прояв фізичного дефекту другого каналу – стан непрацездатний) або S_4 прояв ДППЗ (стан непрацездатний).

Багатофрагментна марковська модель (рисунок 4.21) включає наступі стани:

S_1 – стан, в якому система працездатна (початковий стан), у внутрішніх фрагментах даному стану відповідають стани S_{5i+1};

S_2 – стан прихованої відмови ПЗ, у внутрішніх фрагментах цьому стану відповідають стани S_{5i+5};

S_3 – стан виявленої відмови за АК (працездатний стан), у внутрішніх фрагментах цьому стану відповідають стани S_{5i+2};

S_4 – стан состояние виявленої відмови за АК (непрацездатний стан), у внутрішніх фрагментах цьому стану відповідають стани S_{5i+3};

S_5 – стан відмови одного каналу за ПК, другого за АК (стан непрацездатний), у внутрішніх фрагментах цьому стану відповідають стани S_{5i+4};

S_{5k+1} – стан, який належить останньому фрагменту, в якому система працездатна;

S_{5k+2} – стан відмови одного каналу за АК (стан належить останньому фрагменту);

S_{5k+3} – стан відмови двох каналів за АК (стан належить останньому фрагменту).

СДР в узагальненому вигляді:

$\Phi_{п}$- описують рівняння:

$$dP_1 / dt = -\left(2\lambda_p + \lambda_d\right)P_1(t) + \mu_p P_2(t),$$
$$dP_2 / dt = -\left(\lambda_d + \lambda_p + \mu_p\right)P_2(t) + 2\lambda_p P_1(t) + 2\mu_p P_3(t),$$
$$dP_3 / dt = -2\mu_p P_3(t) + \lambda_p P_2(t),$$
$$dP_4 / dt = -\mu_d P_4(t) + \lambda_d P_2(t),$$
$$dP_5 / dt = -\mu_d P_5(t) + \lambda_d P_1(t);$$

$\Phi_{вні}$ – описують рівняння:

$$dP_{5i+1} / dt = -\left(2\lambda_p + \lambda_d - i\Delta\lambda_d\right)P_{5i+1}(t) + \mu_p P_{5i+2}(t) + \mu_d P_{5i}(t),$$
$$dP_{5i+2} / dt = -\left(\lambda_d - i\Delta\lambda_d + \lambda_p + \mu_p\right)P_{5i+2}(t) +$$
$$+2\lambda_p P_{5i+1}(t) + 2\mu_p P_{5i+3}(t) + \mu_d P_{5i-1}(t),$$
$$dP_{5i+3} / dt = -2\mu_p P_{5i+3}(t) + \lambda_p P_{5i+2}(t),$$
$$dP_{5i+4} / dt = -\mu_d P_{5i+4}(t) + \left(\lambda_d - i\Delta\lambda_d\right)P_{5i+2}(t),$$
$$dP_{5i+5} / dt = -\mu_d P_{5i+5}(t) + \left(\lambda_d - i\Delta\lambda_d\right)P_{5i+1}(t);$$

(4.9)

$\Phi_{к}$ – описують рівняння

$$dP_{5k+1} / dt = -2\lambda_p P_{5k+1}(t) + \mu_d P_{5k}(t) + \mu_p P_{5k+2}(t),$$
$$dP_{5k+2} / dt = -\left(\mu_p + \lambda_p\right)P_{5k+2}(t) + 2\lambda_p P_{5k+1}(t) + 2\mu_p P_{5k+3}(t) + \mu_d P_{5k-1}(t),$$
$$dP_{5k+3} / dt = -2\mu_p P_{5k+3}(t) + \lambda_p P_{5k+2}(t).$$

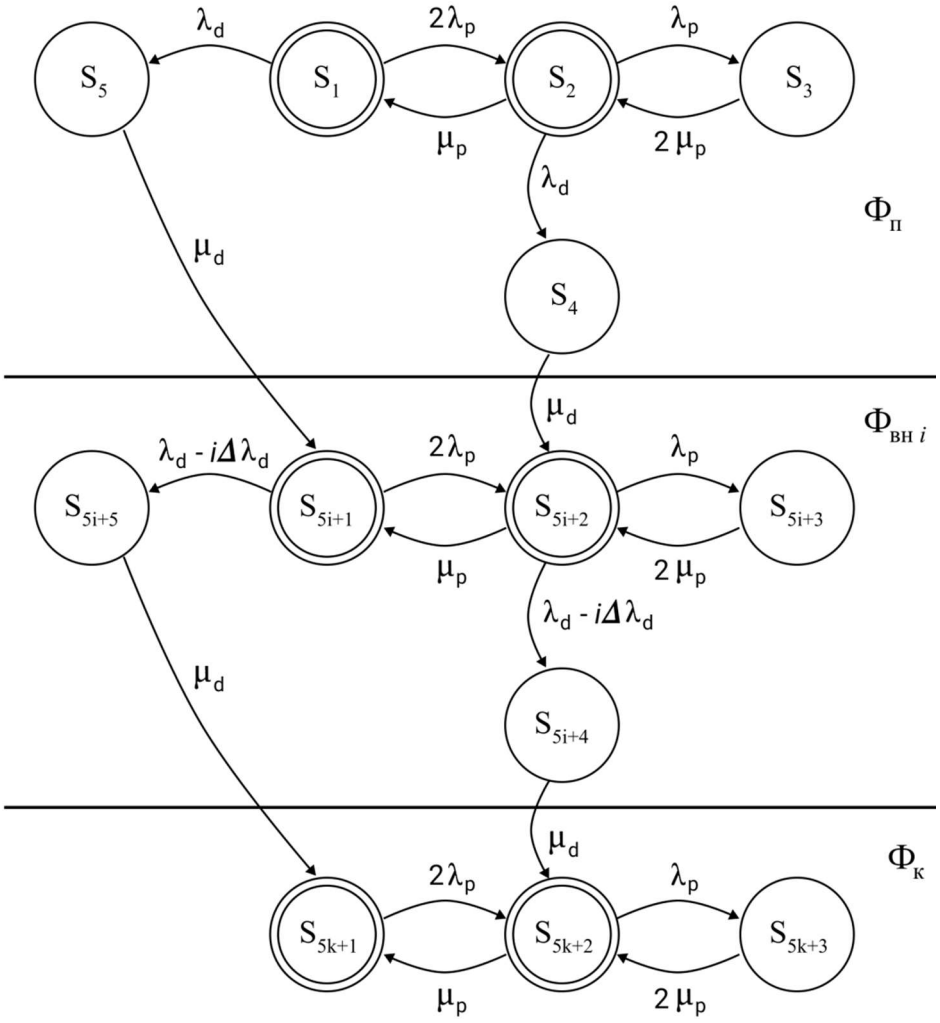


Рис. 4.21 БММ S^p_{21} із засобами реконфігурування каналів

Вирази для обчислення функції готовності та оперативної готовності відповідно:

$$A_{\Gamma}(t)=\sum_{i=0}^{k}\left[P_{5i+1}(t)+P_{5i+2}(t)\right] \tag{4.10}$$

$$A_{O\Gamma}(t,\tau)=\sum_{i=0}^{k}\left[P_{5i+1}(t)P_{БР\,5i+1}(\tau)+P_{5i+2}(t)P_{БР\,5i+2}(\tau)\right] \tag{4.11}$$

4.3.2 Багатофрагмента марковська модель готовності дубльованих двухверсійних ПТК

Розробимо БММ готовності дубльованого двохверсійного ПТК S^p_{22} . Структура даної системи наведена на рисунок 4.10б, структурна схема надійності наведена на рисунку 4.22.

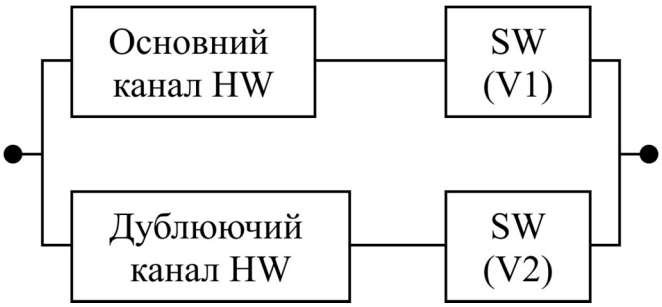


Рис. 4.22 Структурна схема надійності дубльованого двохверсійного ПТК S^p_{22}

Однофрагментний граф для ПТК обраної архітектури наведено на рисунку 4.23.

Логіка функціонування наступна. В початковий момент часу система працездатна і знаходиться у стані S_1. У випадкові моменти часу система може перейти до станів S_2 (прояв фізичного дефекту одного з каналів та реконфігурування в одноканальний режим – стан працездатний) або S_5 (прояв ДП ПЗ та реконфігурування в одноканальний режим – стан працездатний). Відповідно зі стану S_2 система може перейти у стан S_3 (прояв фізичного дефекту другого каналу – стан непрацездатний) або S_4 прояв ДП ПЗ (стан непрацездатний). Зі стану S_5 – система може перейти до непрацездатного стану S_6 у випадку прояву ДП ПЗ другого каналу, та можливі переходи між станами S_4 та S_5 у випадках проявів або відновлень ДП ПЗ відповідних каналів.

Сценарій зміни параметрів і відповідно ББМ №1 залишаємо (1.2.1.1) – $\Delta\lambda_d$ – величина є не змінною в кожному фрагменті, $\Delta\lambda_{d\,i}$ = const, i $\in$1…N, де N – число фрагментів.

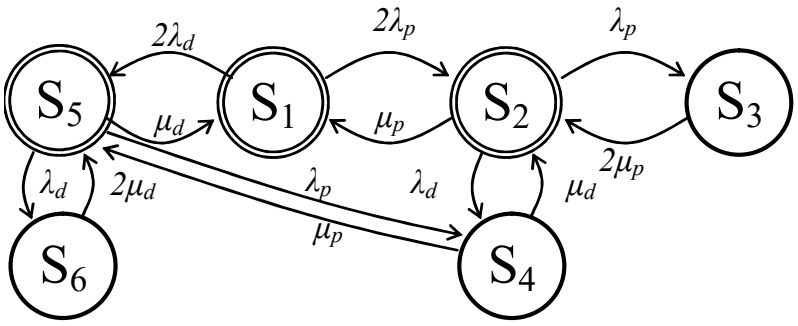


Рис. 4.23 Однофрагментний граф ПТК S^p_{22} із засобами реконфігурування каналів

При розробці багатофрагментного графа встановлено, що внутрішні фрагменти моделі мають значні відмінності. Ці відмінності визначаються різною кількістю станів, розширеною системою зв'язків між фрагментами. Ця обставина вимагає докладного розгляду з метою розробки методики дослідження БММ більш складної структури.

В результаті досліджень виявлено, що множина фрагментів, що визначає набір фрагментів моделі, є наступною:

$$M_Ф = \{Ф_п, Ф_I, Ф_{II}, Ф_{III}, Ф_{IV}, Ф_V, Ф_{по}, Ф_к\},$$

де $Ф_{вн}$ - початковий фрагмент, $Ф_I$ - внутрішні фрагменти I – го ÷ IV типів, , $Ф_{по}$ - передостанній фрагмент, Фк - кінцевий фрагмент.

Відповідні типи фрагментів множини $M_Ф$ наведено на рисунках 4.24 - 4.31. Після кожного фрагменту графу наведено частину загальної СДР.

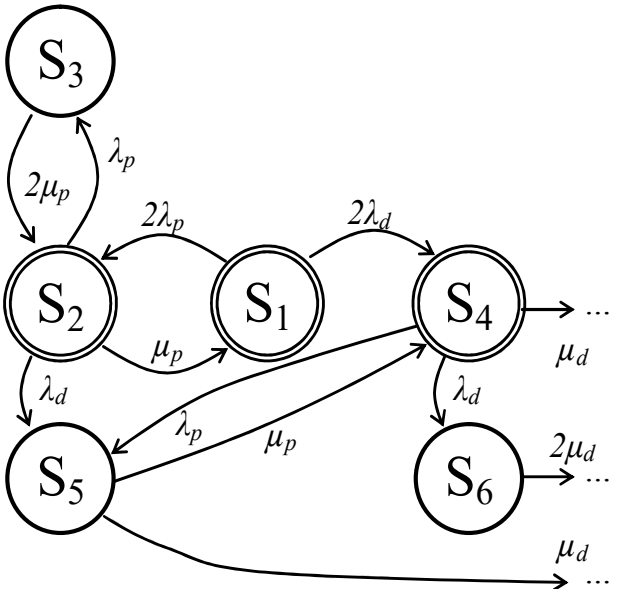


Рис. 4.24 Початковий фрагмент $Ф_п$

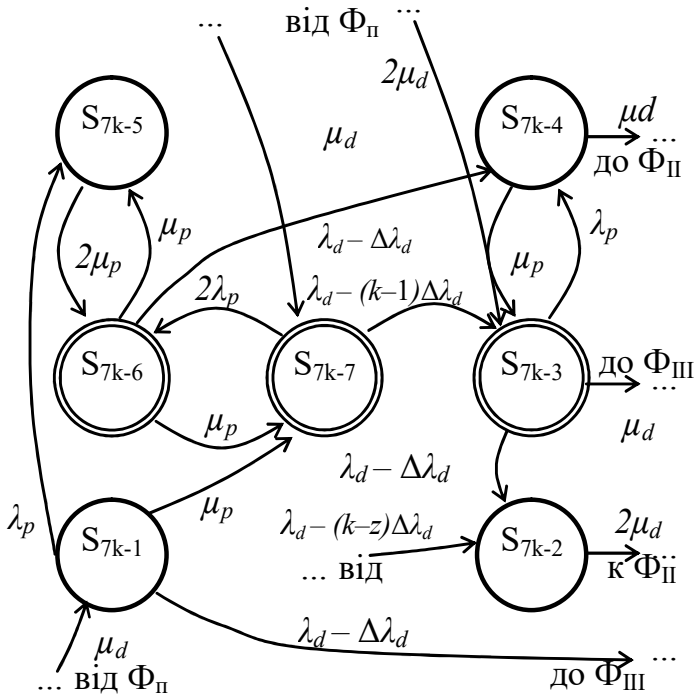


Рис. 4.25 Внутрішній фрагмент I-го типу $Ф_I$

СДР, що описує початковий фрагмент моделі, наступна:

$$
\begin{aligned}
&dP_1/dt = -(2\lambda_p+\Lambda_d)P_1+\mu_pP_2,\\
&dP_2/dt = -(\lambda_p+\lambda_d)P_2+2\lambda_pP_1+2\mu_pP_3,\\
&dP_3/dt = -2\mu_pP_3+\lambda_pP_2,\\
&dP_4/dt = -(\mu_d+\lambda_p+\lambda_d)P_4+\Lambda_dP_1+\mu_pP_5,\\
&dP_5/dt = -(\mu_p+\mu_d)P_5+\lambda_pP_4+\lambda_dP_2,\\
&dP_6/dt = -2\mu_dP_6+\lambda_dP_4
\end{aligned}
\qquad (4.12)
$$

СДР, що описує фрагмент І-го типу БММ готовності дубльованого двохверсійного ПТК S^p_{22}, наступна, де Z є номером першого фргаменту І – виду:

$$
\begin{aligned}
&dP7_{k-7}/dt = -(2\,\lambda_p + [\lambda_d -(k-1)\Delta\,\lambda_d])\,P_{7k-7}+\mu_d\,P_{7k-10}+\mu_pP_{7k-6}+\\
&\mu_pP_{7k-1},\\
&dP7_{k-6}/dt = -(\mu_p+\lambda_p+[\,\lambda_d-[k-2]\,\Delta\,\lambda_d])P_{7k-6}+2\,\lambda_p\,P_{7k-7}+2\mu_pP_{7k},\\
&dP7_{k-5}/dt = -2\mu_pP_{7k-5}+\lambda_p\,P_{7k-6}+\lambda_p\,P_{7k-1},\\
&dP7_{k-4}/dt = -(\mu_p+\mu_d)P_{7k-4}+(\,\lambda_d-[k-2]\Delta\,\lambda_d)P_{7k-6}+\lambda_p\,P_{7k-3},\\
&dP7_{k-3}/dt = -(\,\mu_d+\lambda_p+[\,\lambda_d-\Delta\,\lambda_d])P_{7k-3}+2\,\mu_d\,P_{7k-9}+[\,\lambda_d-(k-1)\Delta\lambda_d]\\
&P_{7k-7}+\mu_pP_{7k-4},\\
&dP7_{k-2}/dt = -2\,\mu_d\,P_{7k-2}+[\,\lambda_d-\Delta\,\lambda_d]P_{7k-3}+(\,\lambda_d-[k-Z]\Delta\,\lambda_d)P_{7k+34},\\
&dP7_{k-1}/dt = -(\mu_p+\lambda_p+[\,\lambda_d-\Delta\,\lambda_d])P_{7k-1}+\mu_d\,P_{7-11}.
\end{aligned}
\qquad (4.13)
$$

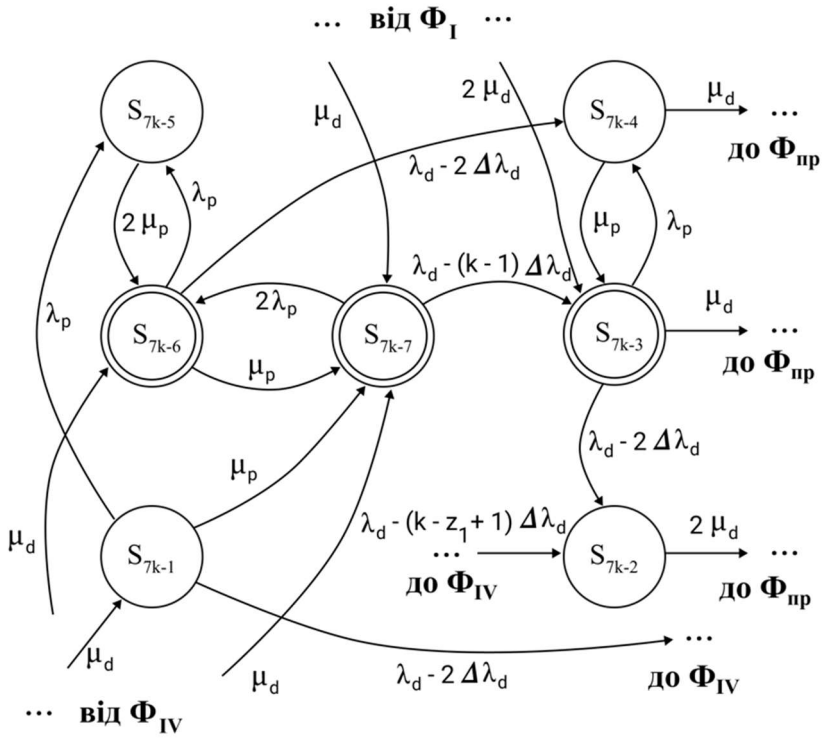


Рис. 4.26 Внутрішній фрагмент II-го типу Φ_{II}

СДР, що описує фрагмент II – го типу моделі, є наступною:

$$
\begin{aligned}
&dP_{7k-7}/dt = -(2\lambda_p + [\lambda_d - (k-1)\Delta\lambda_d])P_{7k-7} + \mu_d P_{7k-10} + \mu_p P_{7k-6} + \mu_p P_{7k-1},\\
&dP_{7k-6}/dt = -(\mu_p + \lambda_p + (\lambda_d - [k-3]\Delta\lambda_d))P_{7k-6} + 2\lambda_p P_{7k-7} + 2\mu_p P_{7k} + \mu_d P_{8k+17},\\
&dP_{7k-5}/dt = -2\mu_p P_{7k-5} + \lambda_p P_{7k-6} + \lambda_p P_{7k-1},\\
&dP_{7k-4}/dt = -(\mu_p + \mu_d)P_{7k-4} + (\lambda_d - [k-3]\Delta\lambda_d)P_{7k-6} + \lambda_p P_{7k-3},\\
&dP_{7k-3}/dt = -(\mu_d + \lambda_p + (\lambda_d - 2\Delta\lambda_d))P_{7k-3} + 2\mu_d P_{7k-9} + [\lambda_d - (k-1)\Delta\lambda_d] *\\
&*P_{7k-7} + \mu_p P_{7k-4},\\
&dP_{7k-2}/dt = -2\mu_d P_{7k-2} + (\lambda_d - 2\Delta\lambda_d)P_{7k-3} + (\lambda_d - (k - [Z_1 - 1])\Delta\lambda_d)P_{7k+34},\\
&dP_{7k-1}/dt = -(\mu_p + \lambda_p + (\lambda_d - 2\Delta\lambda_d))P_{7k-1} + \mu_d P_{7k-11}.
\end{aligned}
\tag{4.14}
$$

Необхідно зазначити, що фрагменти II типу необхідно розбити на

пари, де Z_1 - номер першого фрагменту пари фрагментів II-го типу. Параметр, що описується різницею λ_d - $2\Delta\lambda_d$, відповідає першому фрагменту II-го типу, далі зменшується на $\Delta\lambda$дп в кожній парі фрагментів даного виду.

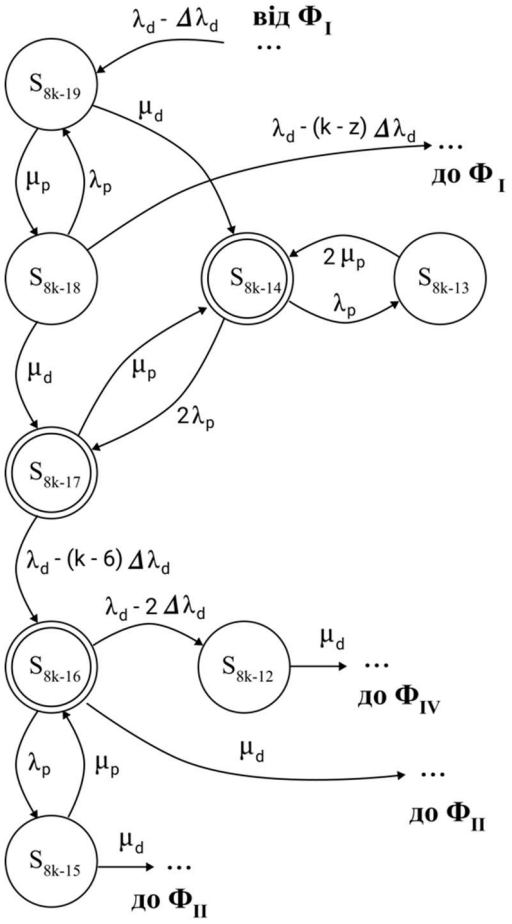


Рис. 4.27 Внутрішній фрагмент III-го типу Φ_{III}

СДР, що описує фрагмент III – го типу моделі, наступна:

$$dP_{8k-19}/dt = -(\mu_d + \mu_p)P_{8k-19} + [\lambda_d - \Delta\lambda_d]P_{7k-29} + \lambda_p P_{8k-18},$$

$$dP_{8k-18}/dt = -([\lambda_d - [k - Z]\Delta\lambda_d] + \mu_d + \lambda_p)P_{8k-18} + \mu_p P_{8k-19},$$

$$dP_{8k-17}/dt = -(2\lambda_p + (\lambda_d - [k - 6]\Delta\lambda_d))P_{8k-17} + \mu_d P_{8k-18} + \mu_p P_{8k-14},$$

$$dP_{8k-16}/dt = -([\lambda_d - 2\Delta\lambda_d] + \lambda_p + \mu_d)P_{8k-16} + (\lambda_d - [k - 6]\Delta\lambda_d)*$$

$$P_{8k-17} + \mu_p P_{8k-15}, \qquad (4.15)$$

$dP_{8k-15}/dt = -(\mu_d + \mu_p)P_{8k-15} + \lambda_p P_{8k-16}$,

$dP_{8k-14}/dt = -(\mu_p + \lambda_p)P_{8k-14} + 2\lambda_p P_{8k-17} - \mu_d P_{8k-19} + 2\mu_p P_{8k-13}$,

$dP_{8k-13}/dt = -2\mu_p P_{8k-13} + \lambda_p P_{8k-14}$,

$dP_{8k-12}/dt = -\mu_d P_{8k-12} + [\lambda_d - 2\Delta\lambda_d]P_{8k-16}$.

В ході застосування виразу (4.12) при визначені різниці $[\lambda_d - \Delta\lambda_d]$ необхідно використовувати Z як номер першого фргаменту I –виду. Відповідно, під час визначення різниці $[\lambda_d - [k - Z]\Delta\lambda_d]$ необхідно враховувати, що Z_1– є номером першого фрагменту пари фрагментів II-го типу.

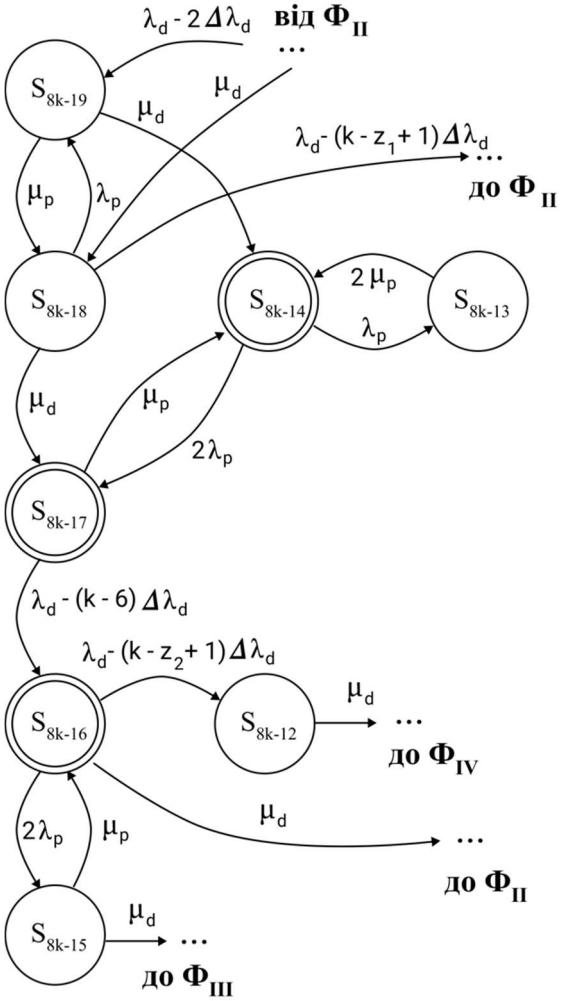


Рис. 4.28 Внутрішній фрагмент IV – го типу Φ_{IV}

СДР, що описує фрагмент IV – го типу моделі, наступна:

$$dP_{8k-19}/dt = -(\mu_d + \mu_p)P_{8k-19} + [\lambda_d - 2\Delta\lambda_d]P_{7k-43} + \lambda_p P_{8k-18},$$

$$dP_{8k-18}/dt = -(\lambda_d + \lambda_p + (\lambda_d - (k - [Z_2-1]\Delta\lambda_d))P_{8k-18} + \mu_d P_{8k-10} + \mu_p P_{8k-19},$$

$$dP_{8k-17}/dt = -(2\lambda_p + (\lambda_d - [k-6]\Delta\lambda_d))P_{8k-17} + \mu_d P_{8k-18} + \mu_p P_{8k-14}, \quad (4.16)$$

$$dP_{8k-16}/dt = -((\lambda_d - (k-[Z_2-4])\Delta\lambda_d) + \lambda_p + \mu_d)P_{8k-16} + (\lambda_d - [k-6]\Delta\lambda_d) * P_{8k-17} + \mu_p P_{8k-15},$$

$$dP_{8k-15}/dt = -(\mu_d + \mu_p)P_{8k-15} + \lambda_p P_{8k-16},$$

$$dP_{8k-14}/dt = -(\mu_p + \lambda_p)P_{8k-14} + 2\lambda_p P_{8k-17} + \mu_d P_{8k-19} + 2\mu_p P_{8k-13},$$

$$dP_{8k-13}/dt = -2\mu_p P_{8k-13} + \lambda_p P_{8k-14},$$

$$dP_{8k-12}/dt = -\mu_d P_{8k-12} + [\lambda_d - (k-[Z_2-4])\Delta\lambda_d]P_{8k-16}.$$

Необхідно розбити фрагменти IV – го типу на пари. Значення параметра λ_d перед змінною P_{7k-43} зменшується на $\Delta\lambda_d$ для кожної пари фрагментів. Значення параметра λ_d, що стоїть перед змінної P_{8k-18}, зменшується на величину $(k - Z_2 + 1)\Delta\lambda_d$, де Z_2 номер першого фрагмента IV типу, таким чином, значення символів k і Z_2 для першого фрагмента пари збігаються. Значення параметра λ_d, що стоїть перед змінної P_{8k-16}, зменшується на величину $(k - Z_2 + 4)\Delta\lambda_d$ для кожної пари фрагментів цього типу.

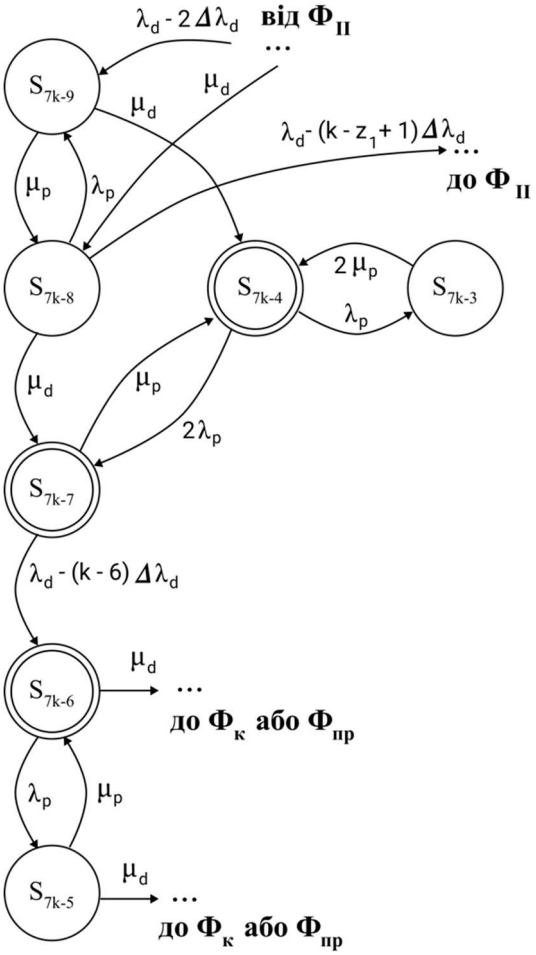


Рис. 4.29 Внутрішній фрагмент V-го типу Φ_V

СДР, що описує фрагмент V – го типу моделі, наступна:

$$dP_{7k-9}/dt = -(\mu_d + \mu_p)P_{7k-9} + \lambda_p P_{7k-8} + 2\Delta\lambda_p P_{7k-33},$$

$$dP_{7k-8}/dt = -([\lambda_d - (k - [z1 - 1]\Delta\lambda_d)) + \lambda_p + \mu_d)P_{7k-8} + \mu_p P_{7k-9} + \mu_d P_{8k-28}, \quad (4.17)$$

$$dP_{7k-7}/dt = -(2\lambda_p + (\lambda_d - [k - 6]\Delta\lambda_d))P_{7k-7} + \mu_d P_{7k-8} + \mu_p P_{7k-4},$$

$$dP_{7k-6}/dt = -(\lambda_p + \mu_d)P_{7k-6} + (\lambda_d - [k - 6]\Delta\lambda_d)P_{7k-7} + \mu_p P_{7k-5},$$

$$dP_{7k-5}/dt = -(\mu_d + \mu_p)P_{7k-5} + \lambda_p P_{7k-6},$$

$$dP_{7k-4}/dt = -(\mu_p + \lambda_p)P_{7k-4} + \mu_d P_{7k-9} + 2\lambda_p P_{7k-7} + 2\mu_p P_{7k-3},$$

$$dP_{7k-3}/dt = -2\mu_p P_{7k-3} + \lambda_p P_{7k-4}.$$

У виразі (4.14) при визначені різниці $\Lambda_d - (k - [z1 - 1]\Delta\lambda_d$ необхідно враховувати, що Z_1 – є номером першого фрагменту пари фрагментів II-го

типу.

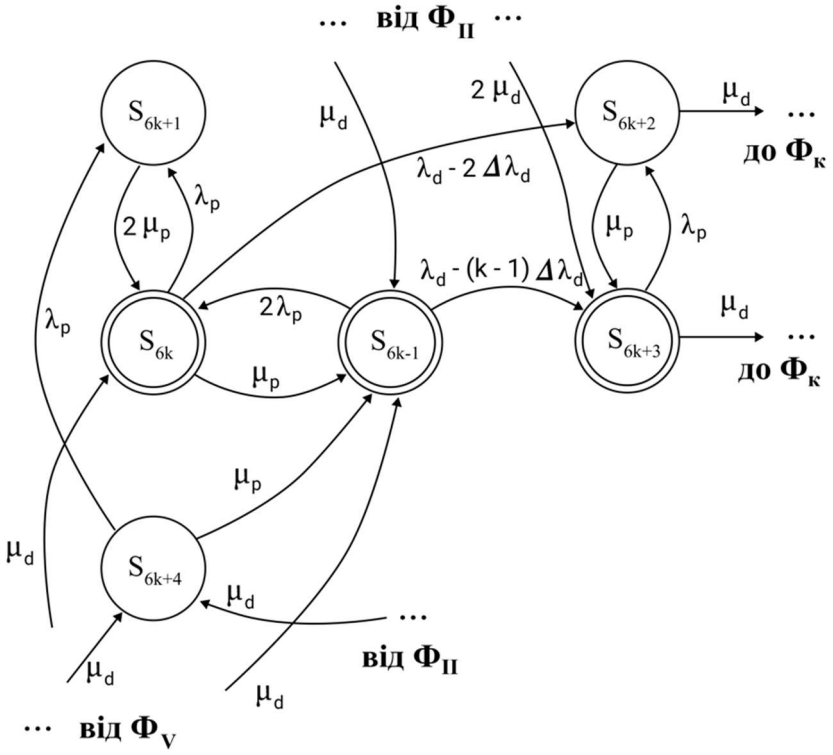


Рис. 4.30 Внутрішній фрагмент VI – го типу (передостанній) $Ф_{VI}$

СДР, що описує фрагмент передостанній фрагмент моделі, наступна:

$$dP_{6k-1}/dt = -(2\lambda_p + (\lambda_d - [k-1]\Delta\lambda_d))P_{6k-1} + \mu_d P_{7k-3} + \mu_p P_{6k} + \mu_p P_{6k+4} + \mu_d P_{6k+28},$$

$$dP_{6k/dt} = -(\mu_p + \lambda_p + 2\Delta\lambda_d)P_{6k} + 2\lambda_p P_{6k-1} + 2\mu_p P_{6k+1} + \mu_d P_{6k+28}, \quad (4.18)$$

$$dP_{6k+1}/dt = -2\mu_p P_{6k+1} + \lambda_p P_{6k},$$

$$dP_{6k+2}/dt = -(\mu_p + \mu_d)P_{6k+2} + 2\Delta\lambda_d P_{6k} + \lambda_p P_{6k+3},$$

$$dP_{6k+3}/dt = -(\lambda_p + \mu_d)P_{6k+3} + 2\mu_d P_{6k-3} + (\lambda_d - [k-1]\Delta\lambda_d)P_{6k-1} + \mu_p P_{6k+2},$$

$$dP_{6k+4}/dt = -(\mu_p + \lambda_p)P_{6k+4} + \mu_d P_{6k-5}.$$

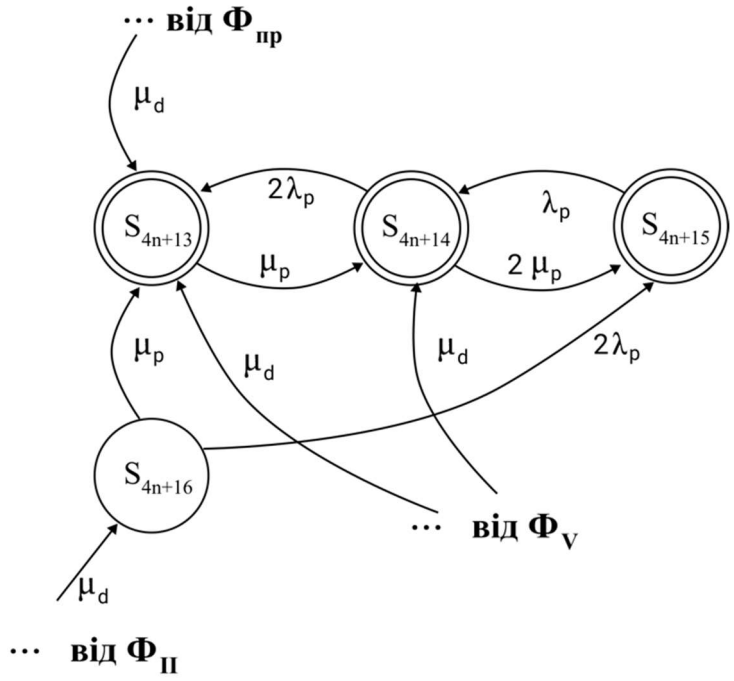


Рис. 4.31 Граф кінцевого фрагменту $Ф_к$

СДР, що описує кінцевий фрагмент моделі, наступна:

$$dP_{4n+13}/dt = -2\lambda_p P_{4n+13} + \mu_d P_{4n+11} + \mu_p P_{4n+14} + \mu_p P_{4n+16} + \mu_d P_{4n+43}, \quad (4.19)$$

$$dP_{4n+14}/dt = -(\lambda_p + \mu_p)P_{4n+14} + 2\lambda_p P_{4n+13} + 2\mu_p P_{4n+15} + \mu_d P_{4n+44},$$

$$dP_{4n+15}/dt = -2\mu_p P_{4n+15} + \lambda_p P_{4n+14} + \lambda_p P_{4n+16},$$

$$dP_{4n+16}/dt = -(\mu_p + \lambda_p)P_{4n+16} + \mu_d P_{4n+10}.$$

Необхідно зазначити, що послідовність нумерації визначається розробником. Наприклад, в даній роботі була прийнята наступна послідовність нумерації фрагментів: $Ф_п$ - 1; $Ф_i$ - 2,3; $Ф_{II}$ - 4,5; $Ф_{VI}$. - 6; $Ф_к$ - 7; $Ф_{III}$ - 8,9; $Ф_V$ - 10,11.

Отримана БММ готовності дубльованого двохверсійного ПТК S^p_{22} може бути класифікована, як багатозв'язкова, з неоднорідними фрагментами.

Функція готовності визначаєтсья як сума ймовірностей знаходження

системи в працездатних станах у всіх фрагментах. Сума складових функції готовності за фрагментами наступна:

$$A_{\Gamma}(t) = A_{\Gamma(\Pi)}(t) + A_{\Gamma(I)}(t) + A_{\Gamma(II)}(t) + A_{\Gamma(II)}(t) + A_{\Gamma(IV)}(t) + A_{\Gamma(\Pi)}(t) + A_{\Gamma(V)}(t) + A_{\Gamma(VI)}(t) + A_{\Gamma(K)}(t). \quad (4.20)$$

4.3.3 Багатофрагментна марковська модель готовності одноверсійної мажоритарної архітектури ПТК

Виконаємо розробку багатофрагментної марковської моделі готовності одноверсійного мажоритарного ПТК $S_{31.}$ Структурна схема ПТК наведена на рисунку 4.11а. Структурна схема надійності наведена на рисунку 4.32.

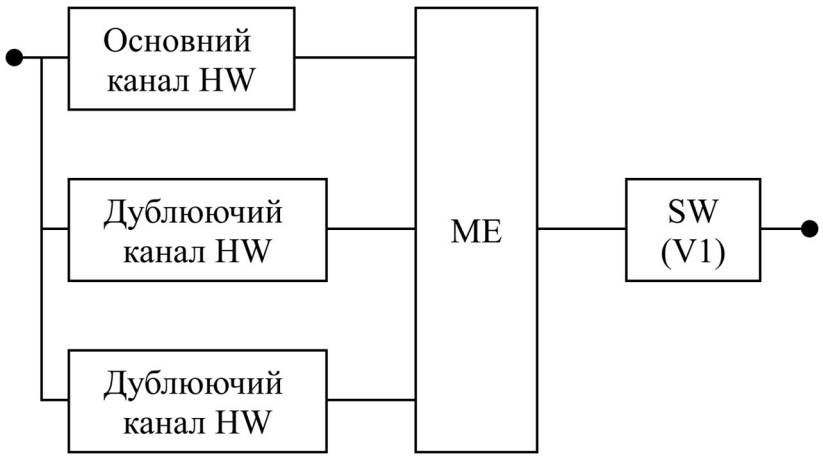


Рис. 4.32 Структурна схема надійності
одноверсійного мажоритарного ПТК S_{31}

Однофрагментний граф для ПТК обраної архітектури наведено на рисунку 4.33.

Логіка функціонування наступна. В початковий момент часу система працездатна і знаходиться у стані S_1. У випадкові моменти часу система

може перейти до станів S_2 (прояв фізичного дефекту одного з каналів та реконфігурування в двохканальний режим – стан працездатний) або S_5 (прояв ДП ПЗ – стан непрацездатний, можливий випадок, коли наступає подія прихованої відмови пролграмної компонети. В цьому випадку настає ситуація не безпечної відмови, коли всі три канали обчислюють не вірний результат). Відповідно зі стану S_2 система може перейти у стан S_3 (прояв фізичного дефекту другого каналу – стан непрацездатний) або S_4 прояв ДП ПЗ (стан непрацездатний).

Сценарій зміни параметрів і відповідно ББМ №1 залишаємо (1.2.1.1) – $\Delta\lambda_d$ – величина є не змінною в кожному фрагменті, $\Delta\lambda_{d\,i}$ = const, i $\in$1…N, де N – число фрагментів.

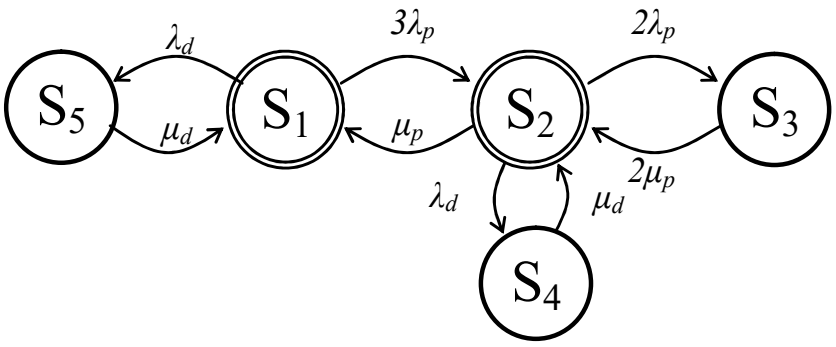


Рис. 4.33 Однофрагментний граф ПТК S_{31}

Відповідно до обраного сценарію (1.2.1.1) макрограф ББМ №1 для даної структури відповідає зображеному на рис. 4.17.

На рисунку 4.34 наведено багатофрагментну марківську модель готовності одноверсійного мажоритарного ПТК S_{31}.

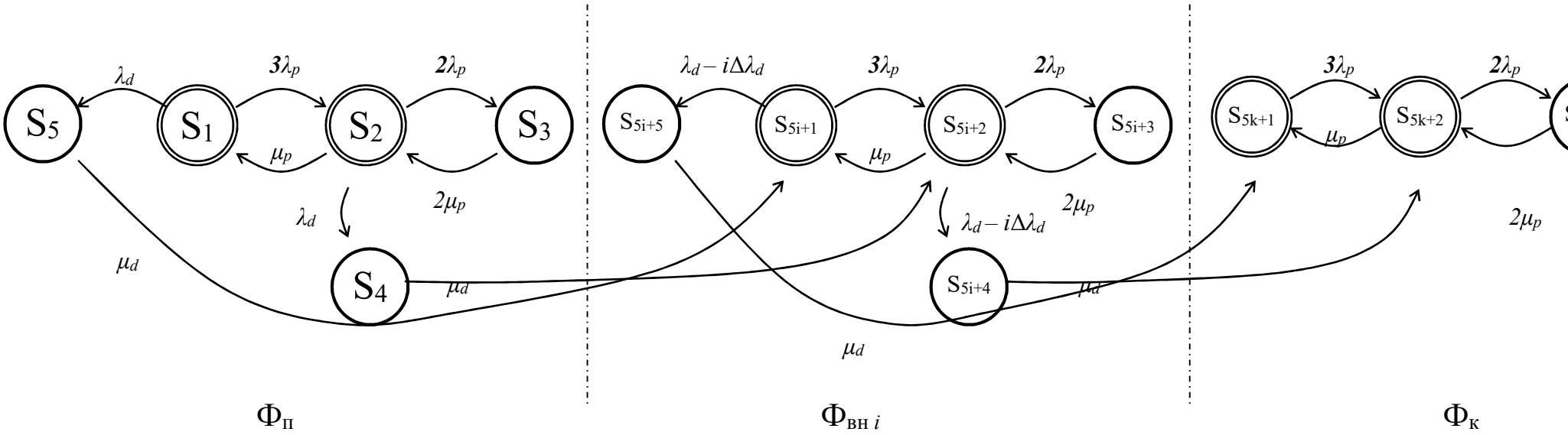


Рис. 4.34 БММ№1 S_{31}

БММ включає в себе наступну множину станів:

- $MS_р=\{S_1,S_2,..S_{5i+1},\ldots,S_{5i+2},S_{5k+1},S_{5k+2}\}$ – множина працездатних станів;

- $MS_{нп}=\{S_5,\ldots,S_{5i+5}, S_{3k+2}\}$ – множина непрацездатних станів (відмова одного із апаратних каналів);

- $MS_{нп}=\{S_3,\ldots,S_{5i+3}, S_{5k+3}\}$ – множина непрацездатних станів (відмова двох каналів за апаратною компонентою);

- $SF_{нп}=\{S_4,S_5,\ldots,S_{5i+4},\ldots,S_{5i+5}\}$ - множина непрацездатних станів (відмова програмної компоненти).

Логіка функціонування системи наступна. Реалізується схема мажоритарного поканального порівняння. Відмова двох каналів за АК приводить до відмови всієї системи. У початковий момент часу система реалізує всі функції й знаходиться в стані S_1. У випадковий момент часу виявляються ДП ПЗ або возникають ДФ АК. При прояві ДФ АК система переходить у стан S_2 з інтенсивністю $3\lambda_p$. Далі з інтенсивністю μ_p система відновлюється. При прояві ДП ПЗ система переходить у стан S_5 з інтенсивністю λ_d і з інтенсивністю μ_d відновлюється і система переходе у другий фрагмент (стан S_{5i+1}). У відповідності до прийнятих припущень, після кожної події, пов'язаної з проявом ДП ПЗ, величина інтенсивності λ_d зменшується на постійну величину $\Delta\lambda_d$. Параметри μ_d, залишається постійним, а параметр $\Delta\lambda_d$ обчислюється за виразом (4.1). Число дефектів визначається за виразом (4.2).

Система веде себе аналогічно у всіх внутрішніх фрагментах. У кінцевому фрагменті усі ДП ПЗ усунено й порушення функціонування системи може бути викликано лише ДФ АК.

Аналізуючи граф нескладно одержати СДР Колмогорова-Чепмена для $Ф_п$-початкового, $Ф_{внi}$ - множини внутрішніх та $Ф_к$ – кінцевих фрагментів:

$\Phi_{п}$- описують рівняння:

$$dP_1 / dt = -(3\lambda_p + \lambda_d)P_1(t) + \mu_p P_2(t),$$
$$dP_2 / dt = -(2\lambda_p + \lambda_d + \mu_p)P_2(t) + 2\mu_p P_3(t) + 3\lambda_p P_1(t),$$
$$dP_3 / dt = -2\mu_p P_3(t) + 2\lambda_p P_2(t);$$
$$P_4 / dt = -\mu_d P_4(t) + \lambda_d P_2(t);$$
$$P_5 / dt = -\mu_d P_5(t) + \lambda_d P_1(t);$$

$\Phi_{внi}$ – описують рівняння:

$$dP_{5i+1} / dt = -\left(3\lambda_d + [\lambda_d - i\Delta\lambda_d]\right)P_{5i+1}(t) + \mu_d P_{5i+5}(t) + \mu_p P_{5i+2}(t),$$
$$dP_{5i+2} / dt = -(2\lambda_p + \mu_p + [\lambda_d - i\Delta\lambda_d])P_{5i+2}(t) + 3\lambda_p P_{5i+1}(t) + 2\mu_p P_{5i+3}(t) + \mu_d P_{5i+5}(t),$$
$$dP_{5i+3} / dt = -2\mu_p P_{5i+3}(t) + 2\lambda_p P_{5i+2}(t),$$
$$dP_{5i+4} / dt = -\mu_d P_{5i+4}(t) + [\lambda_d - i\Delta\lambda_d]P_{5i+2}(t),$$
$$dP_{5i+5} / dt = -\mu_d P_{5i+5}(t) + [\lambda_d - i\Delta\lambda_d]P_{5i+1}(t);$$

$\Phi_{к}$ – описують рівняння: (4.21)

$$dP_{5k+1} / dt = -3\lambda_p P_{5k+1}(t) + \mu_p P_{5k+2}(t) + \mu_d P_{5i+4}(t),$$
$$dP_{5k+2} / dt = -(2\lambda_p + \mu_p)P_{5k+1}(t) + 3\lambda_p P_{5k+1}(t) + 2\mu_p P_{5k+3}(t) + \mu_d P_{5i+4}(t$$
$$dP_{3k+3} / dt = -2\mu_p P_{3k+3}(t) + 2\lambda_p P_{3k+2}(t).$$

Функція готовності визначається як сума ймовірностей знаходження системи в працездатних станах $MS_p = \{ S_1, S_2, ..S_{5i+1}, \ldots, S_{5i+2}, S_{5k+1}, S_{5k+2} \}$ за виразом (4.4). Функція оперативної готовності за виразом (4.5).

4.3.4 Результати багатофрагментного марковського моделювання готовності ПТК побудованими за дубльованою та мажоритарною архітектурами

Аналіз моделей показав зростання розмірності вирішуваних завдань, пов'язаних з ускладненням розглянутих структур систем, що призводить до збільшення розмірності матриці СДУ Колмогорова-Чепмена. Так, для ПТК побудованого за архітектурою S^p_{22} (рис.4.22) залежність кількісті

фрагментів і станів моделі від числа неусунутих ДП ПЗ, оцінена за допомогою виразу (4.2), наведена в таблиці 4.3.

Таблиця 4.3.

Залежність кількісті фрагментів і станів моделі від числа неусунутих ДП ПЗ

Число фрагментів (N)	Число станів фрагмента	$N_{дп\ пз}=6$	$N_{дп\ пз}=50$
$Ф_п=1$	6	1	1
$Ф_I=1$	7	2	2
$Ф_{II}=N-2$	7	2	46
$Ф_{III}=2$	8	2	2
$Ф_{IV}=N-6$	8	0	44
$Ф_V=2$	7	2	2
$Ф_{передостанній}=1$	6	1	1
$Ф_к=4$	4	1	1
Усього фрагментів		11	99
Усього станів		74	744

За допомогою модифікованого експоненціального методу та використовуя кількісні значення параметрів моделей одержано оцінки значень показника надійності – функції готовності для дубльованих та мажоритарно-резервованих архітектур ПТК.

Таблиця 4.4.

Кількісні значення параметрів

λ_p (1/г)	μ_p (1/г)	λ_d (1/г)	μ_d (1/г)	$\Delta\mu_d$ (1/г)	$\Delta\lambda_d$ (1/г)	$\Delta_{\mu d}$ (1/г)	$\Delta_{\lambda d}$ (1/г)
10^{-3}	$4{,}1\cdot10^{-2}$	$1{,}5\cdot10^{-3}$	0,2	$5\cdot10^{-2}$	$5\cdot10^{-4}$	10^{-5}	10^{-4}

Результати обчислень представлені у вигляді графічної залежності функції готовності від часу функціонування системи на рісунках.4.35-4.18.

Аналіз результатів моделювання дубльованих архітектур дозволяє зробити наступні висновки. Найбільш «сприятливий» результат

моделювання в обох випадках дають ББМ 1 (найбільш швидкий перехід до сталого режиму функціонування), а найменш «сприятливий» БММ 7,

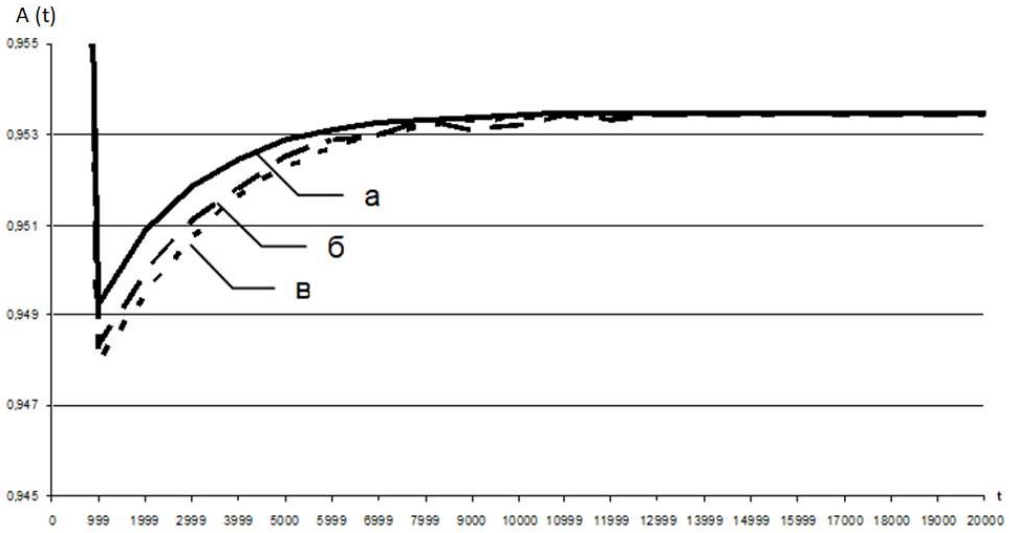


Рис. 4.35 Результати оцінювання готовності дубльованого одноверсійного ПТК S_{21} за наступними ББМ: а) ББМ 1, б) ББМ XII, в) ББМ VII

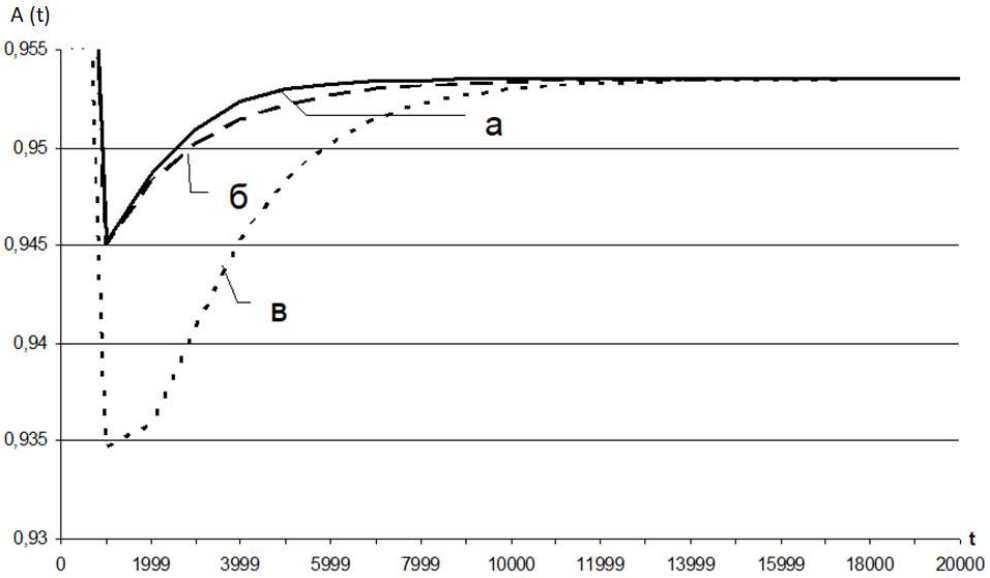


Рис. 4.36 Результати оцінювання готовності дубльованого двохверсійного ПТК S_{22} за наступними ББМ: а) ББМ 1, б) ББМ XII, в) ББМ VII

що безумовно пов'язано зі збільшенням часу, необхідного на усунення чергового програмного дефекту. Показник готовності, отриманий за допомогою БММ 12 має незначні нестабільні коливання протягом усього періоду дослідження (рисунок .4.35). Таке явище легко пояснити

«випадковим» характером зміни параметрів потоків відмов і відновлень ПС при переході від одного фрагмента до іншого.

Порівняння результатів моделювання одно- і двухверсіонних архітектур показав, що в процесі усунення ДП ПЗ готовність систем асимптотично прагне до прямої A = 0,954, яка характеризує сталий режим функціонування системи.

Очикуваний результат дає аналіз результатів моделювання за ББМ I та VIII для обох архітектур (рисунок 4.37). Функція готовності для двохверсійної архітектури має більш «глибоку» та довшу фазу зменшення.

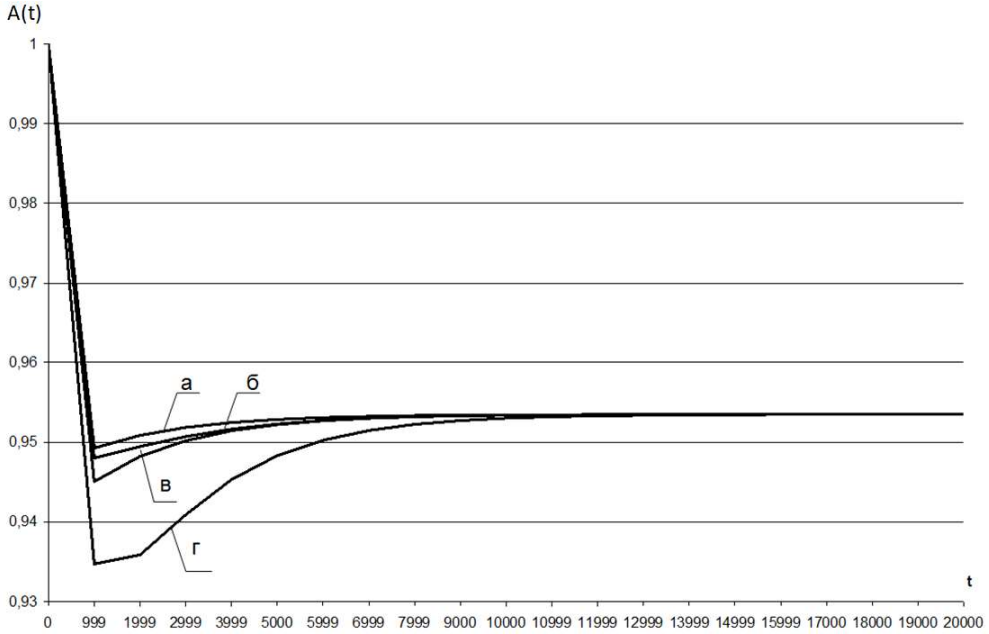


Рис. 4.37 Результати оцінювання готовності дубльованих архітектур за наступними ББМ: а) S_{21} ББМ 1, б) S_{21} ББМ VII, в) S_{22} ББМ I, г) S_{22} ББМ VII

На рис.4.38 показані графічні залежності зміни функції готовності в часі при моделюванні ПТК комплексом ББМ, що враховують зміну параметра μ_d. Аналіз представлених залежностей показав, що найбільш "несприятливі" результати моделювання дає допомогою ББМ VIII ($\Delta\lambda_d$ = const, $\Delta\mu_d$ = var). Для даної моделі етап приробітки має найбільшу тривалість (6800 годин) і на даному етапі коефіцієнт готовності приймає

мінімальне (в порівнянні з результатами моделювання ББМ IV і ББМ VI) значення (Кг = 0,933).

Порівняння результатів моделювання ПТК за допомогою ББМ IV ($\Delta\lambda_d = 0$, $\Delta\mu_d$= var) і ББМ VI ($\Delta\lambda_d = 0$, $\Delta\mu_d$ = const) показало, що в разі збільшення тривалості часових інтервалів між усунення ДП ПЗ (БММ 6) період приробotки більш затяжний (криві а і б).

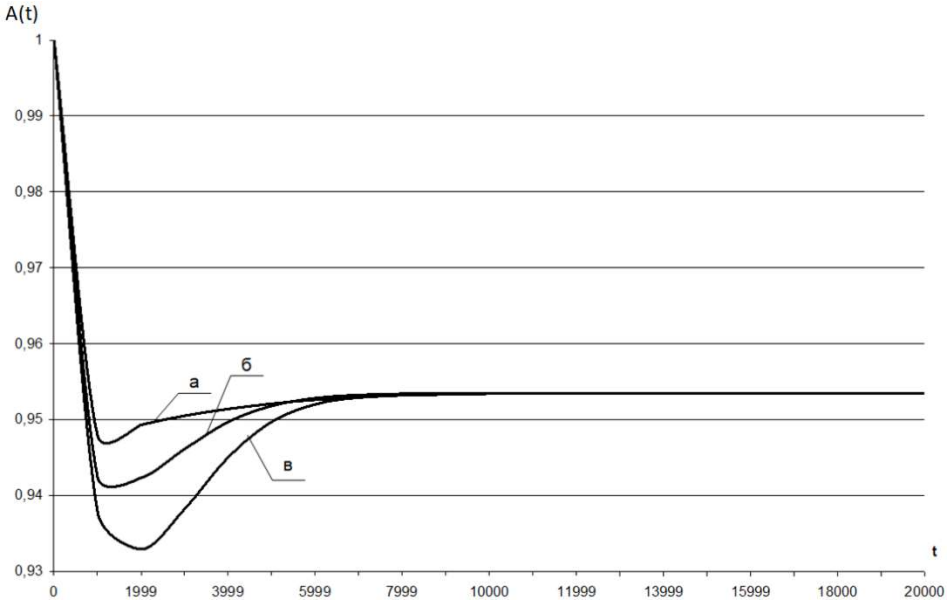


Рис. 4.38 Результати оцінювання готовності ПТК S_{21}
за наступними ББМ: а) ББМ IV, б) ББМ VI, в) ББМ VIII

Аналіз графіків на рис.4.39 дозволяє зробити висновок, що результати однофрагментного моделювання на ранніх етапах функціонування системи дають завищену оцінку, а після певного «переломного» моменту часу- занижену. При цьому коливання функції готовності проходять кілька оціночних рівнів шкали готовності. Відповідно, при виборі ОФМ можливий ризик помилкового визначення часового інтервалу «стабілізування» функції готовності (кінця етапу приробітки системи), а також неправильного визначення класу готовності ПТК.

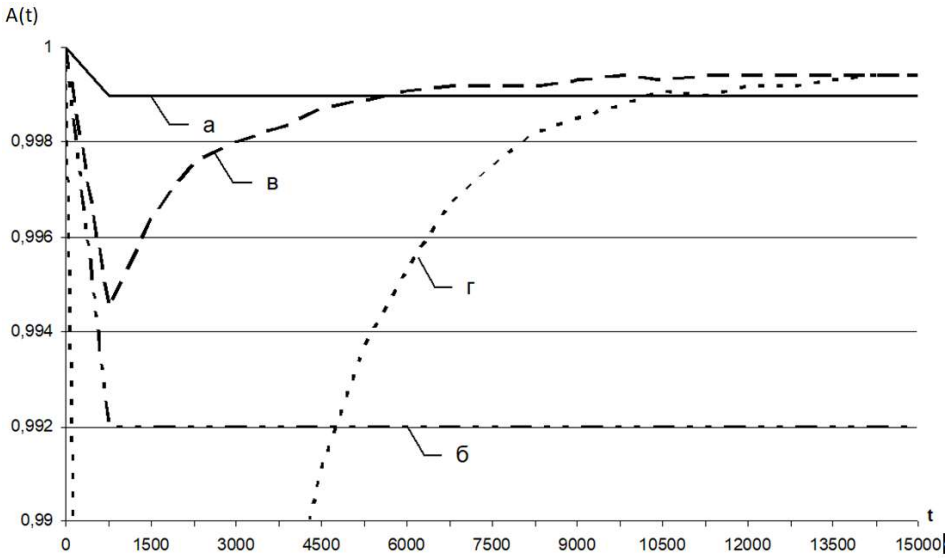


Рис. 4.39 Результати оцінювання готовності ПТК S_{21} за наступними ББМ: а) S^p_{22} ОФМ, б) S^p_{21} ОФМ, в) S^p_{22}ББМ I, г) S^p_{21} ББМ I

На рисунках.4.40-4.49 представлені деталізовані графіки зміни функції готовності дубльованих одно-і двухверсіонних ПТК, одержані в результаті застосування різних ББМ. Аналіз цих графіків показав, що на ранніх етапах функціонування ПТК велику роль відіграє вибір стратегії відновлення, яка впливає як на характер зміни функції готовності (зростає або зменшується), так і на кількісні результати оцінки готовності системи.

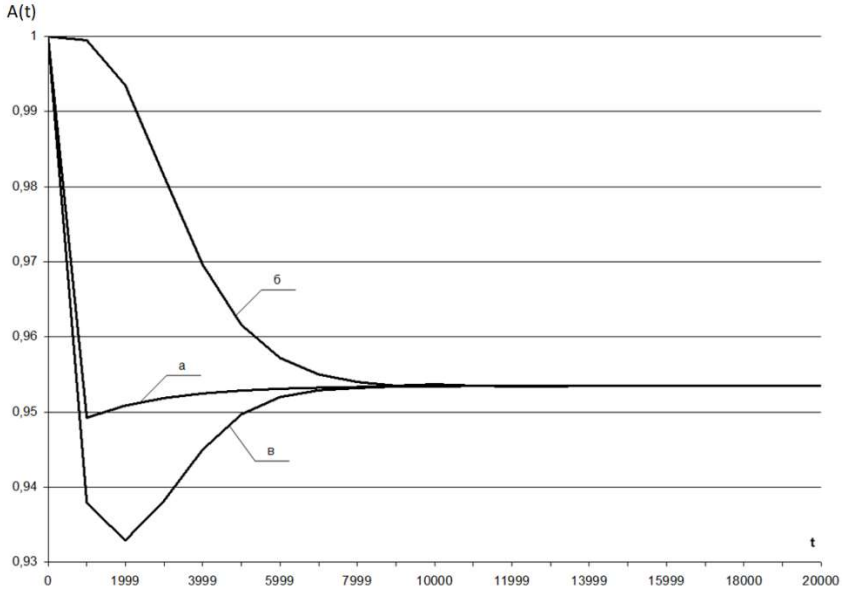


Рис. 4.40 Результати оцінювання готовності ПТК S_{21} за наступними ББМ: а) ББМ I, б) ББМ V, в) ББМ VI

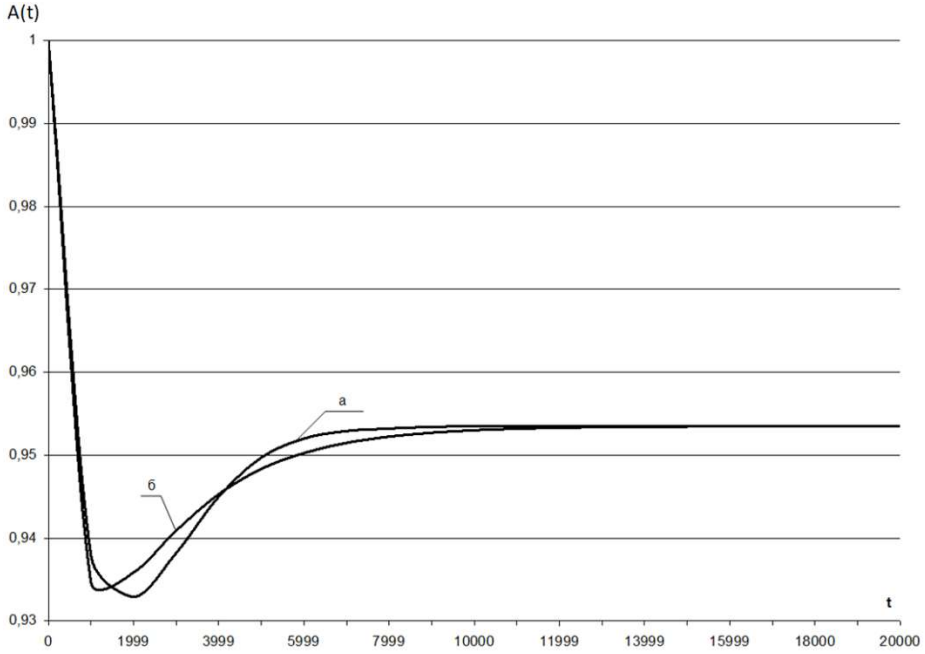


Рис. 4.41 Результати оцінювання готовності ПТК S_{21} за наступними ББМ: а) ББМ VII, б) ББМ VII

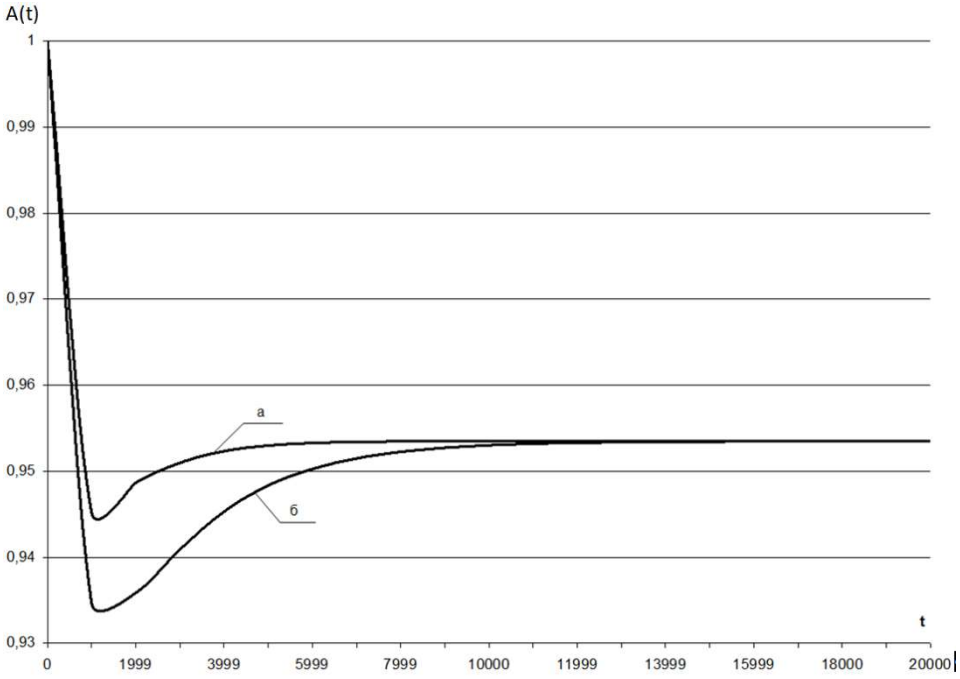


Рис. 4.42 Результати оцінювання готовності ПТК S_{22} за наступними ББМ: а) ББМ III, б) ББМ VII

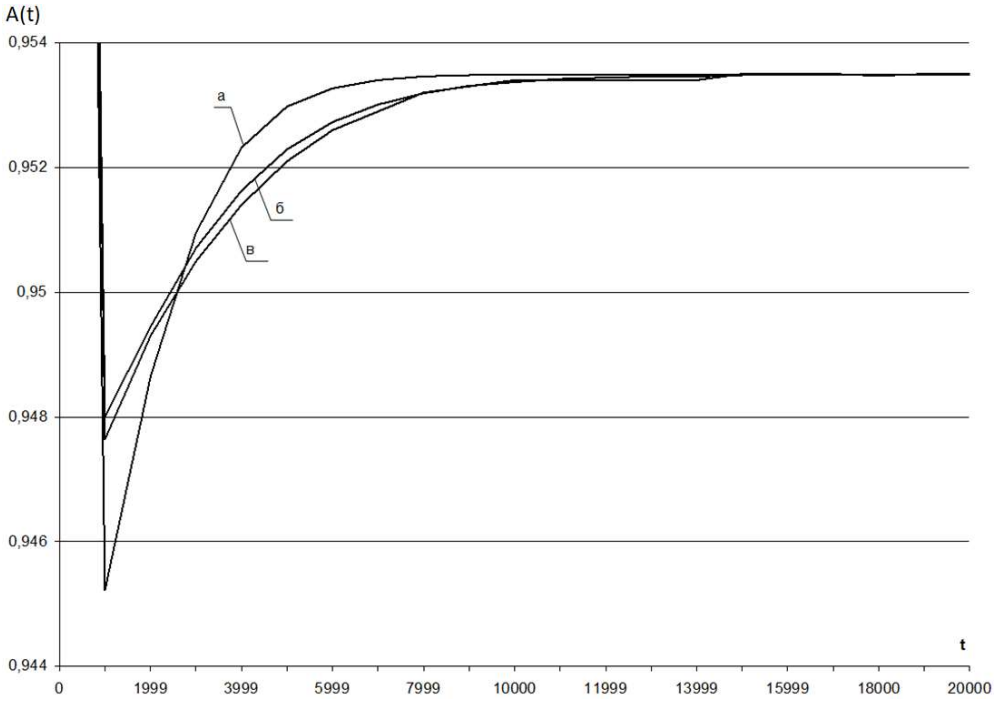


Рис. 4.43 Результати оцінювання готовності ПТК S_{21}
за наступними ББМ: а) S_{22} ББМ III, б) S_{21} ББМ VII, в) S_{21} ББМ VIII

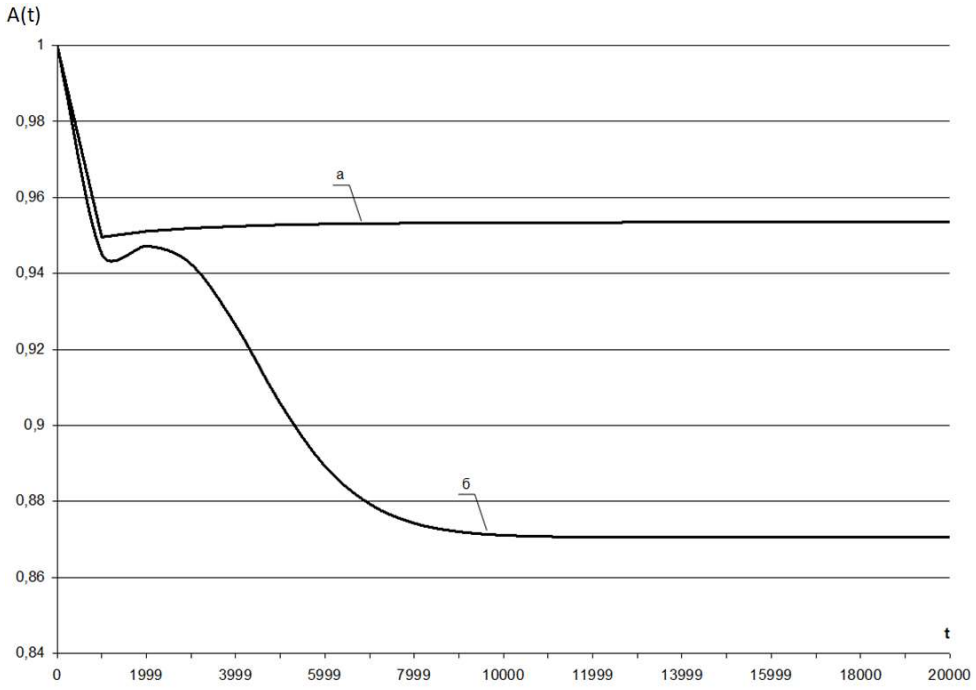


Рис. 4.44 Результати оцінювання готовності ПТК
за наступними ББМ: а) S_{21} ББМ II, б) S_{22} ББМ II

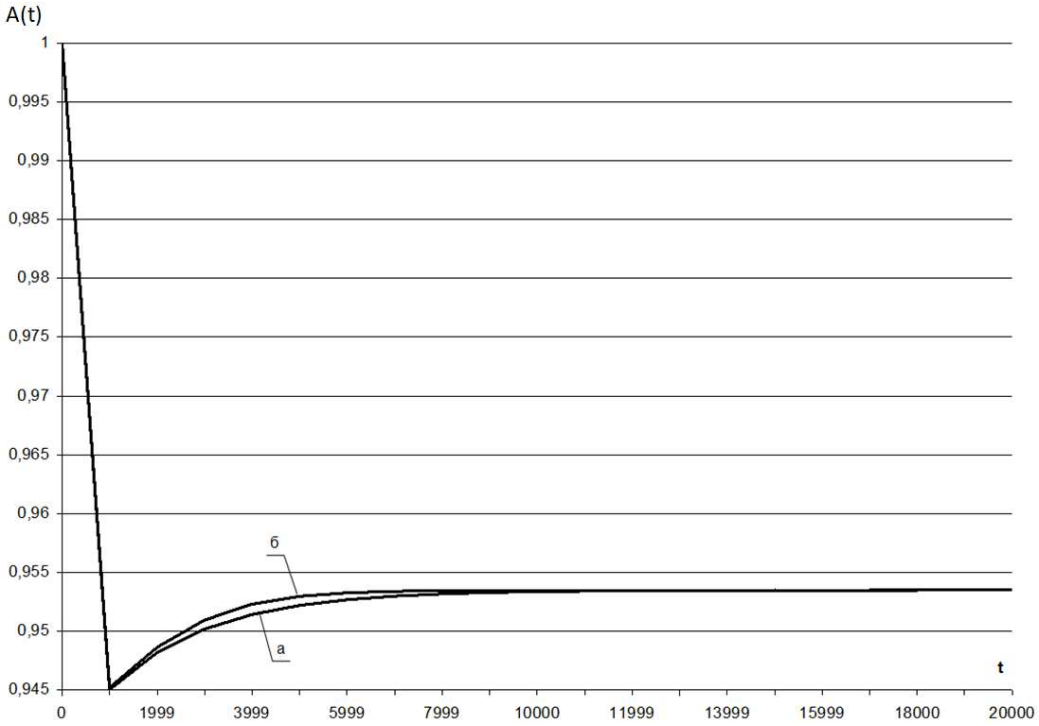


Рис. 4.45 Результати оцінювання готовності ПТК S_{22}

за наступними ББМ: а) ББМ I, б) ББМ III

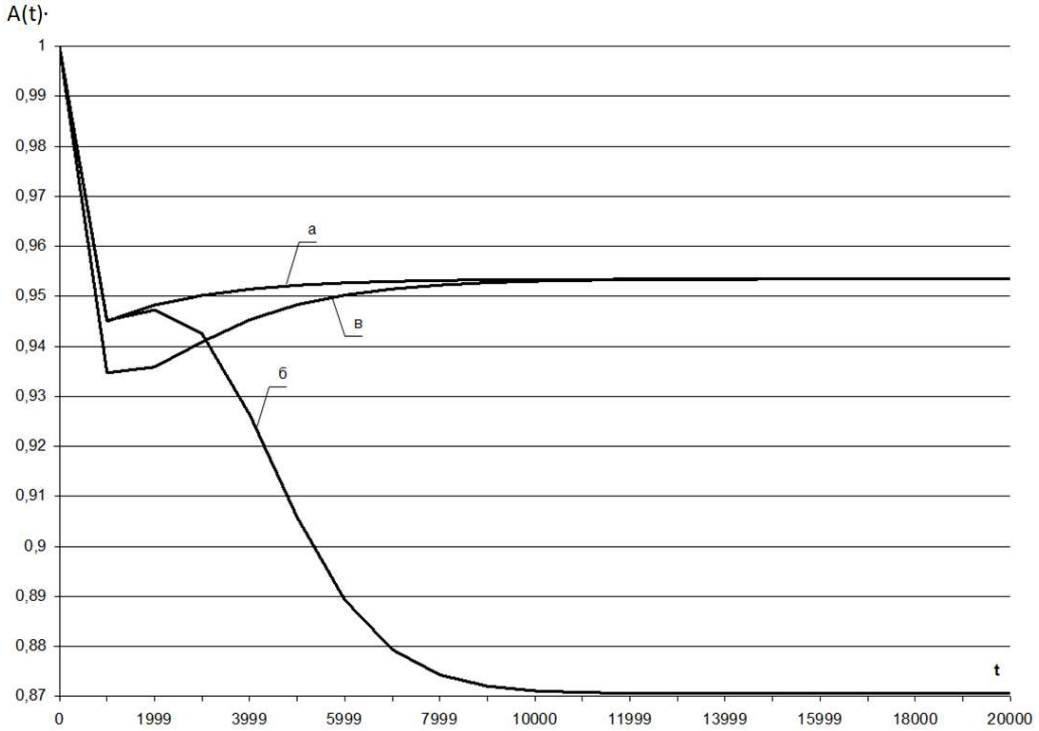


Рис. 4.46 Результати оцінювання готовності ПТК S_{22}

за наступними ББМ: а)ББМ I, б)ББМ II, в)ББМ II

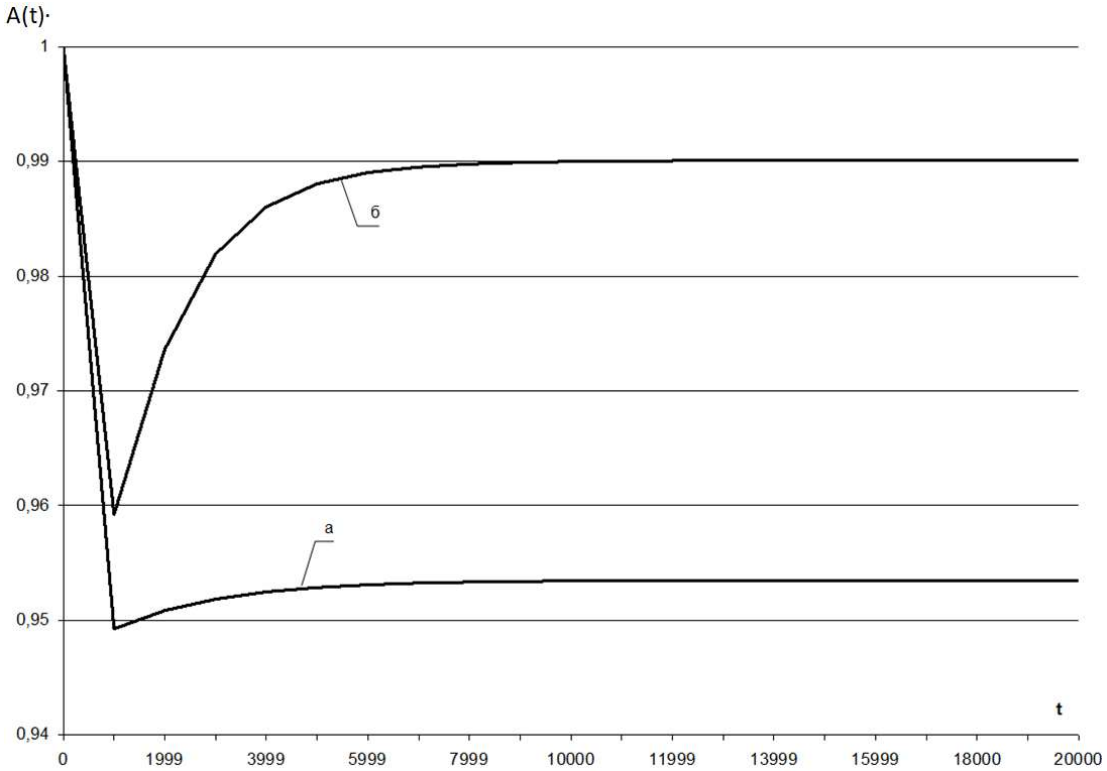


Рис. 4.47 Результати оцінювання готовності ПТК S_{21}

за наступними ББМ: а)ББМ I, б)ББМ IX

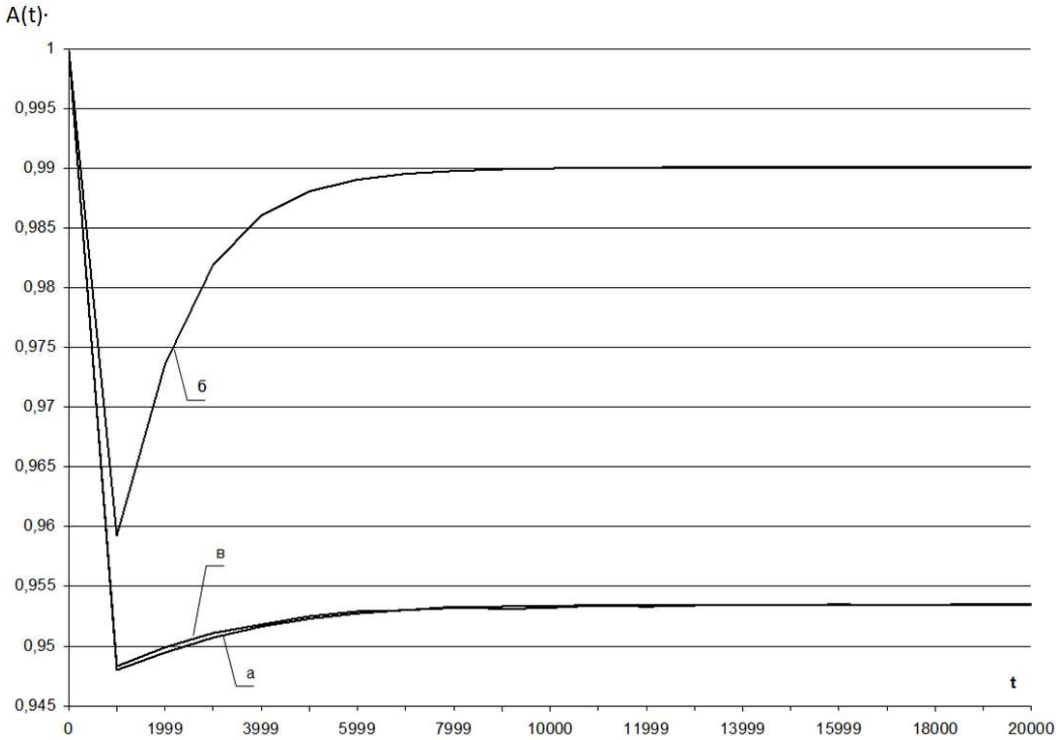


Рис. 4.48 Результати оцінювання готовності ПТК S_{21}

за наступними ББМ: а) ББМ VII, б)ББМ IX, в) ББМ XII

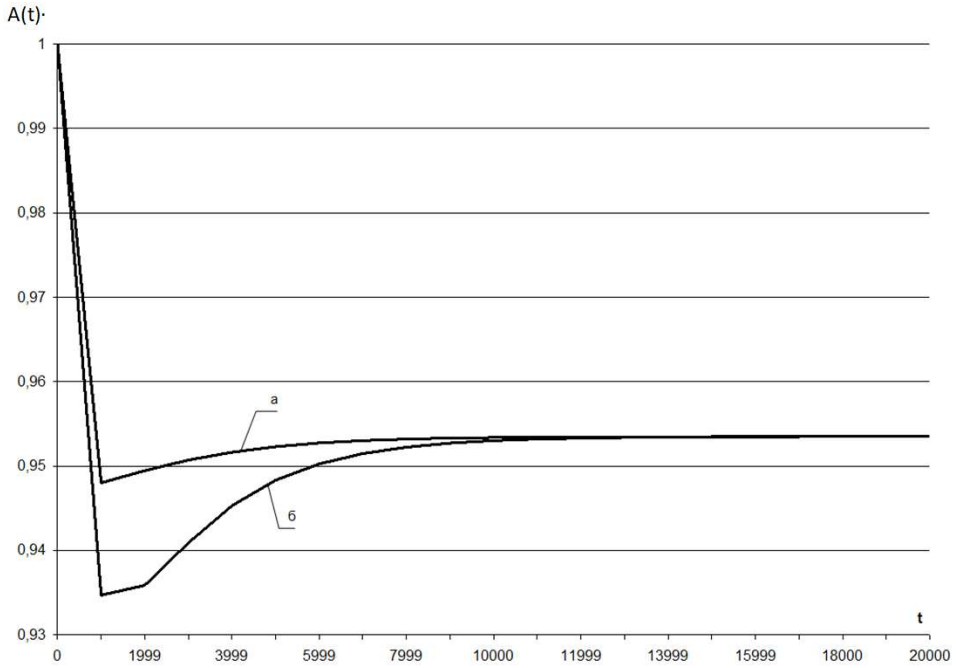


Рис. 4.49 Результати оцінювання готовності ПТК
за наступними ББМ: а) S_{21} ББМ VII, б) S_{22} ББМ VII

4.4 Розроблення і дослідження моделей готовності ПТК побудованих за двохкаскадними архітектурами

4.4.1 Багатофрагмента марковська модель готовності ПТК побудованого за структурою перший каскад 2/3, другий каскад 1/2

Розробимо БММ готовності двоверсійного ПТК, побудованого за двокаскадною схемою голосування, де перший каскад використовує логіку «2-з-3», а другий «1-з-2». Структуру даної системи наведено на Рисунку 4.12. Відповідно до даної структури побудовано ССН (Рисунок 4.50).

Використаємо сценарій зміни параметрів ББМ №1(1.2.1.1) згідно якого величина зміни інтенсивності прояву ДП ПЗ ($\Delta\lambda_d$) є сталою для кожного фрагмента, $\Delta\lambda_{di}$ = const, i $\in$1…N, де N – кількість фрагментів.

На рисунку 4.50 зображено базовий фрагмент ББМ, що описується станами:

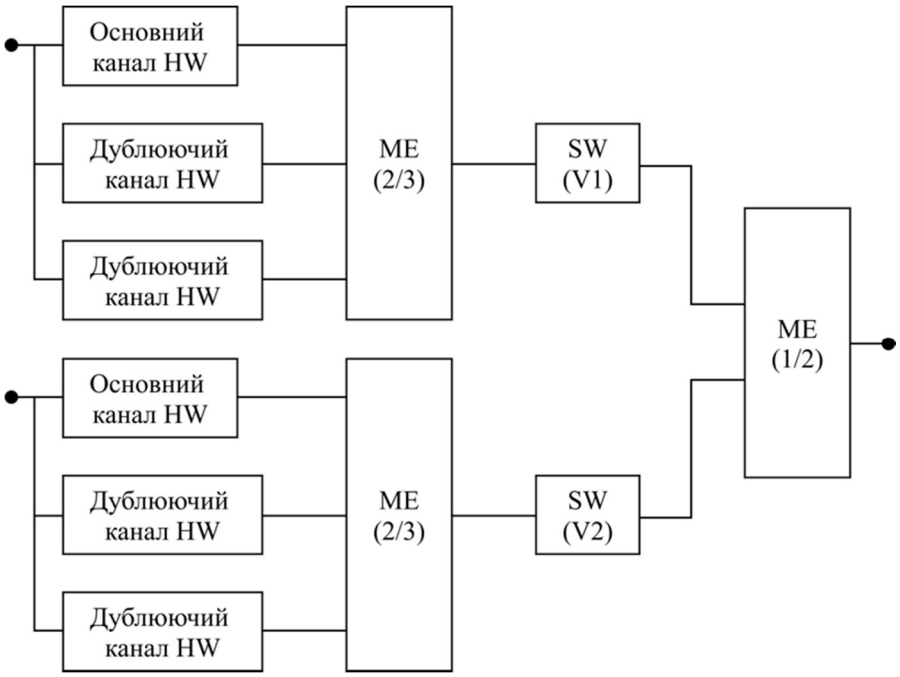


Рис. 4.50 Структурна схема надійності двоверсійного ПТК з двокаскадною логікою «2-з-3» та «1-з-2»

- S_1 – стан справний, справна робота обох підсистем;
- S_2 – стан працездатний, виявлено відмову одного каналу (основного або дубльованого) в одній з підсистем;
- S_3 – стан працездатний, виявлено другу відмову одного каналу (основного або дубльованого) у підсистемі, що вже містить одну відмову;
- S_4 – стан працездатний, відмова одного каналу (основного або дубльованого) у кожній з підсистем;
- S_5 – стан працездатний, відмова двох каналів у одній підсистемі та одного каналу (основного або дубльованого) у другій підсистемі;
- S_6 – стан непрацездатний, відмова двох каналів у кожній з підсистем.

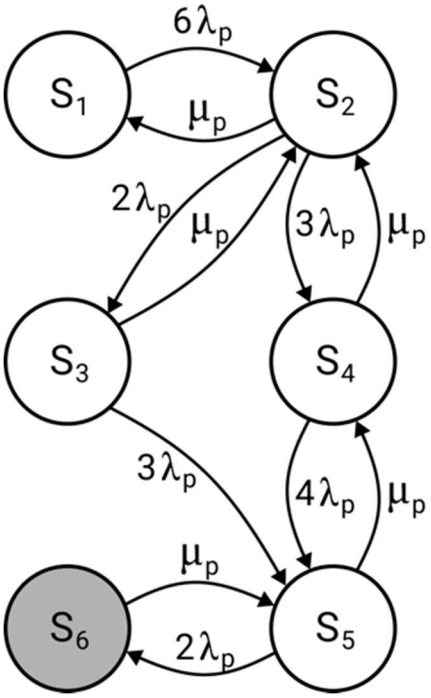


Рис. 4.51 Базовий фрагмент ББМ двоверсійної ПТК з двокаскадною логікою голосування «2-з-3» та «1-з-2»

Логіка функціонування системи, що описується базовим фрагментом є наступною. У початковий момент часу система реалізує всі функції й знаходиться у стані S_1. У випадковий момент часу в одному із каналів підсистем (основному або дубльованому) відбувається прояв фізичного дефекту й система переходить у стан S_2 з інтенсивністю $6\lambda_p$. При відновленні каналу після прояву дефекту система повертається до S_1 з інтенсивністю μ_p. Якщо протягом ремонту зламаного каналу один із двох справних каналів даної підсистеми також відмовляє, то відбувається переход зі стану S_2 у стан S_3 з інтенсивністю $2\lambda_p$ й відновлення до стану S_2 з інтенсивністю μ_p. Система переходить зі стану S_3 у стан S_5 з інтенсивністю $3\lambda_p$ якщо протягом відновлення другого каналу, що відмовило в цьому каналі, відмовляє одне шасі на справному каналі. Якщо протягом ремонту зламаного каналу (система знаходиться у стані S_2) відбувається відмова одного каналу у справній підсистемі, то система переходить зі стану S_2 у стан S_4 з інтенсивністю $3\lambda_p$ й відновлюється до

стану S_2 з інтенсивністю μ_p. Система переходить зі стану S_4 у стан S_5 з інтенсивністю $4\lambda_p$, якщо в одній з працездатних підсистем відмовляє другий канал. Використовуючи припущення обмеженості ресурсу відновлення, а саме те, що канали з відмовами відновлюються послідовно та при ремонтних роботах пріоритет віддається відновленню максимально можливої кількості підсистем [257], система переходить за стану S_5 у стан S_4 з інтенсивністю μ_p. Якщо відмовляє один з двох каналів у останній працездатній підсистемі, система переходить із S_5 у непрацездатний стан S_6. Відповідно до обраного сценарію (1.2.1.1) було побудовано макрограф досліджуваної системи зображений на Рисунку 4.52. Необхідно підкреслити, що дана модель розглядає такі рідкісні дефекти, які можуть спричинити відмову системи в цілому таким чином, було введено припущення про наявність не більше двох дефектів у кожній програмній версії системи [247]. Також із метою регулювання розмірності моделі, кількісні значення інтенсивностей відмов, спричинених ДП ПЗ для двох розглянутих програмних версій вважаються рівними [257, 313]. Описаний вище процес функціонування базового фрагмента притаманний усім внутрішнім фрагментам Φ_I – Φ_{VI} (Рисунок 4.52). Також макрограф містить фрагмент Φ_{SW} розподілений між Φ_I – Φ_{VI}, що включає в себе множину станів у яких проявився проектний дефект. БММ двоверсійного ПТК побудованого за схемою голосування, де перший каскад використовує логіку «2-з-3», а другий «1-з-2» (Рисунок 4.54) містить наступні стани:

− $\{S_1, S_{12}, S_{23}, S_{34}, S_{50}, S_{61}\}$ – стани, що описують справну роботу обох підсистем;

− $\{S_2, S_{13}, S_{24}, S_{35}, S_{51}, S_{62}\}$ – стани в яких відбулась відмова одного каналу (основного або дубльованого) в одній із підсистем;

− $\{S_3, S_{14}, S_{25}, S_{36}, S_{52}, S_{63}\}$ – стани в яких відбулась відмова другого каналу в одній із підсистем;

− $\{S_4, S_{15}, S_{26}, S_{37}, S_{53}, S_{64}\}$ – стани в яких відмовив один канал (основний або дубльований) у одній з підсистем;

– $\{S_5, S_{16}, S_{27}, S_{38}, S_{54}, S_{65}\}$ – стани в яких відмовило два канала в одній із підсистем, та один канал у другій;

– $\{S_6, S_{17}, S_{28}, S_{39}, S_{55}, S_{66}\}$ – стани в яких ДФ АК спричинив непрацездатність всієї системи;

– $\{S_7 – S_{10}, S_{18} – S_{21}, S_{29} – S_{32}, S_{40} – S_{43}, S_{45} – S_{48}, S_{56} – S_{59}\}$ – стани в яких виявився ДП ПЗ;

– $\{S_{11}, S_{22}, S_{33}, S_{44}, S_{49}, S_{60}\}$ – стани в яких поява ДП ПЗ спричинила непрацездатність всієї системи.

Зобразимо логіку функціонування системи шляхом подання процесу переходу від фрагменту $Ф_I$ до $Ф_{II}$, для чого використовуємо опис базового фрагменту (Рисунок 4.52), наданий раніше. Виходячи з припущення наявності двох ДП ПЗ, початковий фрагмент можна означити як (Рисунок 4.53):

$$Ф_I = \{(n_1; n_2)| \, n_1 = 2; n_2 = 2\} \quad (4.22)$$

де n_1 і n_2 – кількість ДП ПЗ у першій і другій версіях програмного забезпечення відповідно.

У початковий момент часу t_0 система виконує всі функції й справно функціонує (фрагмент $Ф_I$ стан S_1). При появі ДП ПЗ система переходить у стан S_7 (фрагмент $Ф_{SW}$) з інтенсивністю $2\lambda_d$ і відновлюється до S_{12} із μ_d. Стан S_{12} належить до множини станів першого внутрішнього фрагмента $Ф_{II}$:

$$Ф_{II} = \{(n_1; n_2)| \, \{n_1 = 1; n_2 = 2\} \text{ або } \{n_1 = 2; n_2 = 1\}\} \quad (4.23)$$

При появі ДП ПЗ у стані S_2, система переходить у S_8 з інтенсивністю $2\lambda_d$ і відновлюється до стану S_{12} з першого внутрішнього фрагмента $Ф_{II}$ з інтенсивністю μ_d. Переходи зі станів S_3, S_4, S_5 у стани S_9, S_{10}, S_{11} з інтенсивністю $2\lambda_d$ і відновлення до відповідних станів фрагмента $Ф_{II}$ описують процес появи й усунення ДП ПЗ. Надалі, внаслідок послідовного прояву ДП ПЗ й відновлення відбуваються переходи між наступними фрагментами $Ф_{III} – Ф_{VI}$:

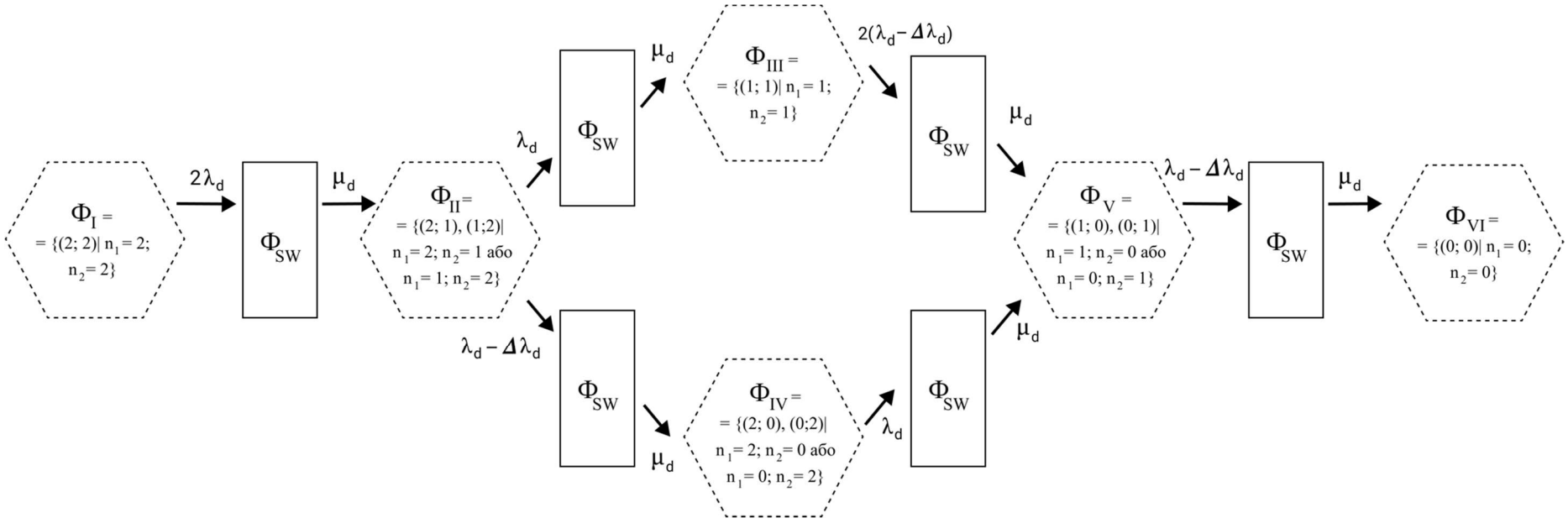


Рис. 4.52 – Макрограф ББМ двоверсійної ПТК з двокаскадною логікою «2-з-3» та «1-з-2»

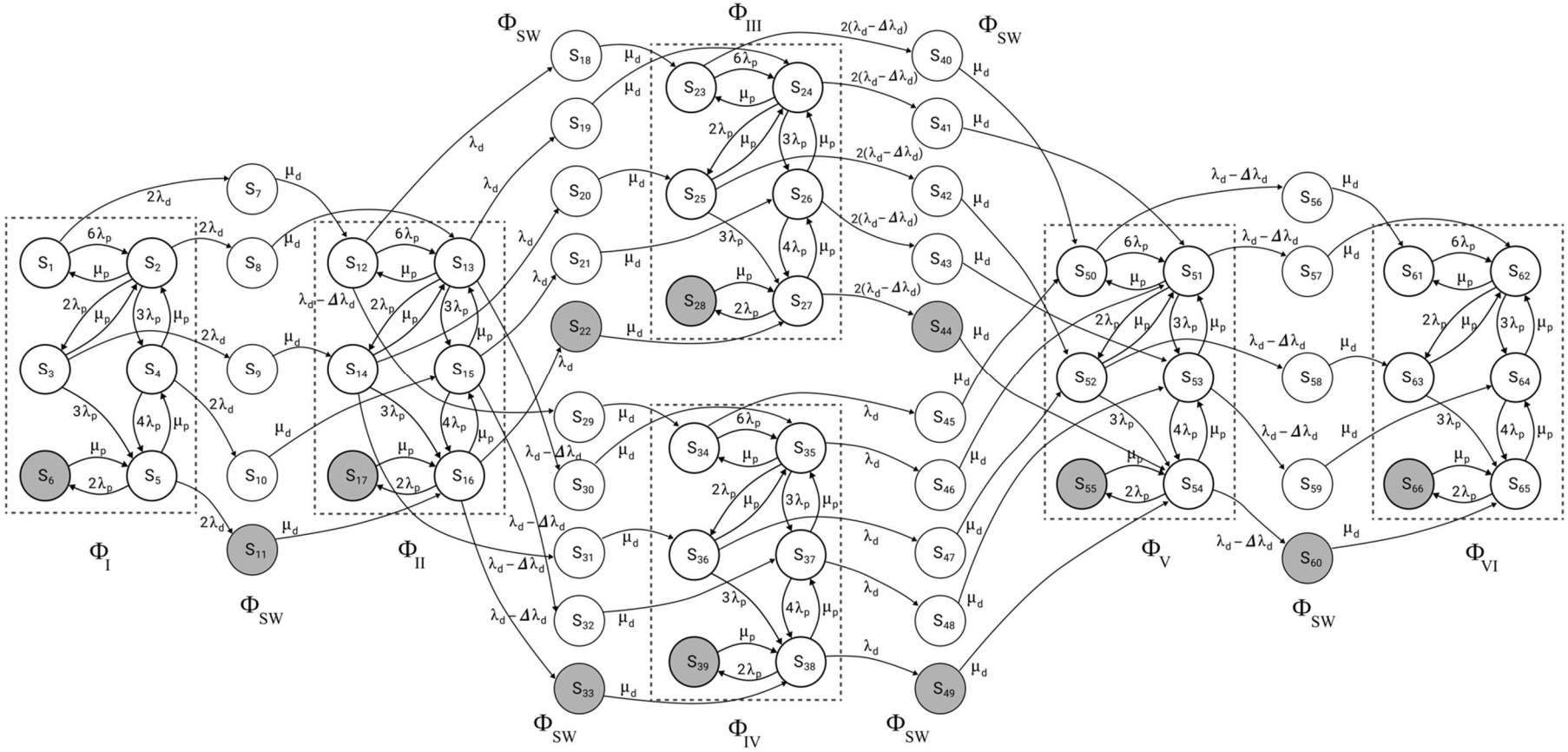


Рис. 4.53 – ББМ двоверсійної ПТК з двокаскадною логікою «2-з-3» та «1-з-2»

$$\Phi_{III} = \{(n_1; n_2)|\ n_1 = 1;\ n_2 = 1\} \quad (4.24)$$

$$\Phi_{IV} = \{(n_1; n_2)|\ \{n_1 = 0;\ n_2 = 2\}\ \text{або}\ \{n_1 = 2;\ n_2 = 0\}\} \quad (4.25)$$

$$\Phi_{V} = \{(n_1; n_2)|\ \{n_1 = 0;\ n_2 = 1\}\ \text{або}\ \{n_1 = 1;\ n_2 = 0\}\} \quad (4.26)$$

$$\Phi_{VI} = \{(n_1; n_2)|\ n_1 = 0;\ n_2 = 0\} \quad (4.27)$$

У кінцевому фрагменті Φ_{VI} усі ДП ПЗ усунено й подільше порушення функціонування системи може бути спричинене ДФ АЗ.

СДР Колмогорова-Чепмена, складена згідно з графом, зображеним на рисунку 4.53, має наступний вигляд:

– для початкового фрагмента Φ_I

$$\begin{aligned}
&dP_1 / dt = -(6\lambda_p + 2\lambda_d)P_1(t) + \mu_p P_2(t);\\
&dP_2 / dt = -(5\lambda_p + 2\lambda_d + \mu_p)P_2(t) + 6\lambda_p P_1(t) + \mu_p P_3(t) + \mu_p P_4(t);\\
&dP_3 / dt = -(3\lambda_p + 2\lambda_d + \mu_p)P_3(t) + 2\lambda_p P_2(t);\\
&dP_4 / dt = -(4\lambda_p + 2\lambda_d + \mu_p)P_4(t) + 3\lambda_p P_2(t) + \mu_p P_5(t);\\
&dP_5 / dt = -(2\lambda_p + \lambda_d + \mu_p)P_5(t) + 4\lambda_p P_4(t) + 3\lambda_p P_3(t) + \mu_p P_5(t);\\
&dP_6 / dt = -\mu_p P_6(t) + 2\lambda_p P_5(t);
\end{aligned} \quad (4.28)$$

– для першого внутрішнього (типового внутрішнього) фрагмента Φ_{II}

$$\begin{aligned}
&dP_{12}(t) / dt = -(2\lambda_d - \Delta\lambda_d + 6\lambda_p)P_{12}(t) + \mu_d P_7(t) + \mu_p P_{13}(t);\\
&dP_{13}(t) / dt = -(2\lambda_d - \Delta\lambda_d + 5\lambda_p + \mu_p)P_{13}(t) + 6\lambda_p P_{12}(t) + \mu_p P_{14}(t) + \mu_p P_{15}(t) + \mu_d P_{8}(t);\\
&dP_{14}(t) / dt = -(2\lambda_d - \Delta\lambda_d + \mu_p + 3\lambda_p)P_{14}(t) + 2\lambda_p P_{13}(t) + \mu_d P_9(t);\\
&dP_{15}(t) / dt = -(2\lambda_d - \Delta\lambda_d + 4\lambda_p + \mu_p)P_{15}(t) + 3\lambda_p P_{13}(t) + \mu_d P_{10}(t) + \mu_p P_{16}(t);\\
&dP_{16}(t) / dt = -(2\lambda_d - \Delta\lambda_d + 2\lambda_p + \mu_p)P_{16}(t) + 4\lambda_p P_{15}(t) + 3\lambda_p P_{14}(t) + \mu_d P_{11}(t) + \mu_p P_{17}(t);\\
&dP_{17}(t) / dt = -\mu_p P_{17}(t) + 2\lambda_p P_{17}(t);
\end{aligned} \quad (4.29)$$

– для кінцевого фрагмента Φ_{VI}

$$\begin{aligned}
&dP_{61}(t) / dt = -6\lambda_p P_{61}(t) + \mu_d P_{56}(t) + \mu_p P_{62}(t);\\
&dP_{62}(t) / dt = -(5\lambda_p + \mu_p)P_{62}(t) + \mu_d P_{57}(t) + 6\lambda_p P_{61}(t) + \mu_p P_{63}(t) + \mu_p P_{64}(t);\\
&dP_{63}(t) / dt = -(3\lambda_p + \mu_p)P_{63}(t) + \mu_d P_{58}(t) + 2\lambda_p P_{62}(t);\\
&dP_{64}(t) / dt = -(4\lambda_p + \mu_p)P_{64}(t) + \mu_d P_{59}(t) + 3\lambda_p P_{62}(t) + \mu_p P_{66}(t);\\
&dP_{65}(t) / dt = -(2\lambda_p + \mu_p)P_{65}(t) + \mu_d P_{60}(t) + 3\lambda_p P_{63}(t) + \mu_p P_{66}(t) + 4\lambda_p P_{59}(t);\\
&dP_{66}(t) / dt = -\mu_d P_{66}(t) + 2\lambda_p P_{65}(t);
\end{aligned} \quad (4.30)$$

- початкові умови

$$P_1(0) = 1, P_i(0) = 0, i \in 2,3,...,66\ . \tag{4.31}$$

4.4.2 Багатофрагмента марковська модель готовності ПТК побудованого за структурою перший каскад 1/2, другий каскад 2/3

Розробимо БММ готовності двоверсійного ПТК побудованого за двокаскадною структурою, де перший каскад використовує логіку «1-з-2», а другий «2-з-3». Структуру досліджуваної системи наведено на Рисунку 4.13 та відповідно до неї побудовано ССН (Рисунок 4.54).

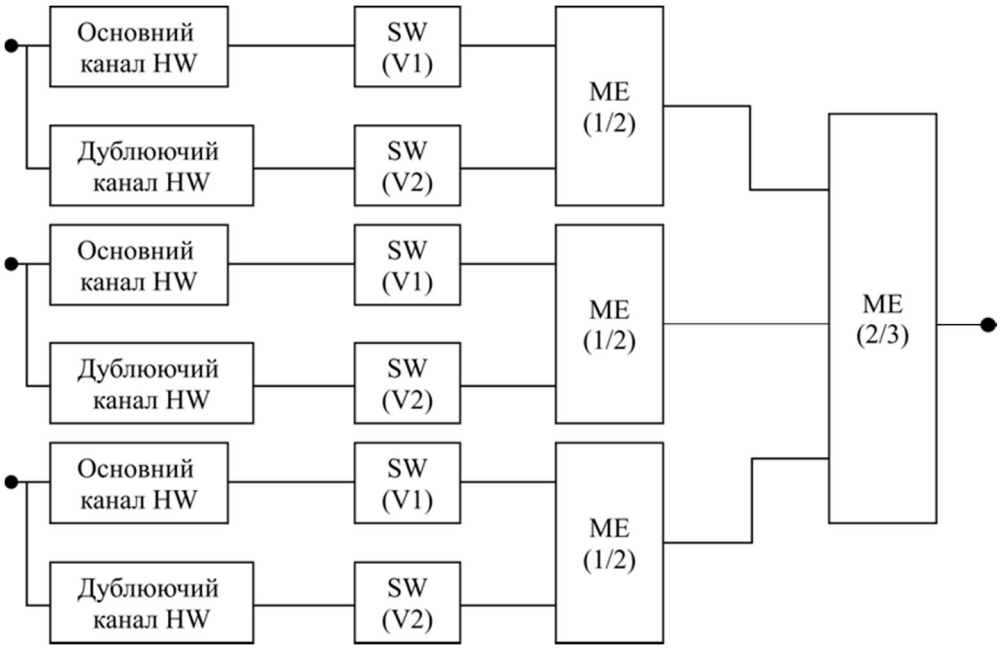


Рис. 4.54 Структурна схема надійності двоверсійного ПТК з двокаскадною логікою «1-з-2» та «2-з-3»

Як і для попередньо розробленої моделі використаємо сценарій зміни параметрів ББМ№1(1.2.1.1) відповідно до якої величина $\Delta\lambda_d$ є сталою для кожного фрагменту. На рисунку 4.55 зображено базовий фрагмент ББМ, що описується наступними станами:

- S_1 – стан справний, справна робота трьох підсистем;

- S_2 – стан працездатний, відмова каналу в одній з трьох підсистем;
- S_3 – стан працездатний, у двох підсистемах відбулась відмова одного каналу;
- S_4 – стан працездатний, відмова однієї підсистеми;
- S_5 – стан працездатний, відмова одного каналу в кожній підсистемі;
- S_6 – стан працездатний, відмова однієї підсистеми та відмова основного або дубльованого каналу в одній із працездатних підсистем;
- S_7 – стан працездатний, відмова однієї підсистеми та відмова одного каналу в кожній працездатній підсистемі;
- S_8 – стан непрацездатний, відмова двох підсистем, остання підсистема справна;
- S_9 – стан непрацездатний, відмова двох підсистем, остання підсистема праццездатна.

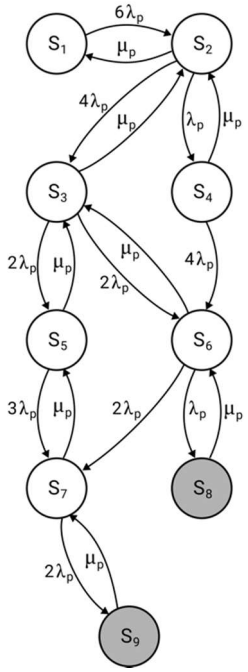


Рис. 4.55 Базовий фрагмент ББМ двоверсійної ПТК з двокаскадною логікою «1-з-2» та «2-з-3»

Базовий фрагмент (Рисунок 4.55) описує таку логіку функціонування системи. У початковий момент часу t_0 система є справною, знаходиться у стані S_1 й виконує всі функції. У випадковий момент часу виявляється ДФ АЗ та система переходить зі S_1 у S_2 з інтенсивністю $6\lambda_p$ та відновлюється до S_1 з інтенсивністю $\mu_р$. У разі, якщо в процесі відновлення зламаного каналу ДФ АЗ виявляється на іншому компоненті, модель досліджує два варіанти поводження системи:

а) якщо в процесі відновлення відбувається повторний прояв ДФ АЗ у цій підсистемі, то система переходить у S_4 з інтенсивністю λ_p і відновлюється до S_2 з μ_p. Даний варіант приводить систему в режим роботи з двома підсистемами. Система переходить із S_4 у S_6 з інтенсивністю $4\lambda_p$ при виявленні ДФ АЗ на одному з каналів у справній підсистемі. Стан S_6 також описує режим роботи при одній справній та другій працездатній підсистемах. Враховуючи пріоритет відновлення до максимальної кількості підсистем, із S_6 система переходить у S_3 з μ_p. Якщо у S_6 відбувається відмова одного каналу в справній підсистемі, то відбувається перехід системи у S_7 із інтенсивністю $2\lambda_p$; якщо в стані S_6 відбувається відмова через появу ДФ АЗ у працездатній підсистемі, то система переходить у S_8 з інтенсивністю λ_p і відновлюється у S_6 з μ_p;

б) якщо в процесі відновлення відмова відбувається в одній із справних підсистем, то система переходить із S_2 у S_3 з інтенсивністю $4\lambda_p$ і відновлюється у S_2 з інтенсивністю μ_p. Стан S_3 описує варіант роботи системи з лише однією справною підсистемою та двома працездатними. Якщо відмова, спричинена появою ДФ АЗ, відбувається в справній підсистемі, система переходить у S_5 з $2\lambda_p$ і відновлюється назад з μ_p. У разі відмови однієї з працездатних підсистем відбувається перехід у стан S_6 і відновлюється з μ_p. Зі стану S_5 система переходить у стан S_7 з інтенсивністю $3\lambda_p$ і відновлюється назад з інтенсивністю μ_p, якщо відбулась повторна відмова в одній з трьох працездатних підсистем. При появі відмови в одній з двох працездатних підсистем система переходить зі стану S_7 у непрацездатний стан S_8 з $2\lambda_p$ і відновлюється назад з μ_p.

Процеси виявлення та усунення ДП ПЗ для даної системи, за умови використання припущення наявності не більше двох дефектів у кожній версії програмного забезпечення [313], можуть бути досліджені використовуючи макрограф ідентичний побудованому для двоверсійної ПТК з двокаскадною логікою «2-з-3» та «1-з-2» (Рисунок 4.53). Описаний вище процес функціонування базового фрагмента є аналогічним для всіх внутрішніх фрагментів ББМ. ББМ готовності двоверсійного ПТК побудованого за двокаскадною схемою голосування, де перший каскад використовує логіку «1-з-2», а другий «2-з-3» (Рисунок 4.56) містить наступні стани:

- $\{S_1, S_{17}, S_{33}, S_{49}, S_{72}, S_{88}\}$ –стани в яких усі три підсистеми справні;
- $\{S_2, S_{18}, S_{34}, S_{50}, S_{73}, S_{89}\}$ –стани в яких сталася відмова одного каналу в одній з трьох підсистем;
- $\{S_3, S_{19}, S_{35}, S_{51}, S_{74}, S_{90}\}$ – стани в яких сталася відмова одного каналу в двох підсистемах;
- $\{S_4, S_{20}, S_{36}, S_{52}, S_{75}, S_{91}\}$ – стани в яких сталася відмова однієї підсистеми;
- $\{S_5, S_{21}, S_{37}, S_{53}, S_{76}, S_{92}\}$ – стани в яких відбулась відмова одного каналу в кожній з підсистем;
- $\{S_6, S_{22}, S_{38}, S_{54}, S_{77}, S_{93}\}$ – стани в яких сталася відмова однієї підсистеми й основного або дубльованого каналу в одній з справних підсистем; $\{S_7, S_{23}, S_{39}, S_{55}, S_{78}, S_{94}\}$ – стани в яких відбулась відмова однієї підсистеми й одного каналу в кожній з двох підсистем;
- $\{S_8, S_9, S_{24}, S_{25}, S_{40}, S_{41}, S_{56}, S_{57}, S_{79}, S_{80}, S_{95}, S_{96}\}$ – стани в яких поява ДФ АЗ спричинила непрацездатність всієї системи;
- $\{S_{10} – S_{16}, S_{26} – S_{32}, S_{42} – S_{48}, S_{58} – S_{71}, S_{81} – S_{87}\}$ – стани в яких виявився ДП ПЗ;

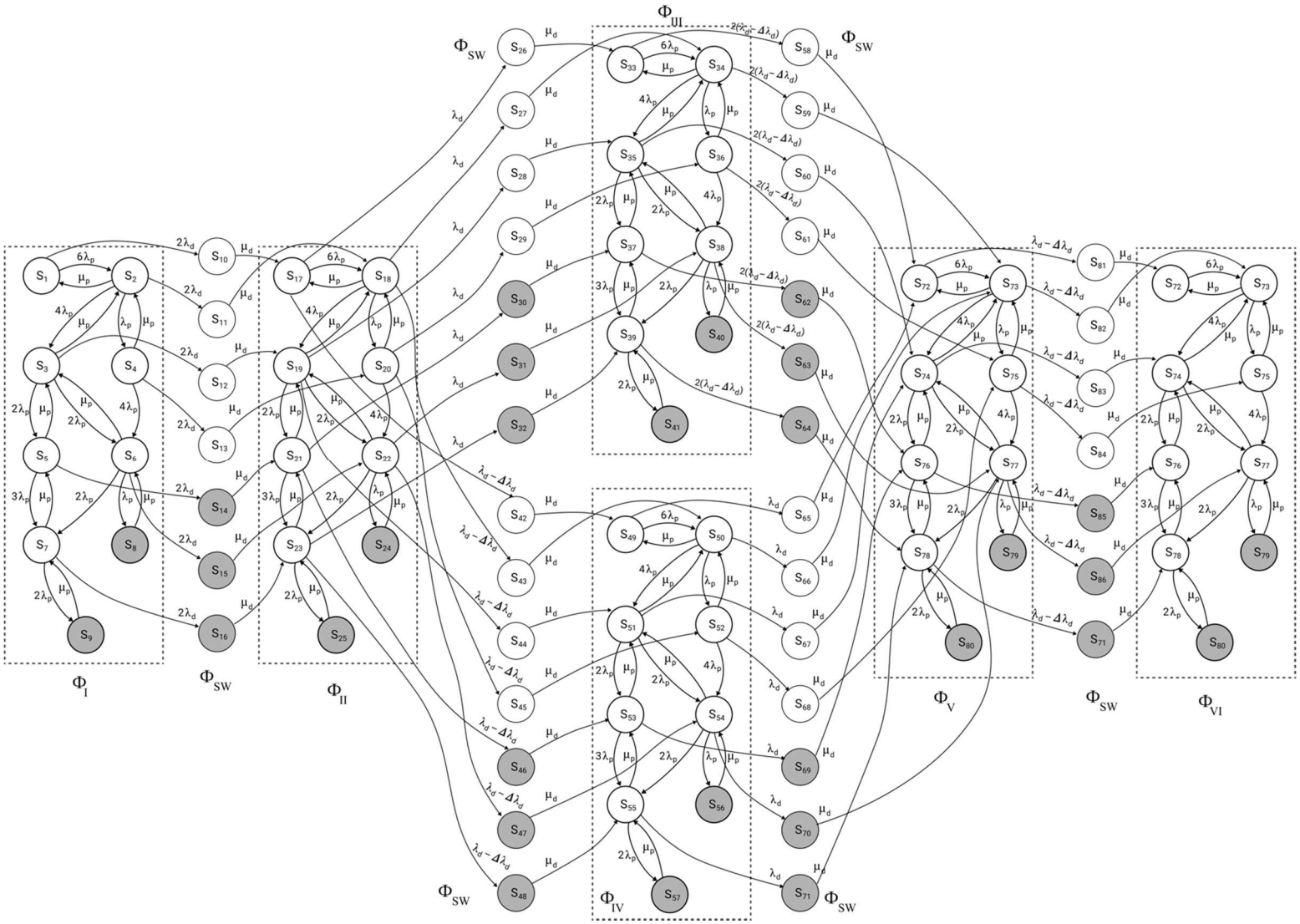


Рис. 4.56 ББМ двоверсійної ПТК з двокаскадною логікою «1-з-2» та «2-з-3»

– $\{S_{14} – S_{16},\ S_{30} – S_{32},\ S_{46} – S_{48},\ S_{62} – S_{64},\ S_{69} – S_{71},\ S_{85} – S_{87}\}$ – стани в яких поява ДП ПЗ призвела до непрацездатності всієї системи.

Логіка функціонування укрупненої ББМ, зображеної на рисунку 4.56, є ідентичною логіці функціонування ББМ двоверсійної ПТК з двокаскадною логікою «2-з-3» та «1-з-2» (Рисунок 4.53). Переходи між фрагментами здійснюються згідно процесів появи та усунення ДП ПЗ для двох версій програмного забезпечення.

СДР Колмогорова, складена згідно з графом зображеним на рисунку 4.56, має наступний вигляд:

– для початкового фрагмента Φ_I

$$
\begin{aligned}
&dP_1(t)/dt = -(6\lambda_p + 2\lambda_d)P_1(t) + \mu_p P_2(t);\\
&dP_2(t)/dt = -(\mu_p + 5\lambda_p + 2\lambda_d)P_2(t) + 6\lambda_p P_1(t) + \mu_p P_4(t) + \mu_p P_3(t);\\
&dP_3(t)/dt = -(\mu_p + 2\lambda_d + 4\lambda_p)P_3(t) + 4\lambda_p P_2(t) + \mu_p P_6(t) + \mu_p P_5(t);\\
&dP_4(t)/dt = -(4\lambda_p + \mu_p + 2\lambda_d)P_4(t) + \lambda_p P_2(t);\\
&dP_5(t)/dt = -(\mu_p + 2\lambda_d + 3\lambda_p)P_5(t) + 2\lambda_p P_3(t) + \mu_p P_7(t);\\
&dP_6(t)/dt = -(\mu_p + 2\lambda_d + 3\lambda_p)P_6(t) + 4\lambda_p P_4(t) + 2\lambda_p P_3(t) + \mu_p P_8(t);\\
&dP_7(t)/dt = -(\mu_p + 2\lambda_d + 2\lambda_p)P_7(t) + 3\lambda_p P_5(t) + 2\lambda_p P_6(t) + \mu_p P_9(t);\\
&dP_8(t)/dt = -\mu_p P_8(t) + \lambda_p P_6(t);\\
&dP_9(t)/dt = -\mu_p P_9(t) + 2\lambda_p P_7(t);
\end{aligned}
\qquad (4.32)
$$

– для першого внутрішнього (типового внутрішнього) фрагмента Φ_{II}:

$$
\begin{aligned}
&dP_{17}(t)/dt = -(6\lambda_p + 1.5\lambda_d)P_{17}(t) + \mu_p P_{18}(t) + \mu_d P_{10}(t);\\
&dP_{18}(t)/dt = -(\mu_p + 5\lambda_p + 1.5\lambda_d)P_{18}(t) + 6\lambda_p P_{17}(t) + \mu_p P_{19}(t) + \mu_p P_{20}(t) + \mu_d P_{11}(t);\\
&dP_{19}(t)/dt = -(\mu_p + 1.5\lambda_d + 4\lambda_p)P_{19}(t) + 4\lambda_p P_{18}(t) + \mu_d P_{12}(t) + \mu_p P_{22}(t) + \mu_d P_{21}(t);\\
&dP_{20}(t)/dt = -(4\lambda_p + \mu_p + 1.5\lambda_d)P_{20}(t) + \lambda_p P_{18}(t) + \mu_d P_{13}(t);\\
&dP_{21}(t)/dt = -(\mu_p + 1.5\lambda_d + 3\lambda_p)P_{21}(t) + 2\lambda_p P_{19}(t) + \mu_p P_{23}(t) + \mu_d P_{14}(t);\\
&dP_{22}(t)/dt = -(\mu_p + 1.5\lambda_d + 3\lambda_p)P_{22}(t) + 2\lambda_p P_{19}(t) + 4\lambda_p P_{20}(t) + \mu_p P_{24}(t) + \mu_p P_{15}(t);\\
&dP_{23}(t)/dt = -(\mu_p + 1.5\lambda_d + 2\lambda_p)P_{23}(t) + 3\lambda_p P_{21}(t) + 2\lambda_p P_{22}(t) + \mu_p P_{25}(t) + \mu_p P_{16}(t);\\
&dP_{24}(t)/dt = -\mu_p P_{24}(t) + \lambda_p P_{22}(t);\\
&dP_{25}(t)/dt = -\mu_p P_{25}(t) + 2\lambda_p P_{23}(t);
\end{aligned}
\qquad (4.33)
$$

– для кінцевого фрагмента Φ_{VI}

$$
\begin{aligned}
&dP_{88}(t)/dt = -6\lambda_p P_{88}(t) + \mu_p P_{89}(t) + \mu_d P_{81}(t);\\
&dP_{89}(t)/dt = -(\mu_p + 5\lambda_p)P_{89}(t) + 6\lambda_p P_{88}(t) + \mu_p P_{91}(t) + \mu_p P_{90}(t) + \mu_d P_{82}(t);\\
&dP_{90}(t)/dt = -(\mu_p + 4\lambda_p)P_{90}(t) + \mu_d P_{83}(t) + 4\lambda_p P_{89}(t) + \mu_p P_{93}(t) + \mu_p P_{92}(t);\\
&dP_{91}(t)/dt = -(4\lambda_p + \mu_p)P_{91}(t) + \lambda_p P_{89}(t) + \mu_d P_{84}(t);\\
&dP_{92}(t)/dt = -(\mu_p + 3\lambda_p)P_{92}(t) + 2\lambda_p P_{90}(t) + \mu_p P_{94}(t) + \mu_d P_{85}(t);\\
&dP_{93}(t)/dt = -(\mu_p + 3\lambda_p)P_{93}(t) + \mu_d P_{86}(t) + 4\lambda_p P_{98}(t) + 2\lambda_p P_{90}(t) + \mu_p P_{95}(t);\\
&dP_{94}(t)/dt = -(\mu_p + 2\lambda_p)P_{94}(t) + 3\lambda_p P_{92}(t) + 2\lambda_p P_{93}(t) + \mu_d P_{87}(t) + \mu_p P_{96}(t);\\
&dP_{95}(t)/dt = -\mu_p P_{95}(t) + \lambda_p P_{93}(t);\\
&dP_{96}(t)/dt = -\mu_p P_{96}(t) + 2\lambda_p P_{94}(t);
\end{aligned}
\qquad (4.34)
$$

– початкові умови:

$$P_1(0) = 1, P_i(0) = 0, i \in 2,3,...,96\ . \qquad (4.35)$$

4.4.3 Результати багатофрагментного марковського моделювання готовності ПТК побудованими за дубльованою та мажоритарною архітектурами

Аналіз результатів моделювання готовності ПТК побудованими за двохкаскадними архітектурами (рисунки 4.57, 4.58) дозволяє одержати наступні висновки. Найбільш «сприятливими» для обох архітектур є результати, отримані при значенні параметра $\lambda_d = 1\cdot10^{-5}$, 1/год і $\Delta\lambda_d = 5\cdot10^{-6}$, що відповідає першому набору параметрів у таблиці 4.4, а найменш «сприятливими» – $\lambda_d = 1\cdot10^{-5}$, 1/год і $\Delta\lambda_d = 5\cdot10^{-6}$, що безумовно є наслідком збільшення кількісного значення інтенсивності відмов ПЗ, що були спричинені проектними дефектами. Необхідно зазначити, що зі збільшенням кількісного значення для архітектури «2-з-3» та «1-з-2» збільшується також період припрацьовування, набуваючи максимального значення t = 10200 год при наборі $\lambda_d = 1\cdot10^{-5}$, 1/год і $\Delta\lambda_d = 5\cdot10^{-6}$. Для архітектури «1-з-2» та «2-з-3» практично на всьому досліджуваному часовому інтервалі функція готовності стрімко зростає при $\lambda_d = 1\cdot10^{-5}$, 1/год і $\Delta\lambda_d = 1\cdot10^{-5}$. Таке зростання є наслідком збільшення швидкості появи проектних дефектів і їх подальшого усунення.

Таблиця 4.5

Кількісні значення інтенсивностей відмов і відновлень АЗ і ПЗ досліджуваних ПТК

№ п/п	λ_d, 1/год	$\Delta\lambda_d$, 1/год	λ_p , 1/год	μ_d, 1/год	μ_p, 1/год
1	0.00001	0.000005	0.0001	0.01	1
2	0.000025	0.0000125	0.0001		
3	0.00005	0.000025	0.0001		
4	0.000075	0.0000375	0.0001		

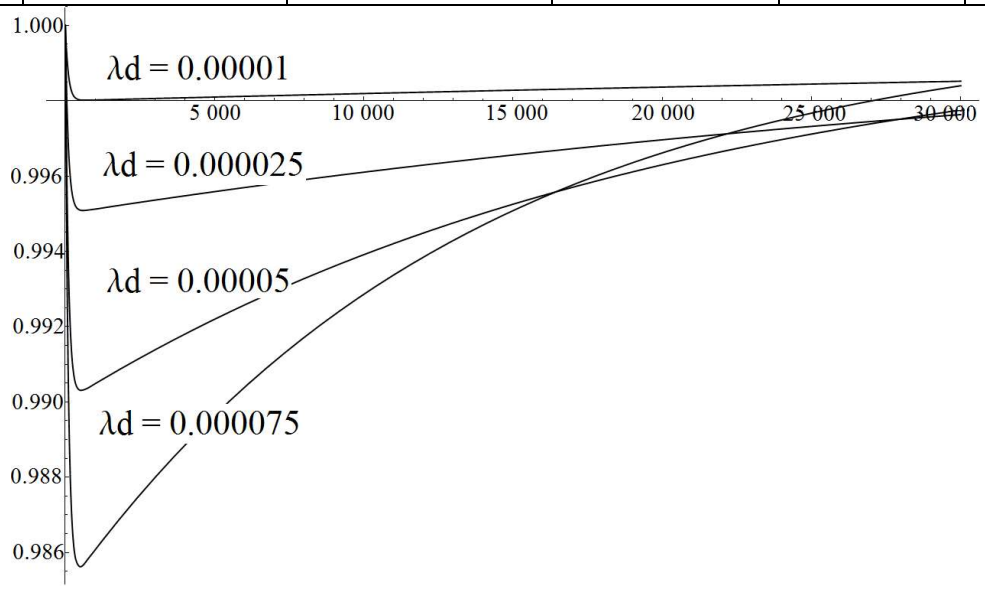


Рис. 4.57 Результати оцінювання готовності двоверсійного ПТК з двокаскадною архітектурою «2-з-3» та «1-з-2»

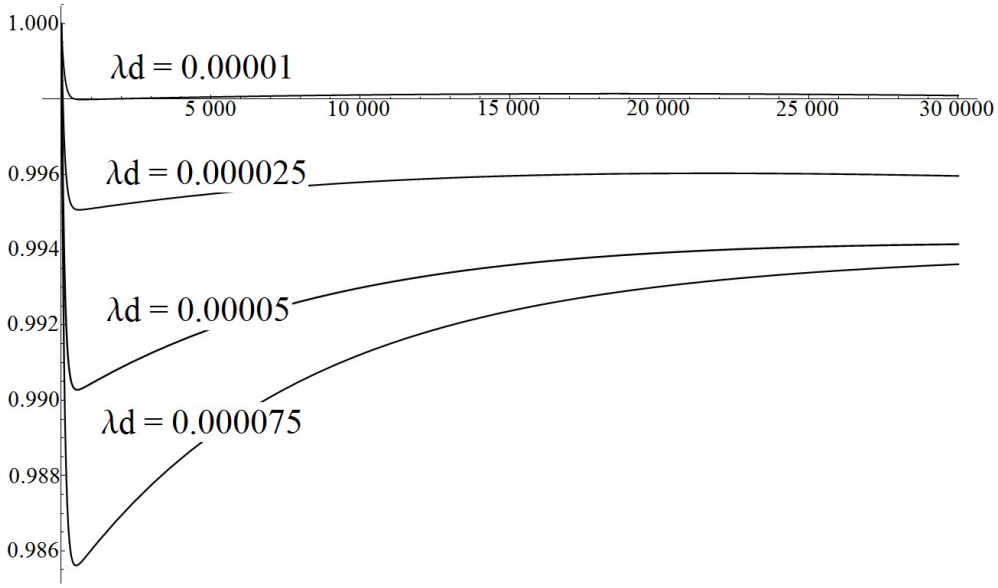


Рис. 4.58 Результати оцінювання готовності триканального ПТК з двокаскадною архітектурою «1-з-2» та «2-з-3»

Виконані дослідження базових архітектур ПТК дозволили побудувати їх пріоритетні ряди, де під цим терміном розуміється послідовність архітуктур побудована на зростаючими кількістними значенями показників надійності та функційної безпечності. Дані показники були обчислені з використанням однакових значень інтенсивностей відмов та відновлень АК та ПК. Таким чином, маємо наступні пріоритетні ряди архітектур ПТК (Рис. 4.58).

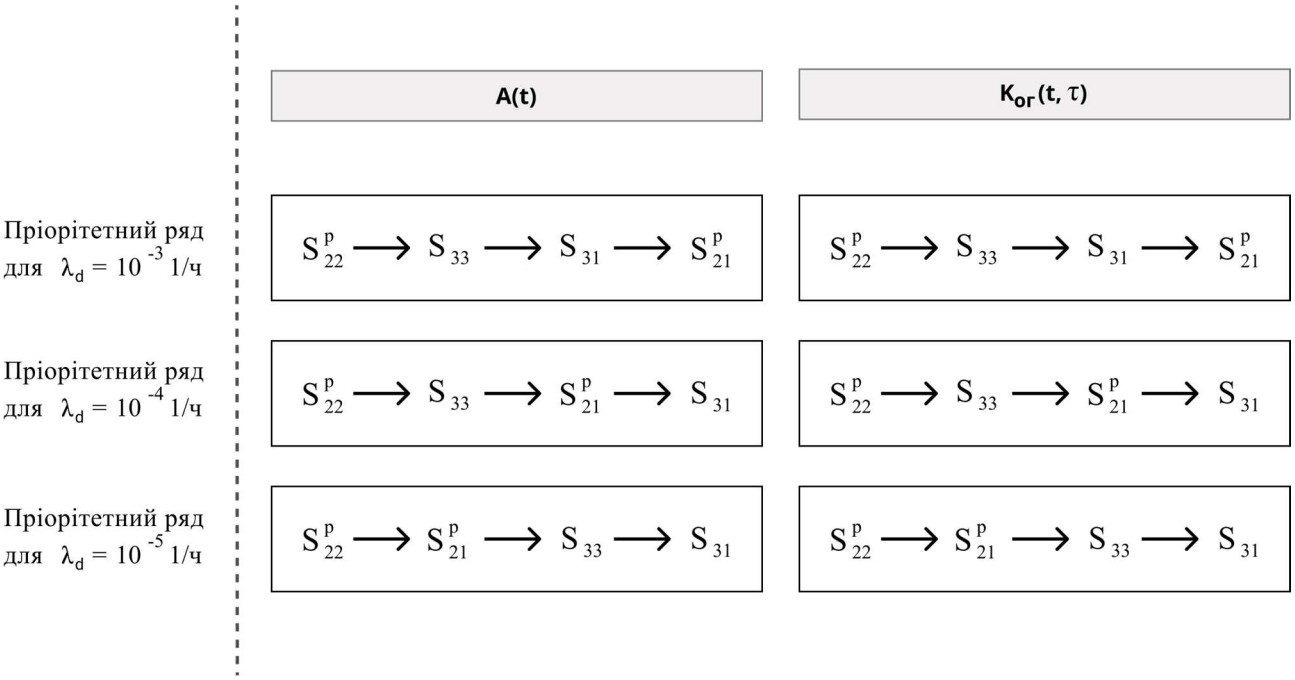


Рис. 4.58 Пріоритетні ряди базових архітектур побудови ПТК для функцій готовності і оперативної готовності обчислених для однакових значень інтенсивностей відмов ПЗ

Аналіз наведених вище пріорітетних рядів дозволяє сформулювати наступні висновки. Найкращий результат за значеннями обчислених показників в усьому діапазоні застосованого параметру демонструє дубльована двохверсіна архітектура з засобами реконфігурації. Крім того, за умови застосування різних програмних версій, достовірність виявлення дефектів для такої архітектури є високою. Далі за пріоритетом кращий результат демонструє мажоритарно резервована архітектура, хоча із зменшенням значення λ_d її випереджає дубльована одноверсійна архітектура з вбудованими засобами

реконфігурації. Таким чином, розроблений метод дозволяє виконувати комплексне оцінювання та спрямований пошук архітектури побудови ПТК з урахуванням множин обраних параметрів та варіантів зміни цих параметрів у часі.

4.5 Метод оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю

До основних етапів метода оцінювання надійності та функціональної безпеки програмно-технічних комплексів зі структурно-версійною надмірністю відносяться наступні:

Eman 1. А1 – Аналіз системи.

Початкові дані етапу наступні:

- специфікація системних вимог (опис системних функцій, опис сценаріїв функціонування, функціональні вимоги, вимоги до інтерфейсів, вимоги до продуктивності, вимоги до оточующого середовища, вимоги до інформаційної безпеки, вимоги до надійності);
- специфікація вимог до програмної компоненти (software);
- специфікація вимог до апаратної компоненти (hardware), архітектурні вимоги.

Результатами виконання етапу 1 є детальні вимоги до software та hardware й обрана для аналізу архітектура.

Eman 2. А2 – Визначення множини змінних параметрів системи ΔМЗП ∈ МЗП.

Початковими даними етапу є архітектура системи та детальний аналіз software і hardware.

Результатами виконання етапу 2 є множини змінних параметрів МЗП = {ЗІВм, ЗІВн, ЗКВн}, ΔМЗП С МЗП, де ЗІВм -змінні інтенсивності відмов ($\Delta\lambda_d$, $\Delta\lambda_{int}$), ЗІВн – змінні інтенсивності відновлень ($\Delta\mu_d$, $\Delta\mu_{int}$), ЗКВн – запас

компонент для відновлення.

Етап 3. А3 – Визначення варіанту (стратегії) зміни для змінних параметрів (∀ ЗП ∈ ΔМЗП, Δ, $\Delta_{\Delta..}$)ΔМЗП ∈ МЗП.

Початковими даними етапу є множини змінних параметрів МЗП = {ЗІВм, ЗІВн, ЗКВн}, ΔМЗП ∈ МЗП.

Результатами виконання етапу є множини змінних параметрів – МЗП = {ЗІВм, ЗІВн, ЗКВн}, ΔМЗП С МЗП, де ЗІВм -змінні інтенсивності відмов ($\Delta\lambda_{d,}$ Δ λ_{int}), ЗІВн – змінні інтенсивності відновлень ($\Delta\mu_{d,}$ $\Delta\mu_{int}$), ЗКВн – запас компонент для відновлення.

Етап 4. А4 - Вибір базової багатофрагментної моделі на основі аналізу можливої стратегії зміни параметрів ($ББМ_k$ ∈ МББМ).

Початкові дані етапу наступні:

- множини змінних параметрів МЗП = {ЗІВм, ЗІВн, ЗКВн}, ΔМЗП С МЗП;
- варіант зміни для параметрів ($\Delta\lambda_{d,}$ Δ λ_{int}, $\Delta\mu_{d,}$ $\Delta\mu_{int}$), Δ – const, Δ_{Δ} – var.

Результатами виконання етапу обрана базова баготофрагментна модель ($ББМ_k$ ∈ МББМ).

Етап 5. А5 - Визначення параметрів (кількісна оцінка всіх параметрів моделі - незмінних, змінних).

Початкові дані етапу наступні:

- множини змінних параметрів МЗП = {ЗІВм, ЗІВн, ЗКВн}, ΔМЗП С МЗП;
- варіант зміни для параметрів ($\Delta\lambda_{d,}$ Δ λ_{int}, $\Delta\mu_{d,}$ $\Delta\mu_{int}$), Δ - const, Δ_{Δ} -var.

А5 має три підетапи (А5.1, А5.2, А5.3):

- підетап А5.1 – спираючись на статистичні данні про відмови і відновлення фізичних компонент системи та систем в цілому визначаються кількісні знаяення параметрів $\lambda_{p,}$ μ_p.

- підетап А5.2 – спираючись на використання обраних моделей надійності програмних засобів та їх комплексування визначаються параметри (λ_d, $\mu_{d,}\Delta\lambda_{d,}$ $\Delta_{\Delta(d)}$.

- підетап А5.3 – визначення параметрів λ_{int}, $\mu_{int,}$ $\Delta\lambda_{int}$ за статистикою фізичної та інформаційної взаємодії системи з оточуючим середовищем

Результатами виконання етапу є кількісні значення параметрів ($\lambda_{p,}$ $\lambda_{d,}$ λ_{int}, $\mu_{p,}$ μ_{d} , $\Delta\lambda_{d,}$ $\Delta\lambda_{int}$, $\Delta\mu_{d,}$ $\Delta\mu_{int}$).

Етап 6. А6 – визначення кількості фрагментів та типи внутрішніх фрагментів.

Етап 7. А7 – побудова багатофрагментної марковської моделі, спираючись на результати попередніх етапів.

Етап 8. А8 – визначення системи диференційних рівнянь Колмогорова-Чемпена виконується обчислення показників надійності та функційної безпечності ((A(t) – функції готовності та $К_{ог}(t, \tau)$) – функції оперативної готовності).

Далі одержані значення шуканих показників порівнюються із заданими та приймається рішення про прийняття обраної архітектури ПТК для подальшої розробки, в протилежному випадку здійснюється перехід до першого етапу.

Алгоритм методу оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю наведено на рисунку 4.59.

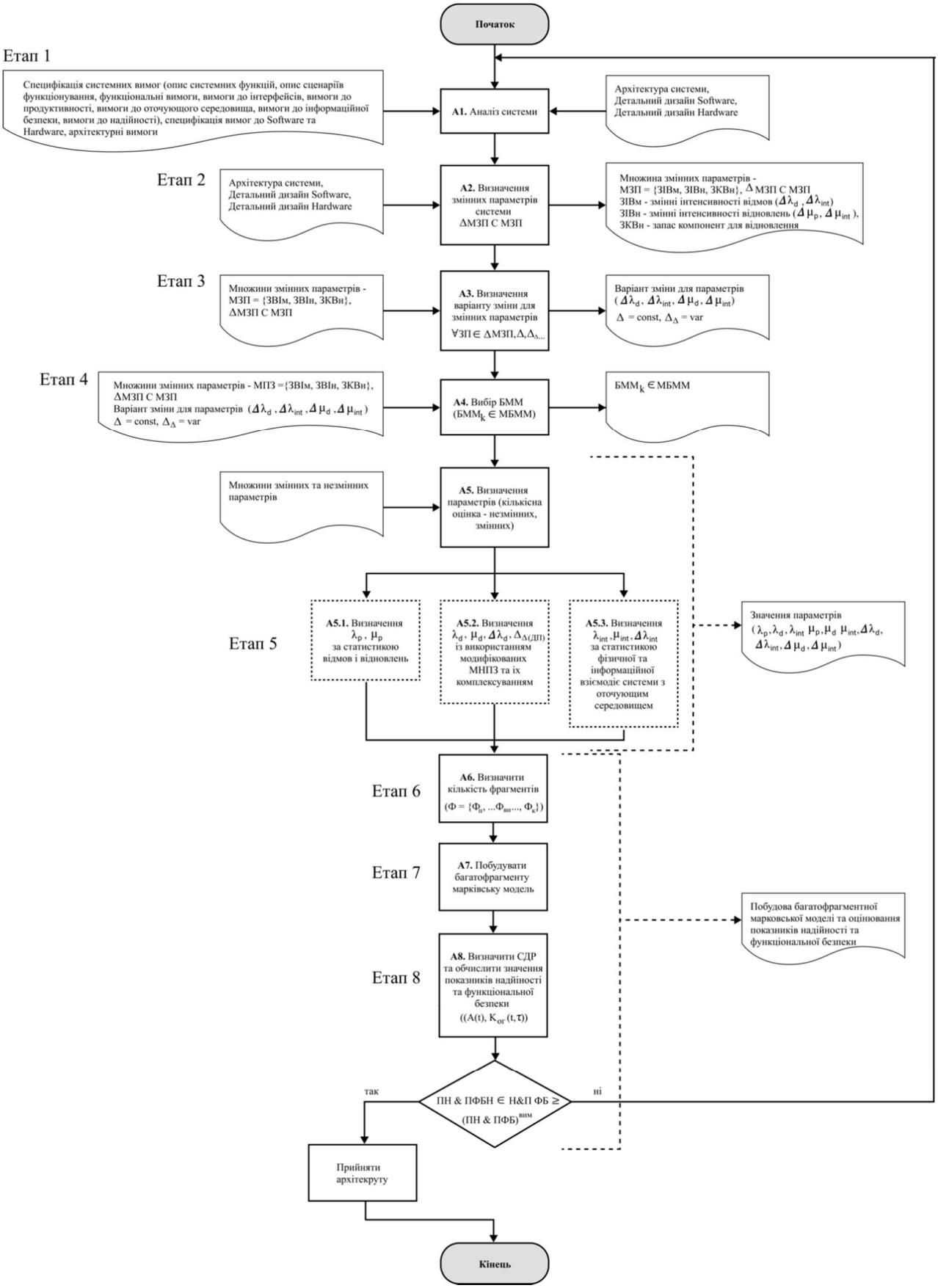


Рис. 4. 59 Алгоритм метода оцінювання надійності та функційної безпечності програмно-технічних комплексів зі структурно-версійною надмірністю

4.6 Висновки за розділом

1. В розділі 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. В основу метода покладено наступне: принципи розроблення багатофрагментних марковських моделей, які відображають основну ідею про доцільність оцінювання показників надійності і функційної безпечності із урахуванням зміни надійнісних параметрів апаратної і програмної компонент ПТК в часі; систематизація змінних параметрів; модель прояву та усунення дефектів прєктування програмних засобів та дефектів взаємодії; загальна модель прояву дефектів та вразливостей; сценарії зміни параметрів; систематизація багатофрагментних моделей. Це дозволило розробити комплекс багатофрагментних моделей оцінювання надійності і функційної безпечності ПТК для базових архітектур їх побудови.

2. Систематизація змінних параметрів дозволила окреслити їх перелік на основі аналіза множин дефектів, груп причин виникнення дефектів та визначити множини коефіцієнтів зміни параметрів і перейти до розроблення комбінації змінних і незмінних параметрів, та коєфіцієнтів їх зміни. Це дозволило одержати множину сценаріїв зміни параметрів для подальшого застосування в моделях оцінювання надійності та функційної безпечності ПТК із різними архітектурами побудови.

3. Множини сценаріїв зміни параметрів дали змогу розробити комплекс макромоделей оцінювання надійності і функційної безпечності ПТК та на їх основі комплекс багатофрагментних марковських моделей, основними первагами яких є можливість урахування змінності параметрів програмних та

апаратних компонентів у часі, що підвищило точність оцінюваннння шуканих показників до 5%.

4. Аналіз комплексу розроблених багатофрагментих марковських моделей дозволив отримати класифікацію цих моделей за основними ознаками, а саме: числа зв’язків між фрагментами моделей; характерів зв’язків між фрагментами моделей; структури фрагментів; кількості фрагментів. Це дає можливість окреслити напрямки подальшої розробки та вдосконалення багатофрагментних моделей оцінювання надійності та функційної безпечності ПТК.

5. Дослідження результатів моделювання із використанням комплексу розроблених багатофрагментих марковських моделей дозволили одержати нову інформацію про надійність і функційну безпечність існуючих і перспективних ПТК, що дозволяє особі, що приймає рішення приймати вчасні рішення щодо розробки та експлуатації систем досліджуваного класу. Прикладами такої нової інформації є наступна:

- для дубльованих архітектур ПТК найбільш «сприятливий» результат моделювання дають ББМ 1 (найбільш швидкий перехід до сталого режиму функціонування), а найменш «сприятливий» БММ 7, що пов'язано зі збільшенням часу, необхідного на усунення чергового програмного дефекту. Показник готовності, отриманий за допомогою БММ 12 має незначні нестабільні коливання протягом усього періоду дослідження. Таке явище пояснюється «випадковим» характером зміни параметрів потоків відмов і відновлень ПЗ при переході від одного фрагмента до іншого;

- функція готовності для дубльованої двохверсійної архітектури має більш «глибоку» та довшу фазу зменшення, що пояснюється збільшенням сумарної інтенсивності відмов комплексів ПЗ каналів;

- важливо виконувати багатофрагментне моделювання, яке враховує зміну параметрів у часі тому, що результати однофрагментного моделювання на ранніх етапах функціонування системи дають завищену оцінку, а після

певного «переломного» моменту часу - занижену. При цьому коливання функції готовності проходять кілька оціночних рівнів шкали готовності. Відповідно, при виборі ОФМ можливий ризик помилкового визначення часового інтервалу «стабілізування» функції готовності (кінця етапу приробітки системи), а також неправильного визначення класу готовності ПТК;

- на ранніх етапах функціонування ПТК велику роль відіграє вибір стратегії відновлення, яка впливає як на характер зміни функції готовності (зростає або зменшується), так і на кількісні результати оцінки готовності системи.

6. Основними перевагами розробленого метода є наступні:

- можливість реалізації комплексного оцінювання надійності та функційної безпечності ПТК, побудови пріорітетних рядів досліджених архітектур;

- можливість виконання спрямованого пошуку архітектури побудови ПТК з урахуванням множин обраних параметрів та варіантів зміни цих параметрів у часі та видачі обгрунтованих рекомендацій особі, що приймає рішення щодо затвердження обраної архітектури побудови ПТК.

Побудувати пріоритетні ряди побудови ПТК для функцій готовності і оперативної готовності обчислених для різних значень вінтенсивностей, що враховуються. Пріоритетні ряди допомогають ЛПР приймати обгрунтовані рішення на різних етапах життєвого циклу ПТК.

Основні положення розділу викладені у публікаціях автора [87, 127, 128, 150, 155, 156, 157, 227, 231, 232, 233, 235, 241, 242, 244, 247, 261, 278].

РОЗДІЛ 5. МОДЕЛІ ОЦІНЮВАННЯ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПТК НА САМОДІАГНОСТОВНИХ ПРОГРАМОВНИХ ПЛАТФОРМАХ З УРАХУВАННЯМ ЗАСОБІВ КОНТРОЛЮ ТА ДІАГНОСТУВАННЯ

5.1 Особливості оцінювання функційної безпечності ПТК з урахуванням контролю, та використання версійної надмірності

Реалізація ПТК функцій захисту, блокування, управління і регулювання на базі ПЛІС на сьогодні є найбільш ефективним засобом для розробки ІКС, що відповідають вимогам державних і міжнародних нормативно-технічних документів з безпеки [279]. Використання ПЛІС для ІКС дозволяє на етапі проектування спочатку закласти алгоритми самодіагностування, які будуть виконуватися окремою функціональною підсистемою контролю і діагностування (ПСКД). Сучасна самодіагностована програмовна платформа може бути описана наступною множиною:

$$SDPP = \{MPM, MFC, MD\}, \quad (5.1)$$

де MPM - множина програмовних модулів платформи, MFC - множина функцій конфігурування, MD – множина дефектів.

Приклад структури SDPP наведено на рисунку 5.1, де множина модулів платформи є наступною:

$$M = \{LM, DM, MI, MO\}, \quad (5.2)$$

де LM – логічний модуль, DM – діагностичний модуль, $MI = \{MI_1,...,MI_i,...,MI_N\}$ – множина модулів входу, $MO = \{MO_1,...,MO_i,...,MO_N\}$ - множина модулів виходу.

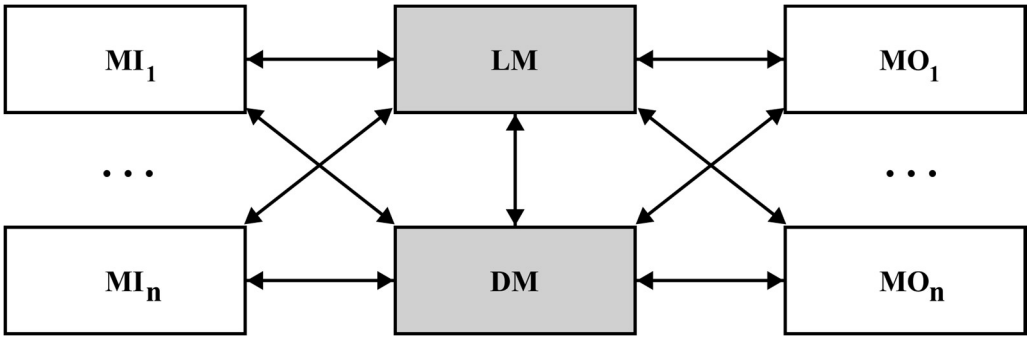


Рис. 5.1 Приклад структури SDPP

У запропонованій ПСКД самодіагностика поділяється на три види:

1. HW SD – вбудована апаратна самодіагностика, що складається з HWU SD – SD рівня вузла модуля та HWM SD – SD – рівня модуля;

2. IF SD – програмна самодіагностика для інтерфейсів передачі даних, яка включає DTP SD – SD самодіагностика для протоколів передачі даних.

3. Вбудована програмна самодіагностика для електронного проекту ПЛІС (ED SD), яка поділяється на самодіагностику даних (RAD SD), які зберігаються в ОЗП ПЛІС, самодіагностику пакетів даних (PD SD) та самодіагностику електронного проекту модуля (MED SD).

Класифікація запропонованої ПСКД SDPP наведено на рисунку 5.2.

Для урахування особливостей функціонування SDPP розроблено базову модель відмов, що базується на марковському моделюванні. В основі побудови моделі лежать наступні припущення:

- відмови розпізнаються із достовірністю D;
- достовірність D ураховує методичну складову, тобто ймовірність виявлення відмови методом, що використовується;
- приховані відмови виникають з ймовірністю (1 - D);
- при виникненні прихованих відмов система може перейти в стан розпізнаної відмови (безпечної відмови), або в стан профілактичного технічного обслуговування (ПТО);
- ПТО проводиться з періодичністю $T_{service}=1/\lambda_{service}$ та триває $T_{ПТО}$ =

$1/\mu_{ПТО}$ (рисунок 5.3).

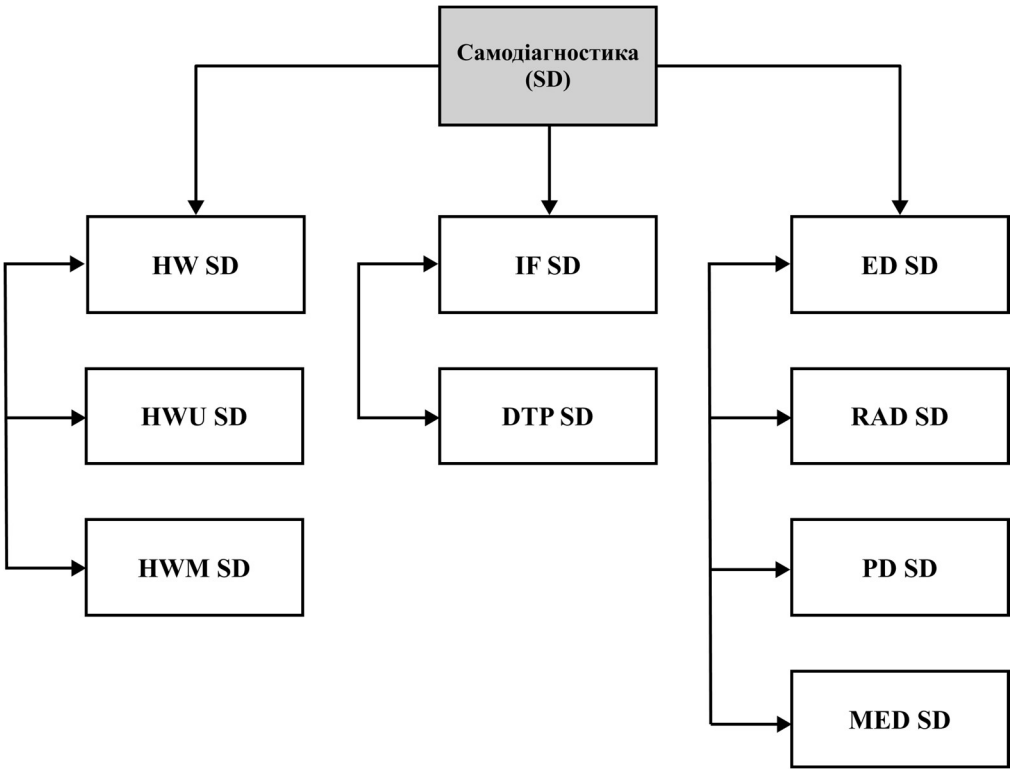


Рис. 5.2 Класифікація вбудованої підсистеми самодіагностики для перспективної SDPP

Достовірність контролю може бути розрахована як діагностичне охоплення - частина небезпечних відмов. Дана частина обчислюється як відношення інтенсивності виявлених діагностичними тестами небезпечних відмов до загальної інтенсивності небезпечних відмов.

$$DC = \frac{\sum_{i=1}^{N} \lambda_{DDi}}{\sum_{i=1}^{N} \lambda_{total_i}} \tag{5.3}$$

де: λ_{DDi} - інтенсивність детектованої небезпечної відмови *i*-го програмно-

апаратного юніта та/або модуля; λ_{totali} є сумою λ_{DDi}, λ_{DUi} – інтенсивності недетектованих небезпечних відмов *i*-го програмно-апаратного юніту модуля, λ_{SDi} - інтенсивності детектованих безпечних відмов *i*-го програмно-апаратного юніту модуля, λ_{SUi} - інтенсивності недетектованих безпечних відмов *i*-го програмно-апаратного юніту та/або модуля.

Дану модель наведено на рисунку 5.3. Модель включає наступні стани: S_0 - початковий працездатний стан, S_1 - стан відмови (безпечна відмова), S_2 - стан прихованої відмови (небезпечна відмова), S_3 - стан профілактичного технічного обслуговування, D - достовірність контроля.

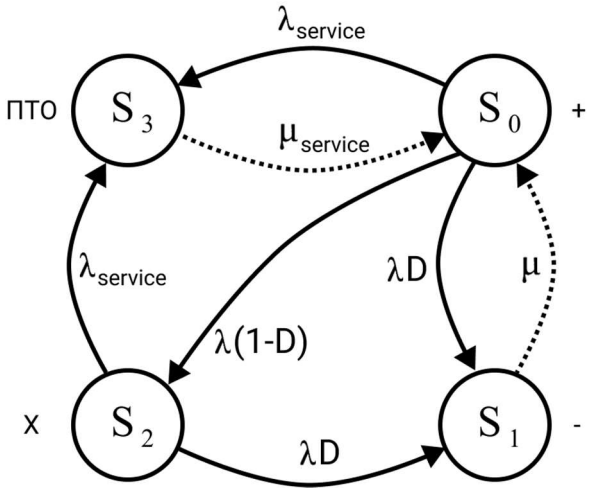


Рис. 5.3 Базова марковська модель відмов ПТК на SDPP

5.2 Розроблення та дослідження моделей надійності та функціональної безпечності з урахуванням засобів контролю та діагностування

5.2.1 Багатофрагментна марковська модель оцінювання надійності та функціональної безпеки ПТК системи нормальної експлуатації

На прикладах ПТК, які розробляються «ТОВ НВП Радій» розглянемо особливості оцінювання їх надійності та функціональної безпеки з урахуванням підсистем контролю та діагностування. Для подальшої роботи обрано

архітектуру ПТК аварійного та попереджувального захисту (АЗ – ПЗ), що входить за класифікацією по призначенню до систем нормальної експлуатації (СНЕ) та систем безпеки. СНЕ є системами призначеними для виконання нормальної експлуатації у той час як системи безпеки призначені для виконання функції безпеки [1÷3].

До складу обраного ПТК СНЕ належать:

− три ідентичних шафи формування сигналів, що утворюють три незалежних канали захисту, які резервують один одного;

− кросова вихідна шафа, що формує вихідні сигнали комплекту на основі даних отриманих від шаф формування сигналів;

− робоча станція, яка здійснює архівування, відображення і реєстрацію даних;

− автоматизоване робоче місце оператора, призначене для відображення контрольованих параметрів, станів дискретних входів і виходів, а також причин, які викликали спрацьовування захистів. Розглянута ПТК виконує мажоритарне голосування за принципом «2-out-of-3».

Структурну схему СНЕ наведено на рисунку 5.4 та стуктурна схема надійності (ССН) зображена на рисунку 5.5.

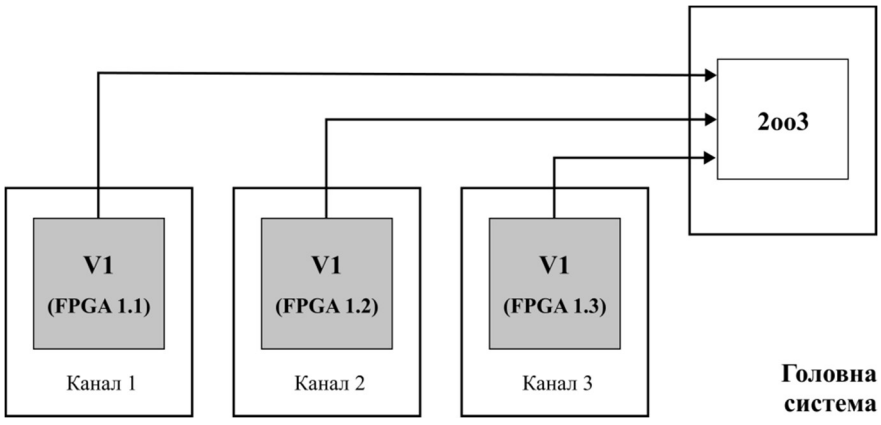


Рис. 5.4 Структура СНЕ

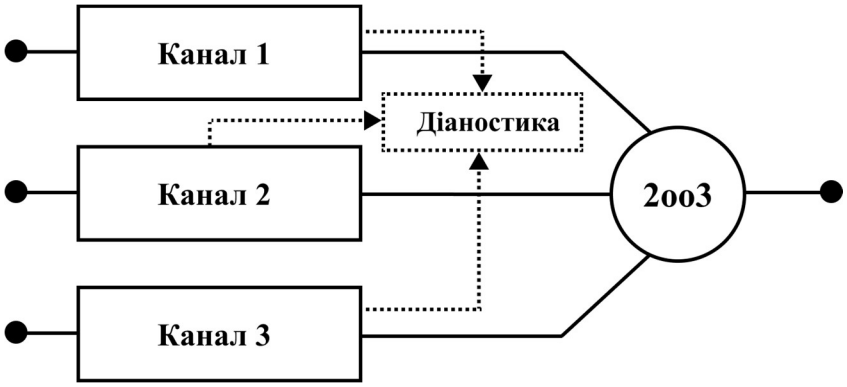


Рис. 5.5 Архітектура СНЕ

Першим етапом побудови моделей є розробка дерева відмов (ДВ), де ДВ є діаграмою, яка відображає відмови компонент системи, події або їх комбінації, що призводять до зміни стану системи.

Відповідно до результатів аналізу процесів відмов та відновлень обраної архітектури побудовано ДВ СНЕ (рисунок 5.6), що є попереднім етапом для переходу до марковського багатофрагментного моделювання. Кожна вершина ДВ відповідає конкретному стану системи. Враховуючи кількість станів й опис вузлів ДВ, визначаємо можливість переходу із одного вузла дерева до іншого. Якщо цей перехід неможливий, то дуга між вершинами відсутня, тобто відсутні перехідні ймовірності між станами системи.

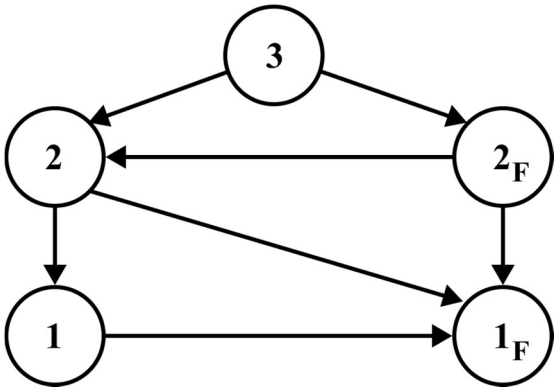


Рис. 5.6 ДВ СНЕ

Дерево відмов СНЕ (рисунок 5.6) містить наступні стани:

- *3* – справна система;

- *2* – працездатна (несправна) система, відмовив один з трьох каналів, відмова виявлена і канал відновлюється;

- *1* – непрацездатна система, відмовили два канали з трьох, відмови виявлені і канал відновлюється;

- 2_F – працездатна (несправна) система, відмовив канал, відмова не виявлена і канал не відновлюється ;

- 1_F – непрацездатна система відмовили два канали, виявлена відмова одного каналу і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється.

Для систем важливих для безпеки стани 1_F , 2_F є небезпечними.

Так як дерево відмов відображає переходи між станами системи, тому на його основі може бути створена БММ.

Перший фрагмент багатофрагментної марковської моделі відповідає за своєю структурою наведеному дереву відмов із додаванням переходів між станами, які відображають процеси відновлення компонент АЗ та ПЗ каналів.

Перехід між фрагментами моделі відбувається якщо відбуваються події відмови та відновлення програмного забезпечення.

Для побудови БММ та кількісного оцінювання шуканих показників застосовуються наступні параметри:

- $\lambda_p = 10^{-4}$ – інтенсивність відмов АЗ;

- $\lambda_d = 5 \times 10^{-5}$ – інтенсивність відмов, обумовлених проявом ДППЗ;

- $\mu_p = 1$ – інтенсивність відновлення АЗ;

- $\mu_d = 0.01$ – інтенсивність відновлення ПЗ;

- $D = 0.95$, $D = 0.99$ – показник діагностичного покриття (diagnostic coverage).

БММ СНЕ наведено рисунку 5.7, де суцільною лінією позначені переходи за умови прояву відповідного типу дефекту (апаратного або програмного), а штрихованою лінією – відновлення каналу СНЕ.

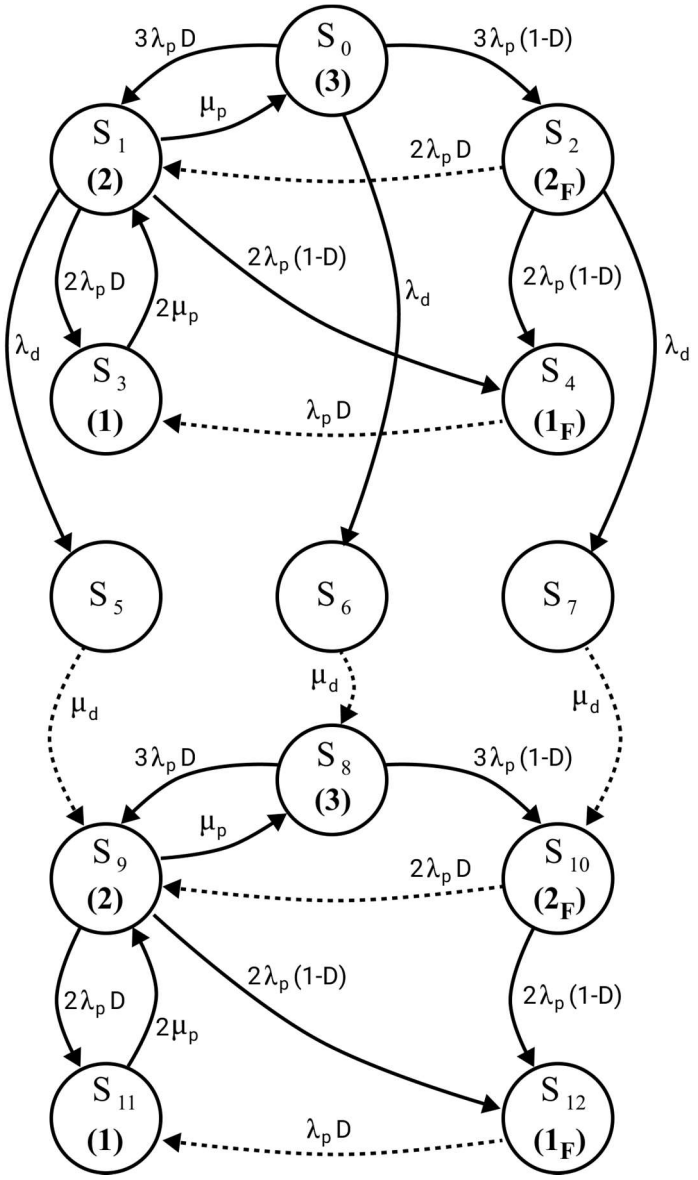


Рис. 5.7 Багатофрагментна марковська модель СНЕ (БММ СНЕ)

Вершини БММ СНЕ відповідають функціональним станам системи.

Всі стани діляться на категорії справний стан, працездатний та непрацездатний стани, а саме: стани, в яких система справна (S_0 (3), S_8 (3)); в яких система працездатна (S_1 (2), S_2 (2_F), S_9 (2), S_{10} (2_F)); стани, в яких система непрацездатна (S_3 (1), S_4 (1_F), S_5 (2), S_6 (3), S_7 (2_F), S_{11} (1), S_{12} (1_F)). Більш детальний опис станів є наступний: S_0 (3) – система справна, працюють 3 канали; S_1 (2) – система працездатна, відмовив 1 канал, відмова виявлена і канал відновлюється;S_2 (2_F) – система працездатна, відмовив 1 канал, відмова не

виявлена і канал не відновлюється; S_3 (1) – система непрацездатна, відмовили 2 канали, відмови виявлені і канал відновлюється; S_4 (1_F) – система непрацездатна, відмовили 2 канали, відмова одного каналу виявлена і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється; S_5 (2) – система непрацездатна, при виявленій відмові одного каналу відмовила програмна частина системи, відмова виявлена і програмна частина відновлюється; S_6 (3) – система непрацездатна, при роботі трьох каналів відмовила програмна частина системи, відмова виявлена і програмна частина відновлюється; S_7 (2_F) – система непрацездатна, при невиявленій відмові одного каналу відмовила програмна частина системи, відмова виявлена і програмна частина відновлюється; S_8 (3) – система справна, після відновлення програмної частини системи працюють 3 канали; S_9 (2) – система працездатна, після відновлення програмної частини відмовив 1 канал, відмова виявлена і канал відновлюється; S_{10} (2_F) – система працездатна, після відновлення програмної частини відмовив 1 канал, відмова не виявлена і канал не відновлюється; S_{11} (1) – система непрацездатна, відмовили 2 канали, відмови виявлені і канал відновлюється; S_{12} (1_F) – система непрацездатна, відмовили 2 канали, відмова одного каналу виявлена і канал відновлюється, відмова іншого каналу не виявлена і канал не відновлюється. Далі відповідно до БММ складено СДР Колмогорова.Далі відповідно до БММ складено систему диференційних рівнянь Колмогорова-Чепмена (СДР КЧ). Всі розрахунки проводяться на проміжку часу $t \in [0; 10\,000]$ з точністю $e = 10^{-6}$.

Після спрощення та зведення подібних доданків одержано СДР КЧ для БММ СНЕ:

$$
\begin{cases}
dP_0/dt = -\left(3\lambda_p D + 3\lambda_p(1-D) + \lambda_d\right)P_0(t) + \mu_p P_1(t);\\
dP_1/dt = -(\mu_p + 2\lambda_p(1-D) + 2\lambda_p D + \lambda_d)P_1(t) + 3\lambda_p D P_0(t) + 2\lambda_p D P_2(t) + 2\mu_p P_3(t);\\
dP_2/dt = -(2\lambda_p D + 2\lambda_p(1-D) + \lambda_d)P_2(t) + 3\lambda_p(1-D)P_0(t);\\
dP_3/dt = -2\mu_p P_3(t) + 2\lambda_p D P_1(t) + \lambda_p D P_4(t);\\
dP_4/dt = -\lambda_p D P_4(t) + 2\lambda_p(1-D)P_1(t) + 2\lambda_p(1-D)P_1(t) + 2\lambda_p(1-D)P_2(t);\\
dP_5/dt = -\lambda_p D P_5(t) + \lambda_d P_0(t);\\
dP_6/dt = -\mu_d P_6(t) + \lambda_d P_0(t);\\
dP_7/dt = -3\mu_d P_7(t) + \lambda_d P_2(t);\\
dP_8/dt = -(3\lambda_p(1-D) + 3\lambda_d D)P_8(t) + \mu_d P_6(t) + \mu_p P_9(t);\\
dP_9/dt = -(\mu_p + 2\lambda_p(1-D) + 2\lambda_p D)P_{10}(t) + 3\lambda_p D P_8(t) + 2\lambda_p D P_{10}(t) + 2\mu_p P_{11}(t) + \mu_d P_5(t);\\
dP_{10}/dt = -(2\lambda_p(1-D) + 2\lambda_p D)P_{10}(t) + \mu_d P + 3\lambda_p(1-D)P_8(t);\\
dP_{11}/dt = -2\mu_p P_{11}(t) + 2\lambda_p D P_9(t) + \lambda_p D P_{12}(t);\\
dP_{12}/dt = -\lambda_p D P_{12}(t) + 2\lambda_p(1-D)P_9(t) + 2\lambda_p(1-D)P_{10}(t).
\end{cases}
\tag{5.4}
$$

5.2.2 Багатофрагментнта марковська модель оцінювання надійності та функційної безпечності ПТК системи аварійного захисту

Система аварійного та попереджувального захисту має двокаскадну схему голосування, де перший каскад використовую принцип «2-out-of-3», а другий «1-out-of-2» (Рисунок 4.12). Особливістю є наявність основної та резервної підсистем, що можуть виконувати одну і ту саму функцію. Така схема є комбінацію двох підсистем із мажоритарною структурою, побудованих за принципом MooN, тобто для виконання всіх функцій безпеки повинні працювати хоча б M каналів із N. Додатково, з метою уникнути прояву однотипних дефектів ПЗ, задіяно принцип диверсності, який в даному випадку реалізовано диверсними програмними версіями у підсистемах V_1 та V_2 [151]. Дерево відмов АЗ ПЗ представлено на рисунку 5.8.

Кожна вершина дерева відмов відповідає конкретному стану АЗ ПЗ, що обумовлюється комбінацією станів двох підсистем. Підсистеми можуть

знаходитись в одному з п’яти станів, а саме:

- 3 – справна система;
- 2 – працездатна система, відмовив канал (система несправна), відмову виявлено й канал відновлюється;
- 1 – непрацездатна система, відмовило два канали, відмови виявлено й канал відновлюється;
- 2_F – працездатна система, відмовив канал (система несправна), відмову не виявлено й канал не відновлюється;
- 1_F – непрацездатна система, відмовили два канали, виявлено відмову одного каналу й канал відновлюється, відмову іншого каналу не виявлено й канал не відновлюється.

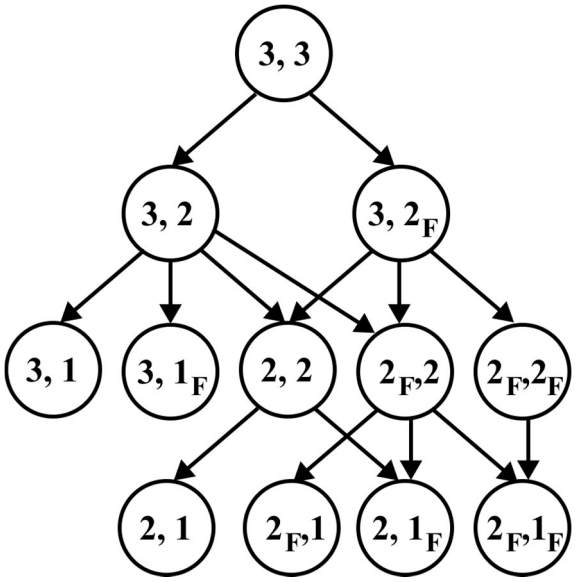


Рис. 5.8 Дерево відмов АЗ ПЗ

БММ АЗ ПЗ, яка побудована з врахуванням помилок засобів контролю і діагностування, наведено на рисунку 5.9. Вершини БММ АЗ ПЗ відповідають наступним функціональним станам:

- множина справних станів (СС) системи: $M_{cc}=\{S_0\,(3,3),\ S_{18}\,(3,3)\}$;

- множина працездатних станів (ПС) системи: $M_{пс}$={ S_0 (3,3), S_{18} (3,3), (S_1 (3,2), S_2 (3,2_F), S_4 (2,2), S_6 (2_F,2), S_7 (2_F,2_F), S_{19} (3,2), S_{20} (3,2_F), S_{22} (2,2), S_{24} (2_F,2), S_{25} (2_F,2_F)};

- множина непрацездатних станів (НС) системи: $M_{сс}$={(S_3 (3,1), S_5 (3,1_F), S_8 (2,1), S_9 (2_F,1), S_{10} (2,1_F), S_{11} (2_F,1_F), S_{12} (3,3), S_{13} (3,2), S_{14} (3,2_F), S_{15} (2,2), S_{16} (2_F,2), S_{17} (2_F,2_F), S_{21} (3,1), S_{23} (3,1_F), S_{26} (2,1), S_{27} (2_F,1), S_{28} (2,1_F), S_{29} (2_F,1_F)}.

Розглянемо всі функціональні стани АЗ ПЗ:

- S_0 (3,3) – дві резервні підсистеми в справному стані;

- S_1 (3,2) – дві резервні підсистеми працездатні (одна справна, у другій відмовив канал в результаті прояву фізичного дефекту АЗ), стан виявленої відмови та відновлення каналу;

- S_2 (3,2_F) – дві резервні підсистеми працездатні (одна справна, у другій відмовив канал в результаті прояву фізичного дефекту АЗ), стан не виявленої відмови (небезпечний стан);

- S_3 (3,1) – одна підсистема справна, відмова двох каналів, система є непрацездатною, відмови виявлено (канали відновлюються);

- S_4 (2,2) – дві підсистеми працездатні, у кожній підсистемі відмовив один канал, відмови виявлені (канали відновлюються);

- S_5 (3,1_F) – одна підсистема справна, у другій відмовили два канали та вона є непрацездатною, виявлено відмову одного каналу (канал відновлюється), відмову другого каналу не виявлено;

- S_6 (2_F,2) – дві підсистеми працездатні, у кожній підсистемі відмовило по одному каналу, але відмову виявлено тільки в одній підсистемі (канал з виявленою відмовою відновлюється);

- S_7 (2_F,2_F) – дві підсистеми працездатні, у кожній підсистемі відмовив один канал, відмови не виявлено (канали не відновлюються);

- S_8 (2,1) – одна підсистема працездатна, у другій відмовили два канали та вона є непрацездатною, всі відмови виявлено й канали відновлюються;

- S_9 (2_F,1) – одна підсистема працездатна, відмову не виявлено та канал не відновлюється, у другій відмовили два канали та підсистема э непрацездатною, відмови другої підсистеми виявлені й канали відновлюються;

- S_{10} (2,1_F) – одна підсистема працездатна, у другій відмовили два канали й підсистема є непрацездатною, одну з відмов не виявлено, у кожній підсистемі відновлюється один канал;

- S_{11} (2_F,1_F) – одна підсистема працездатна, відмовив один канал та відмову не виявлено, а отже канал не відновлюється; друга система є непрацездатною через відмову двох каналів, виявлено відмову одного за двох каналів й канал відновлюється;

- S_{12} (3,3) – система непрацездатна, прояв ДППЗ, відмову виявлено й ПЗ відновлюється, основна і резервна підсистеми справні;

- S_{13} (3,2) – система непрацездатна, прояв ДППЗ, відмову виявлено й ПЗ відновлюється, обидві підсистеми працездатні та одна із систем справна, у другій підсистемі відмовив канал, відмову виявлено;

- S_{14} (3,2_F) – система непрацездатна, прояв ДППЗ, відмову виявлено й ПЗ відновлюється, обидві підсистеми працездатні та одна із систем справна, у другій підсистемі відмовив канал, відмову не виявлено;

- S_{15} (2,2) – система непрацездатна, прояв ДППЗ, відмову виявлено й ПЗ відновлюється, обидві підсистеми працездатні, у кожній підсистемі відмовив один канал, відмови виявлено;

- S_{16} (2_F,2) – система непрацездатна, прояв ДППЗ, відмову виявлена і ПЗ відновлюється, обидві підсистеми працездатні, у кожній підсистемі відмовив один канал, але відмову виявлено тільки в одному каналі;

- S_{17} (2_F,2_F) – система непрацездатна, прояв ДППЗ, відмова виявлено й ПЗ відновлюється, обидві підсистеми працездатні, у кожній підсистемі відмовив один канал та відмови не виявлено;

- S_{18} (3,3) – ПЗ відновлено, основна й резервна підсистеми справні;

- S_{19} (3,2) – ПЗ відновлено, обидві підсистеми працездатні та у другій підсистемі відмовив канал, відмову виявлено й канал відновлюється;

- S_{20} (3,2_F) – ПЗ відновлено, обидві підсистеми працездатні, у другій підсистемі відмовив канал й відмову не виявлено, а отже канал не відновлюється;

- S_{21} (3,1) – одна підсистема справна, у другій відмовило два канали тому підсистема є непрацездатною, відмови виявлені (канали відновлюються);

- S_{22} (2,2) – ПЗ відновлена, обидві підсистеми працездатні, у кожній підсистемі відмовив один канал, відмови виявлено (канали відновлюються);

- S_{23} (3,1_F) – одна підсистема справна, у другій відмовило два канали, виявлено відмову одного каналу та канал відновлюється, відмову другого каналу не виявлена;

- S_{24} (2_F,2) – ПЗ відновлено, обидві підсистеми працездатні, у кожній підсистемі відмовив один канал, відмову виявлено тільки в одному та канал із виявленою відмовою відновлюється;

- S_{25} (2_F,2_F) – ПЗ відновлено, обидві підсистеми працездатні, у кожній підсистемі відмовив один канал, відмови не виявлено (канали не відновлюються);

- S_{26} (2,1) – одна підсистема працездатна, у другій відмовили два канали та всі відмови виявлені (канали відновлюються);

- S_{27} (2_F,1) – одна підсистема працездатна, відмову не виявлено та канал не відновлюється, у другій відмовило два канали та відмови виявлені (канали відновлюються);

- S_{28} (2,1_F) – одна підсистема працездатна, у другій відмовило два канали, а отже підсистема є непрацездатною, одну з відмов не виявлено (у кожній підсистемі відновлюється один канал);

- S_{29} (2_F,1_F) – одна підсистема працездатна, відмовив один канал, відмову не виявлено (канал не відновлюється), у другій відмовили два канали та

виявлена відмова одного каналу (канал відновлюється), відмова другого каналу невиявлена.

На основі складеної БММ ПТК АЗ ПЗ була побудована СДР КЧ, яка після спрощення має вигляд :

$$
\begin{cases}
dP_0/dt = -\left(6\lambda_p + \lambda_d\right)P_0(t) + \mu_p P_1(t);\\
dP_1/dt = 6\lambda_p DP_0(t) - \left(\mu_p + 5\lambda_p + \lambda_d\right)P_1(t) + 2\lambda_p DP_2(t) + 2\mu_p P_1(t) + 2\mu_p P_1(t);\\
dP_2/dt = 6\lambda_p(1-D)P_0(t) - \left(5\lambda_p + \lambda_d\right)P_2(t) + \mu_p P_6(t);\\
dP_3/dt = 2\lambda_p DP_1(t) - 2\mu_p P_3(t) + \lambda_p DP_5(t) + \mu_p P_8(t);\\
dP_4/dt = 3\lambda_p DP_1(t) - \left(2\mu_p + 4\lambda_p + \lambda_d\right)P_4(t) + 2\lambda_p DP_6(t) + 2\mu_p P_8(t);\\
dP_5/dt = 2\lambda_p(1-D)P_1(t) + 2\lambda_p(1-D)P_2(t) - \lambda_p DP_5(t) + \mu_p P_{10}(t);\\
dP_6/dt = 3\lambda_p(1-D)P_1(t) + 3\lambda_p DP_2(t) - \left(4\lambda_p + \mu_p + \lambda_d\right)P_6(t) + 4\lambda_p DP_7(t) + 2\mu_p P_9(t);\\
dP_7/dt = 3\lambda_p(1-D)P_2(t) - \left(4\lambda_p + \lambda_d\right)P_7(t);\\
dP_8/dt = 4\lambda_p DP_1(t) - 3\mu_p P_8(t) + 2\lambda_p DP_9(t) + \lambda_p DP_{10}(t);\\
dP_9/dt = 2\lambda_p DP_6(t) - 2\left(\lambda_p D + \mu_p\right)P_9(t) + \lambda_p DP_{11}(t);\\
dP_{10}/dt = 4\lambda_p(1-D)P_4(t) + 2\lambda_p(1-D)P_6(t) - \left(\lambda_p D + \mu_p\right)P_{10}(t) + 2\lambda_p DP_{11}(t);\\
dP_{11}/dt = 2\lambda_p(1-D)P_6(t) + 4\lambda_p(1-D)P_7(t) - 3\lambda_p DP_{11}(t);\\
dP_{12}/dt = \lambda_d P_0(t) - \mu_d P_{12}(t);\\
dP_{13}/dt = \lambda_d P_1(t) - \mu_d P_{13}(t);\\
dP_{14}/dt = \lambda_d P_2(t) - \mu_d P_{14}(t);\\
dP_{15}/dt = \lambda_d P_4(t) - \mu_d P_{15}(t);\\
dP_{16}/dt = \lambda_d P_6(t) - \mu_d P_{16}(t);\\
dP_{17}/dt = \lambda_d P_7(t) - \mu_d P_{17}(t);\\
dP_{18}/dt = \mu_d\ P_{12}(t) - 6\lambda_p P_{18}(t) + \mu_p P_{19}(t);\\
dP_{19}/dt = \mu_d P_{13}(t) + 6\lambda_p DP_{18}(t) - \left(\mu_p + 5\lambda_p\right)P_{19}(t) + 2\lambda_p DP_{20}(t) + 2\mu_p P_{21}(t) + 2\mu_p P_{22}(t);\\
dP_{20}/dt = \mu_d P_{14}(t) + 6\lambda_p(1-D)P_{18}(t) - 5\lambda_p P_{20}(t) + \mu_p P_9(t);\\
dP_{21}/dt = 2\lambda_p DP_{19}(t) - 2\mu_p P_{21}(t) + \lambda_p DP_{23}(t) + \mu_p P_{26}(t);\\
dP_{22}/dt = \mu_d P_{15}(t) + 3\lambda_p DP_{19}(t) - \left(2\mu_p + 4\lambda_p\right)P_{22}(t) + 2\lambda_p DP_{24}(t) + 2\mu_p P_{26}(t);\\
dP_{23}/dt = 2\lambda_p(1-D)P_{19}(t) + 2\lambda_p(1-D)P_{20}(t) - \lambda_p DP_{23}(t) + \mu_p P_{28}(t);\\
dP_{24}/dt = \mu_d P_{16}(t) + 3\lambda_p(1-D)P_{19}(t) + 3\lambda_p DP_{20}(t) - \left(4\lambda_p + \mu_p\right)P_{24}(t) + 4\lambda_p DP_{25}(t) + 2\mu_p P_{27}(t\\
dP_{25}/dt = \mu_d P_{17}(t) + 3\lambda_p(1-D)P_{20}(t) - 4\lambda_p P_{25}(t);\\
dP_{26}/dt = 4\lambda_p DP_{22}(t) - 3\mu_p P_{26}(t) + 2\lambda_p DP_{27}(t) + \lambda_p DP_{28}(t);\\
dP_{27}/dt = 2\lambda_p DP_{24}(t) - \left(2\lambda_p D + 2\mu_p\right)P_{27}(t) + \lambda_p DP_{29}(t);\\
dP_{28}/dt = 4\lambda_p(1-D)P_{22}(t) + 2\lambda_p(1-D)P_{24}(t) - \left(\lambda_p D + \mu_p\right)P_{28}(t) + 2\lambda_p DP_{29}(t);\\
dP_{29}/dt = 2\lambda_p(1-D)P_{24}(t) + 4\lambda_p(1-D)P_{25}(t) - 3\lambda_p DP_{29}(t).
\end{cases}
\tag{5.5}
$$

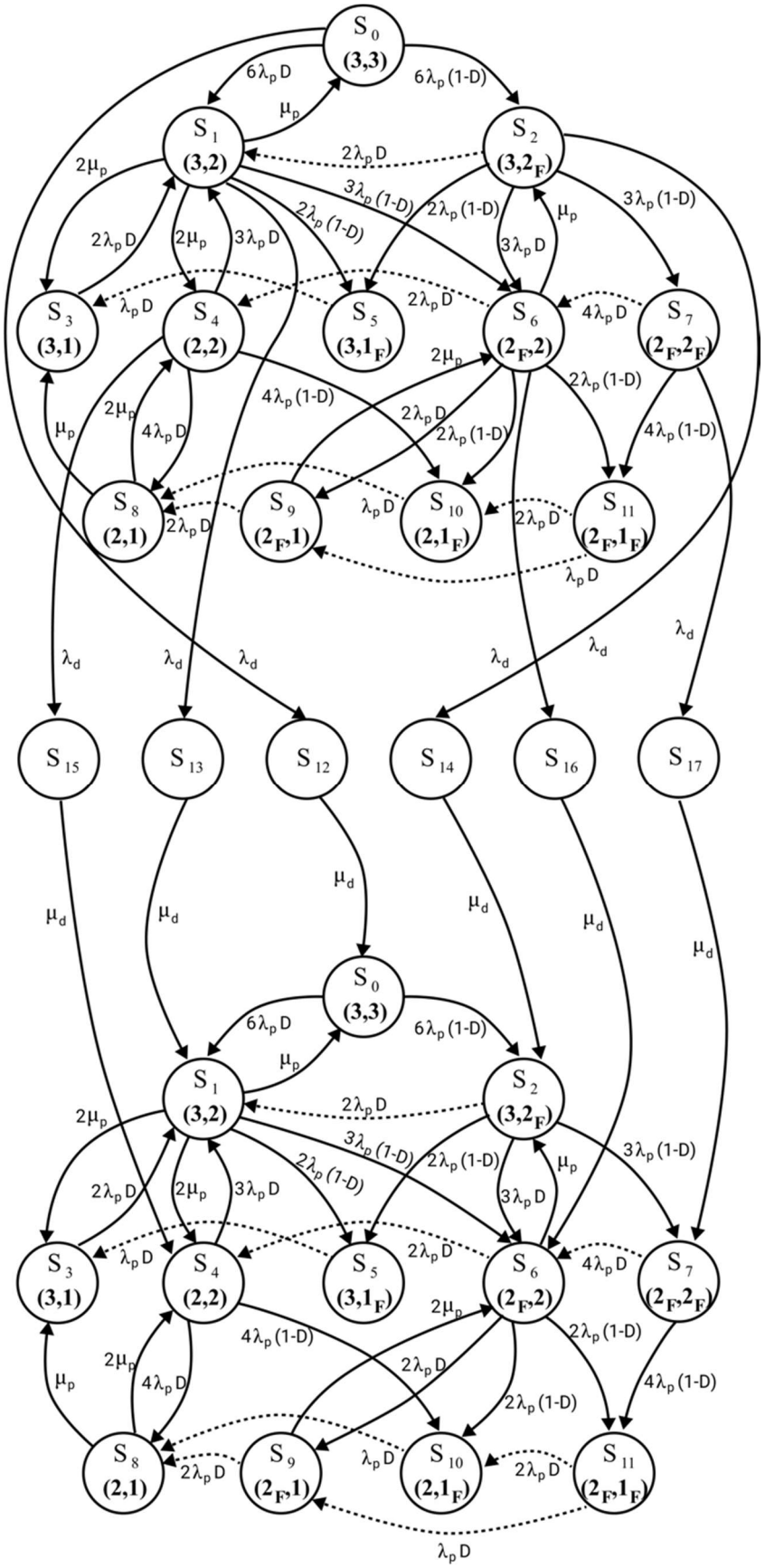


Рис. 5.9 Багатофрагментна марковська модель АЗ ПЗ

5.3 Результати моделювання ПТК СНЕ та АЗ ПЗ

Розв’язок СДР Колмогорова-Чепмена було проведено за допомогою методу Рунге-Кутта вбудованому в інструментальні засоби MATLAB та MATHEMATICA. Для обчислення функції готовності СНЕ також було застосовано інструмент EXPMETH.EXE, що реалізує модифікований експоненційний метод [155] розв’язання лінійних СДР Колмогорова-Чепмена, які мають набір властивостей, описаних у роботі [259].

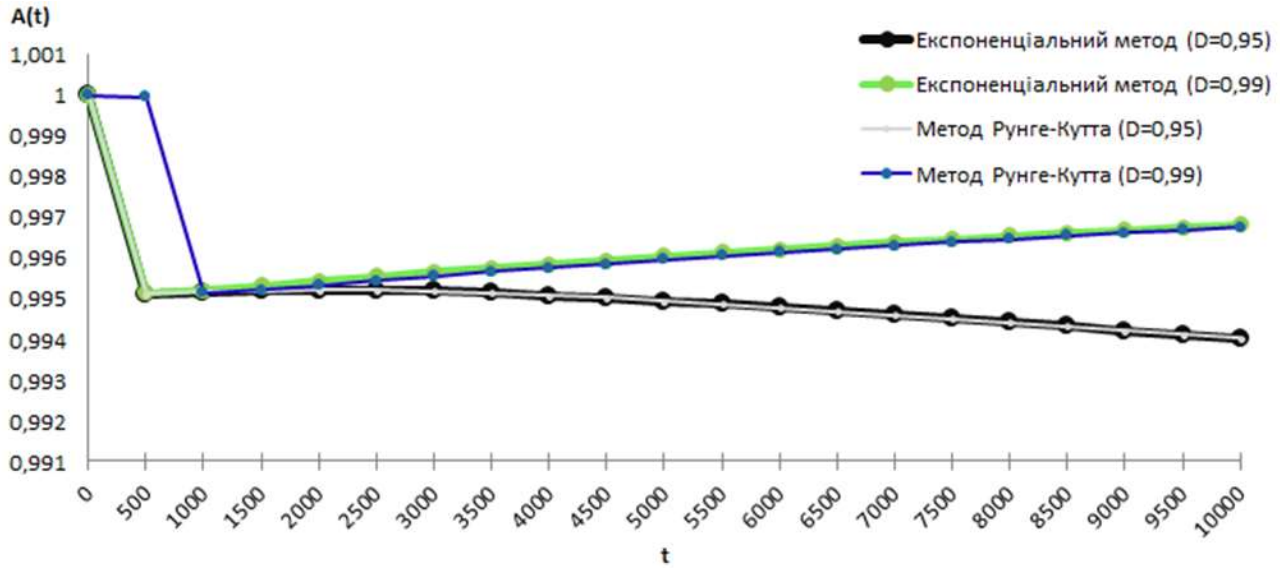


Рис. 5.10 Функція готовності СНЕ для значень параметра (D=0,95, D=0,99)

На початковому інтервалі функціонування системи $t \in [0; 500)$ спостерігається різкий спад показника й далі його повільне зростання. Через неадаптивне обрання інтервалу інтегрування метод Рунге-Кутта, при значенні параметра D = 0,99 дає спад в інтервалі [500;1000], завдяки чому видно значний вплив параметру D на результуючу функцію готовності. Тобто, для забезпечення необхідного рівня надійності й функціональної готовності вкрай важливим є застосування в ході розробки систем таких методів, технологій і технік проектування, які забезпечать максимальне тестове діагностування (самодіагностування), як апаратної так і програмної компонент ПТК.

Таблиця 5.1

Різниця значень функції готовності СНЕ для експоненційного методу та методу Рунге-Кутта 4-го порядку

	Методи, що порівнюються	
Показники порівняння	***1 & 2 D=0,95***	***1 & 2 D=0,99***
Мінімальне значення різниці	0,00	0,00
Максимальне значення різниці	1,00E-06	4,82E-03

Найбільша розбіжніть в результатах обчислень спостерігається при значенні параметру D = 0,99. Обчислені значення функції готовності для ПТК АЗ ПЗ наведені на рисунках 5.10 – 5.11 та таблицях 5.2 – 5.3 для значень D = 0,95 й D = 0,99 відповідно.

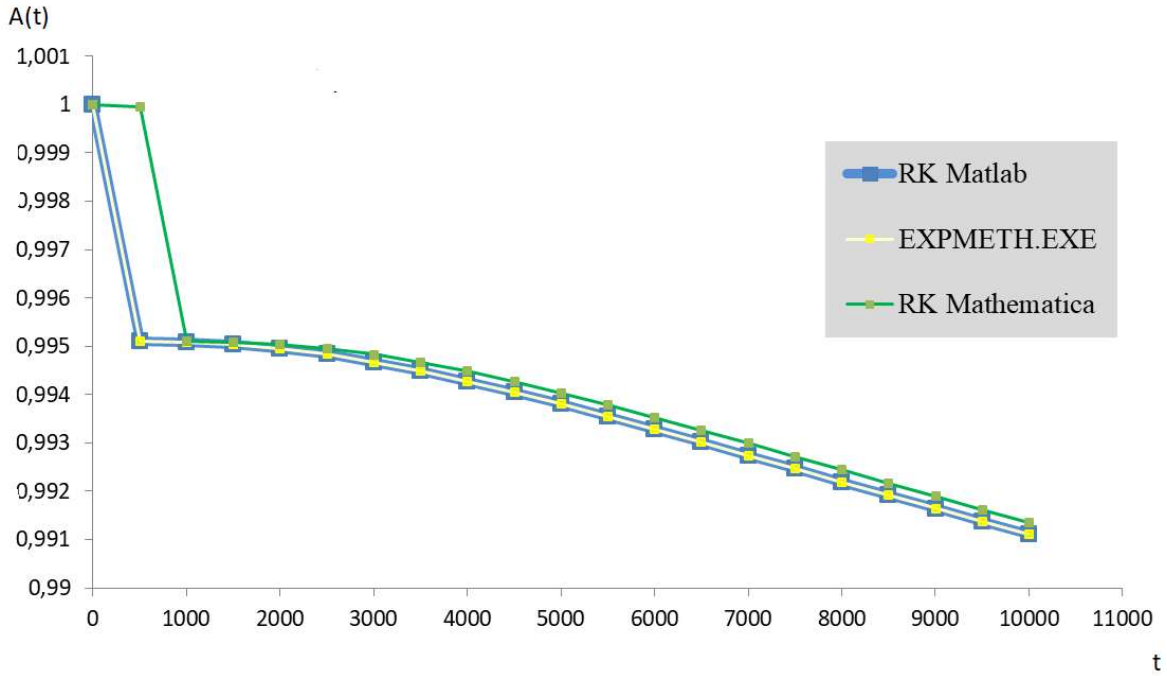


Рис. 5.11 Функція готовності АЗ ПЗ для значень параметру D = 0,95

Характер одержаних залежностей є подібним до попередніх досліджень СНЕ. Спостерігаються розбіжності у кількісних значеннях показників, що пояснюється різними застосованими методами обчислень та безпосередньо їх особливостями, а саме вибором інтервалу інтегрування, глибиною розкладу у ряд, точністю тощо. Всі залежності показують різкий спад на початковому інтервалі $t \in [0; 1000)$, але найбільш важливий висновок щодо архітектури ПТК

та методів їх розроблення дає вплив параметра D. Отже, базовим завданням розробників є його збільшення всіма доступними методами.

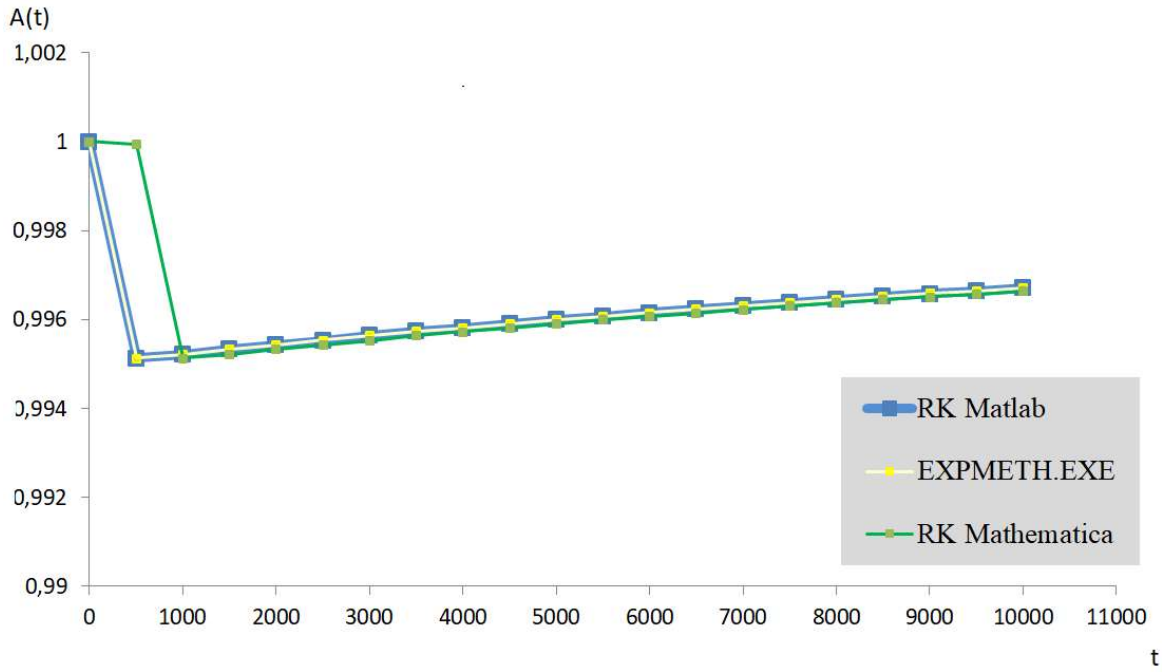


Рис. 5.11 Функція готовності АЗ ПЗ для значень параметру D = 0,99

Таблиця 5.2

Різниця значень функції готовності ПТК АЗ ПЗ для $D_1 = 0,95$

	1. Метод Рунге-Кутта MATLAB	2. Експоненціальний метод EXPMETH.EXE	3. Метод Рунге-Кутта MATHEMATICA
	1. & 2.	1. & 3.	2. & 3.
Мінімальна різниця	4,70E-09	1,30E-05	1,30E-05
Максимальна різниця	1,63E-06	4,85E-03	4,86E-03

Таблиця 5.3

Різниця значень функції готовності ПТК АЗ ПЗ для $D_1 = 0,99$

	1. Метод Рунге-Кутта MATLAB	2. Експоненціальний метод EXPMETH.EXE	3. Метод Рунге-Кутта MATHEMATICA
	1. & 2.	1. & 3.	2. & 3.
Мінімальна різниця	1,17E-08	7,00E-05	7,10E-05
Максимальна різниця	1,74E-06	4,82E-03	4,82E-03

5.4 Метод забезпечення функційної безпечності ПТК на самодіагностовних програмованих платформах шляхом використання різних варіантів диверсності

До основних етапів методу забезпечення функційної безпечності ПТК на самодіагностовних програмованих платформах шляхом використання різних варіантів диверсності, алгоритм якого зображено на рисунку 5.10, відносяться наступні:

Eman 1. А1 – Аналіз системи.

Необхідно відзначити, що перед застосуванням описаного методу необхідно можливо використати метод оцінювання НіФБ ПТК зі структурно-версійною надмірністю для випадку, коли проєктуємий ПТК має програмно-апаратну надмірність.

Початкові дані етапу наступні:

- специфікація системних вимог, що має включати опис системних функцій та опис сценаріїв функціонування, функціональні вимоги до системи, а також вимоги до інтерфейсів, продуктивності, оточуючого середовища, інформаційної безпеки та надійності;

- специфікація вимог до програмного забезпечення (software), специфікація вимог до апаратного забезпечення (hardware), а також архітектурні вимоги.

Результатами виконання етапу є рекомендації щодо структурної (архітектурної) побудови ПТК.

Eman 2. А2 – визначення рівня достовірності контроля та діагностики. На даному етапі необхідно визначити архітектурну, безпекову та технологічну концепцію, яка дозволить досягти рівня надійності й функціональної безпеки, яка вимагається від системи, що розробляється.

Результатами виконання етапу є визначене кількісне значення рівня достовірності контроля та діагностування, опис концепції побудови майбутньої

системи за різними складовими (архітектурною, безпековою, технологічною із визначенням ієрархії підсистем програмно-апаратної самодіагностики) та набір рекомендацій щодо програмно-апаратних технологій, які можливо застосувати.

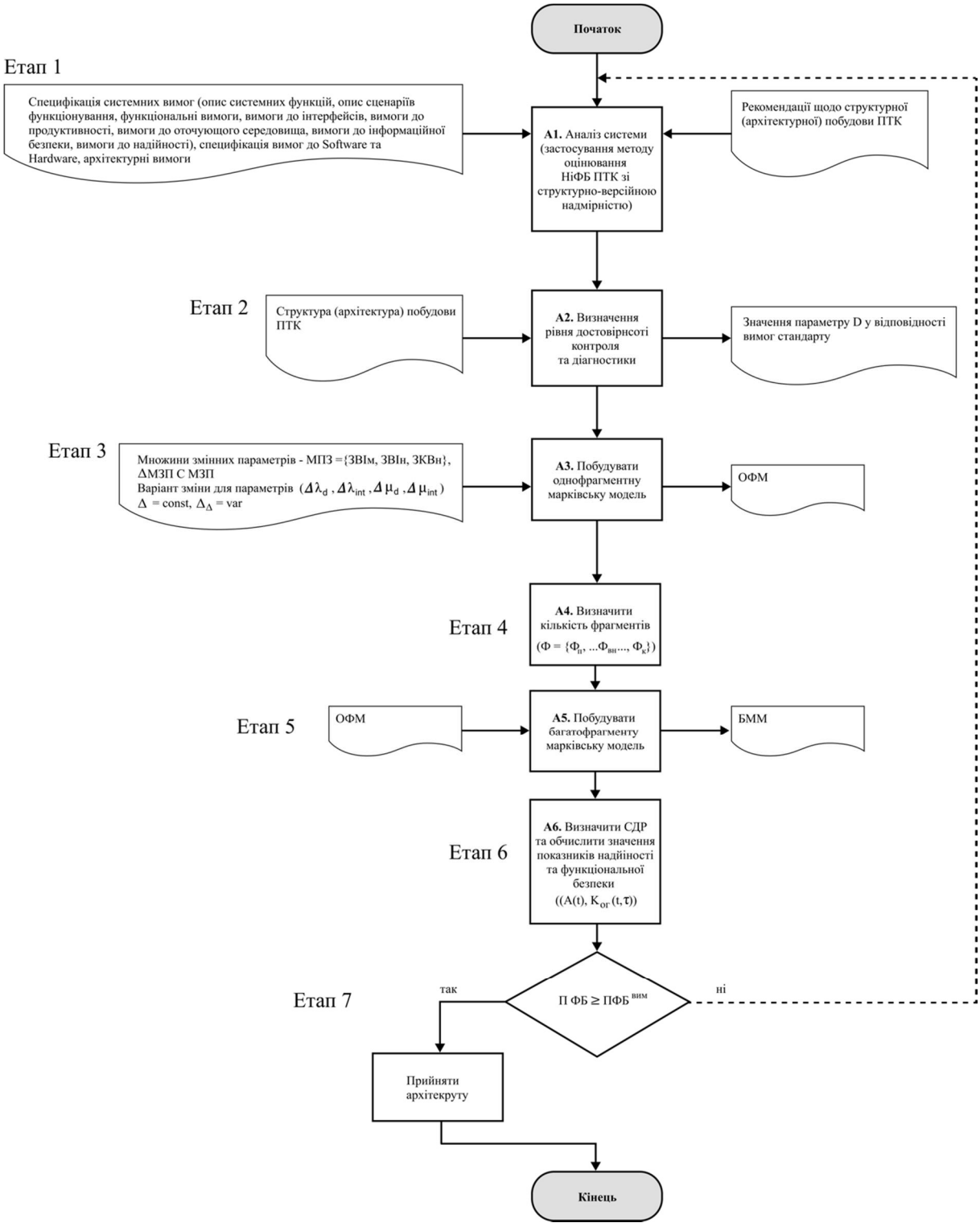


Рис. 5.12 Алгоритм методу забезпечення функціональної безпеки ПТК на самодіагностовних програмованих платформах шляхом використання різних варіантів диверсності

Етап 3. А3 – Уточнення множини змінних параметрів системи ΔМЗП ∈ МЗП та розроблення базової моделі відмов, яка враховує особливості функціонування запропонованої на етапі розроблення системних вимог підсистеми контролю і діагностування.

Результатами виконання етапу є побудова дерева відмов, а саме базової марковської моделі відмов ПТК на SDPP, яка за суттю є однофрагментною марковською моделлю, яка на наступному етапі стане основою розроблення багатофрагментної марковської моделі.

Етап 4. А4 – визначення кількості фрагментів у майбутній багатофрагментній моделі на основі аналіза множини визначених змінних параметрів та обраного варіанту зміни цих параметрів, а саме сценарію зміни параметрів в ході моделювання.

Результатом виконання етапу є: макрограф, який складається з набору фрагментів та визначених за’язків між ними.

Етап 5. А5 – побудова багатофрагментного марковського графу.

Результатом виконання етапу є багатофрагмента маркоувська модель, яка моделює функціонування ПТК з урахуванням: структури системи (склад програмно-апаратних компонент); процеси відмов і відновлень програмних і апаратних компонент; переходи в стани з урахуванням рівня діагностичного покриття засобами підсистем контроля і діагностування; стани прихованих відмов (небезпечних відмов).

Етап 6. А6 – обрання інструментального засобу чисельного інтегрування та обчислення значень показників (функції готовності (A(t)) та оперативної готовності ($К_{ог}(t, \tau)$).

Результатом виконання етапу є обчислені (прогнозовані) значення показхників, що визначають надійність і функційну безпеченість ПТК.

Етап 7. А7 – порівняння значень одержаних показників з тими, які вимагаються та подальше прийняття рішення щодо застосування й детальної розробки ПТК за обраною й оціненою архітектурою.

5.5 Висновки за розділом

1. В розділі 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. Дані моделі відображають переваги технології ПЛІС, які за результатами аналіза є найбільш ефективними для реалізації програмно-технічними комплексами функцій захисту, блокування, управління й регулювання, що відповідають вимогам державних і міжнародних нормативно-технічних документів з безпеки. Практика довела переваги використання технології ПЛІС, які заключаються в тому, що вона ще на етапі проєктування системи дозволяє закладати алгоритми самодіагностування, які далі будуть виконуватись окремими підсистемами контролю та діагностування, як апаратної так і програмної компонент. Дане твердження доведено результатами класифікації підсистем контролю й діагностування перспективної самодіагностовної програмованої платформи RadICS побудованої із використанням технології ПЛІС. Для урахування глибини контроля і діагностування введено показник діагностичного охоплення, який в свою чергу враховує різні види інтенсивностей відмов, а саме: інтенсивності детектованої небезпечної відмови; інтенсивності недетектованої небезпечної відмови; інтенсивності детектованої безпечної відмови; інтенсивності недетектованої безпечної відмови. Відповідно до видів інтенсивностей відмов модель включає відповідні функційні стани і особливо важливим є те, що модель враховує стан недектованої небезпечної відмови, що підвищує точність оцінювання (прогнозування) надійності та функційної безпечності системи.

2. Розроблені багатофрагментні марковські моделі оцінювання надійності та функційної безпечності ПТК системи нормальної експлуатації (СНЕ) та аварійного і попереджувального захисту (АЗ ПЗ) з урахуванням

помилок засобів контролю та діагностування дозволили дослідити зміну показників у часі за умови зміни у часі множини надійнісних параметрів їх програмних та апаратних компонент системи. Дослідження моделей дозволило відстежити характер зміни функції готовності кожного ПТК з урахуванням набору значень параметру діагностичного охоплення. Встановлено, що забезпечення максимального значення цього параметру є вкрай вагомим для систем важливих для безпеки і має бути забезпечено на ранніх етапах проєктування системи шляхом розробки й впровадження спеціальних організаційних та технічних заходів. До даних заходів можуть бути віднесені розробка концепції безпеки системи та її архітектурної побудови, а саме розробка структури підсистем контролю та діагностування.

3. Застосування розробленого метода забезпечення функційної безпечності програмно-технічних комплексів на програмованих платформах шляхом використання різних варіантів версійної надмірності (диверсності) дозволяє зменшує ризики відмов за загальною причиною за умови того, що оцінці підлягають диверсні архітектури ПТК (архітектури, в яких використовується поканально більше однії програмної версії). Основними перевагами метода є наступні:

- з урахуванням інформації що викладена в специфікаціях: системних вимог (опису системних функцій та сценаріїв функціонування, вимог до інтерфейсів, продуктивності системи, оточуючого середовища, інформаційної безпеки та надійності); вимог до програмних (software) та апаратних (hardware) засобів можливо сформулювати рекомендації щодо структурної (архітектурної) побудови ПТК;

- в умовах необхідного (за вимогами технічного завдання) рівня контроля й діагностування до підсистем самодіагностування АК та ПК, враховучі визначену та уточнену множину змінних параметрів системи, можливо побудувати моделі відмов, перейти до багатофрагментного моделювання та отримати більш точні оцінки показників надійності і функційної безпечності.

точність оцінок зростає до 5%;

- метод надає можливість обгрунтовано сформулювати рекомендації щодо архітектури побудови диверсних ПТК, які будуються на самодіагностовних програмовних платформах.

Основні положення розділу викладені у публікаціях автора [80, 87, 170, 259, 277, 260, 261, 269].

РОЗДІЛ 6. МЕТОДИ ВЕРИФІКАЦІЇ, ОЦІНЮВАННЯ ТА ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ І ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ПРИ РОЗРОБЛЕННІ ТА ЛІЦЕНЗУВАННІ ПРОГРАМОВНИХ МОДУЛІВ І ПЛАТФОРМ ДЛЯ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ. ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ

6.1 Метод верифікації та валідації ПТК на програмовних платформах

6.1.1 Модифікована процедура FMEDA

Процесу вводу в експлуатацію ПТК, для систем важливих для безпеки, згідно вимог державних і міжнародних стандартів передують процеси сертифікації та ліцензування ПТК та їх складових (наприклад самодіагностовних програмовних платформ). В основу реалізації процесів сертифікації та ліцензування покладену моделі життєвого циклу ПТК та їх складових. Прикладом такої моделі є V-модель, яка описана у частині 2 стандарта IEC 61508 для розроблення і тестування систем, в обчислювальне ядро який побудовано на схемах ASIC (Application-specific integrated circuit, «інтегральна схема для специфічного застосування»), рисунок 6.1.

Прикладом таких систем є ПЛК, що розробляються на базі технології FPGA (для критично важливих систем безпеки I&C - FPGA PLC-based safety critical I&C systems (FPICS)), що спричинено декількома перевагами FPICS у порівнянні з системами на основі SW, реалізованими за допомогою мікропроцесорів та мікроконтролерів. з універсальною та нерухомою архітектурою.

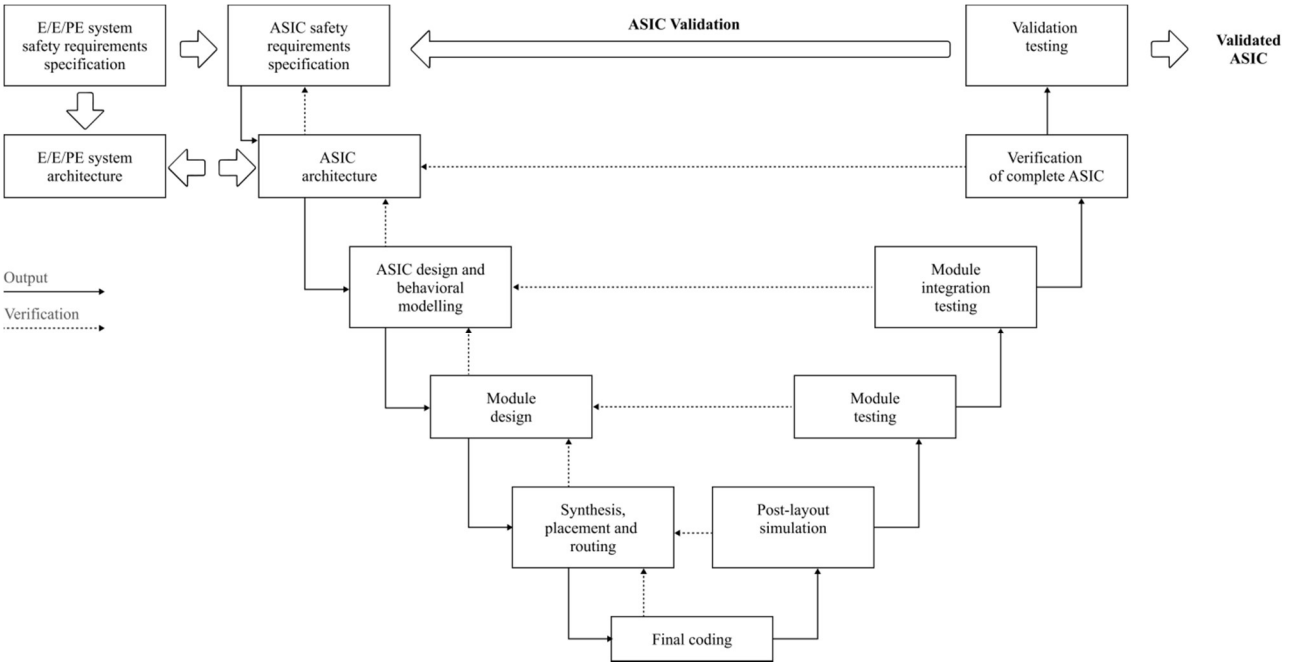


Рис. 6.1 ASIC життєвий цикл (V-Model) IEC 61508 parth 2

Ліва гілка моделі описує послідовність та перелік робот (активностей) розроблення системи, права послідовність та перелік активностей верифікації та валідації. За визначенням міжнародного стандарту IEEE 1012 Standard for software verification and validation [21] *верифікація* - це процес, в ході якого повинні бути отримані об'єктивні докази відповідності розроблюваних продуктів і процесів їх розробки: набору характеристик вимог до системи (необхідності, однозначності, здійсненності, послідовності, коректності, повноти, точності, безпечності, перевіряємості, простежуємості на всіх етапах життєвого циклу (розробки, тестування, приймання, експлуатації та обслуговування); відповідності стандартам, практикам і угодам протягом всього життєвого циклу; успішного завершення всіх робіт (активностей) кожного етапу життєвого циклу і готовності перейти до наступного.

Відповідно *валідація* - це процес, в ході якого повинні бути отримані об'єктивні докази відповідності розроблюваних продуктів і процесів їх розробки: встановленим вимогам на всіх етапах життєвого циклу; вірності підходів (фізичного моделювання розроблювальних систем, що впроваджуються і застосування процесів менеджменту та інш.); здібностей продукту відповідати вимогам споживача.

Авторське визначення цих процесів, яке доповнює попередні наступне. *Верифікація та валідація* - це взаємопов'язані і взаємодоповнюючі процеси, які використовують загальні результати для більш глибокого аналізу відповідності продукту встановленій множині вимог шляхом реалізації різноманітних методів тестування (оглядів проєктної документації, тестування ПЗ (огляд коду програм, статичний аналіз програмного коду, фунційний аналіз ПЗ тощо), тестування з внесенням дефектів в АЗ та ПЗ, інтеграційного тестування, валідаційного тестування та інш.).

Застосування технології FPGA забезпечує більш високу надійність, безпеку та найкращу гнучкість та ремонтопридатність. З іншого боку, застосування FPGA може спричинити конкретні ризики, які повинні бути знижені до прийнятного рівня. FPICS AEC повинні відповідати вимогам стандартів, що стосуються верифікації та валідації (V&V).

Існуючі методи V&V для FPICS базуються на аналізі (англ. Review-огляді) документації, статичному аналізі програмного коду та функціональному тестуванні, інтеграційному та валідаційному етапах тестування та інших [218]. Відповідно до вимог міжнародних стандартів загальний перелік та об’єм робот верифікації та валідації залежить від класу безпечності системи, яка розробляється.

Однією з сучасних та обов'язкових методик, що застосовуються в процесі сертифікації сучасних ПЛК на відповідність вимогам IEC 61508 відповідно до рівня цілісності безпеки (функційної безпечності) (SIL, Safety Integrity Level), є виконання тестування АК і ПК з внесенням дефектів (HW&SW FIT – Hardware and Software Fault Insertion Testing). Вихідні дані для HW&SW FIT готує метод аналізу режимів, ефектів і діагностики відмов (FMEDA - Failure Mode Effect and Diagnostic Analysis).

Існуючий метод FMEDA було розроблено інженерами компанії Exida (Канада) і стала підсумком еволюції ряду методів оцінювання надійності АК, яка мала наступний перелік етапів.

Етап 1. Метод (техніка) FMEA (Failure Mode Effect Analysis) - техніка оцінки надійності розроблена в 60-х рр. минулого століття в США, в рамках програми створення ракети військового призначення «Мінітмен». Метою розробки метода було виявлення та усунення технічних проблем в складних технічних системах. Результатом виконання цього етапу була заповнена експертом (експертами) таблиця 6.1, яка включала наступну інформацію: перелік компонент системи; функції компонент і системи; перелік відмов; перелік причин відмов і перелік наслідків відмов.

Таблиця 6.1

FMEA (Failure Mode Effect Analysis)

Назва компонента системи	Функція, що виконується	Відмова	Причина відмови	Наслідки

Етап 2. Метод (техніка) FMECA (Failure Mode Effect and Criticality Analysis). Метод FMECA в 70-х було розширено врахуванням критичності спрогнозованих відмов.

Таблиця 6.2

FMECA (Failure Mode Effect and Criticality Analysis)

Назва компонента системи	Функція, що виконується	Відмова	Причина відмови	Наслідки	Критичність відмов

Етап 3. Метод (техніка) FMEDA (Failure Mode Effect and Diagnostic Analysis)

В кінці 80-х рр. виникла необхідність моделювати автоматичну діагностику інтелектуальних пристроїв. З'явилася нова архітектура на ринку контролерів безпеки під назвою «один з двох» з діагностичним вимикачем

(1oo2D), вона конкурувала з поширеною тоді мажоритарною архітектурою, що називалася «два з трьох» (2oo3). Оскільки безпека та готовність нової архітектури сильно залежали від реалізації діагностики, її кількісна оцінка стала важливим процесом. Тому метод FMECA було доповнено визначенням: частот відмов та ймовірністю виявлення відмови.

Таблиця 6.3

FMEDA (Failure Mode Effect and Diagnostic Analysis)

Назва компонента системи	Функція, що виконується	Відмова	Причина відмови	Наслідки	Критичність відмов	Частота відмови	Ймовірність виявлення відмови

Етапи методу FMEDA від компанії Exida назвемо технікою. Техніка FMEDA включає наступні етапи:

Етап 1. Виконання експертного аналізу апаратної комопоненти HW (елементної бази, юнітів – вузлів схеми) спираючись інформацію із :

- бази даних для визначення інтенсивностей відмов елементної бази, а також детальний опис (data sheets) на електронні компоненти. Використовуються наступні бази даних: SN 29500; IEC 62380; RAC FMD-91 and RAC FMD-97; Bellcore (Telcordia) standards TR-332 Issue 6 and SR-332 Issue 1; MIL HDBK 217F; exida Electrical & Mechanical Component Reliability Handbook; NSWC-98/LE1;

- бази даних для визначення режимів відмов (failure modes):

Етап 2. Виконання розрахунку інтенсивності відмов відповідного електронного компоненту схеми (наприклад за методиками бази даних MIL HDBK 217F): RAC FMD-91 and RAC FMD-97; IEC 62061; EN 954-2; IEC 61496-1; IEC 62380; exida Electrical & Mechanical Component Reliability Handbook; NSWC-98/LE1 за наступною формулою:

$$\lambda_p = (\lambda_b \, \pi_{cv} \, \pi_q \, \pi_E \, \text{failures})/10^6 \, \text{Haurs}, \qquad (6.1)$$

де λ_b – базова інтенсивність відмов, яка обраховується за формулою:

$$\lambda_b = 3*10^{-3}\,[(S/0.3)^3+1]*e^{(T+273/398)}, \qquad (6.2)$$

де T – температура середовища, S – співвідношення поточної напруги до номінальної; π_{cv} – Capacitable Factor, який залежить від ємності конденсатора ($\pi_{cv} = 41*10^{-2}C^{0.11}$); π_q - Quality Factor; π_E – Environment Factor).

Етап 3. Виконання експертного аналізу одержаних результатів. В ході аналізу експерт визначає можливі режими відмов (наприклад, розрив ланцюга, коротке замикання, відхилення значеннь електричних параметрів тощо). Заповнити таблицю 6.3

Етап 4. Виконати імпакт-аналіз можливого впливу кожної відмови (її критичність) на результати роботи системи в цілому (можливість виконати запрос на виконання функції безпеки). Розділити в залежності від цього інтенсивності відмов на наступні підмножини:

- безпечні діагностовні (λ_{sd} – Safety Detected);
- безпечні недіагностовні (λ_{su} – Safety Undetected);
- небезпечні діагностовні (λ_{dd} – Dangerous Detected);
- небезпечні недіагностовні (λ_{du} – Dangerous Undetected).

Під здібністю до виявлення відмови розуміється здібність підсистем самодіагностування виявляти відмови. Процесс виконання аналізу етапа 4 наведено на рисунку 6.2.

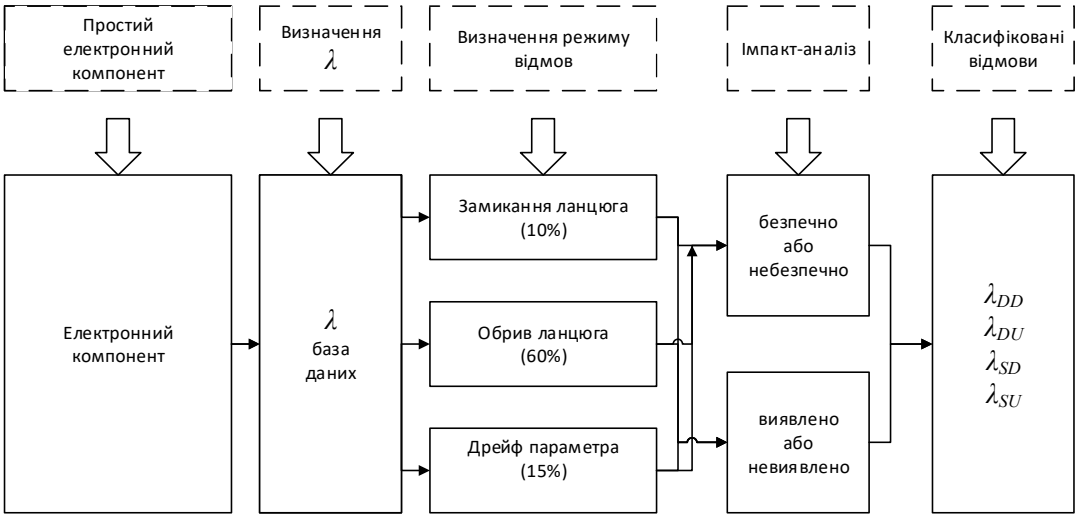


Рис. 6.2 Процесс імпакт-аналізу впливу відмови на стан виходів ситеми

Недоліки техніки FMEDA від Exida:

- вимагає багато рутинної та складної роботи для простих і складних компонент системи;
- нові компоненти (наприклад, типу FPGA) мають специфічні (не проаналізовані) режими відмов;
- не існують нормативні документи, які описують FMEDA та визначають вимоги до її продуктивності для різних типів систем;
- не враховує ненадійність, що вноситься програмною компонентою.

Здійснено модифікацію FMEDA техніки за рахунок автоматизації етапів методу для простих і складних компонент електронної схеми.

Етап 1. Застосувати інструмент генерації списку електронних компонент зі схеми.

Вхідні дані етапу: проєктна документація (опис архітектури системи, специфікації на систему в цілому та компоненти системи окремо, опис компонентної бази); електронні схеми виконані в обраній системі автоматизованого проєктування (САПР) (наприклад Altium Designer); результати FMEA (якщо такий аналіз було виконано); результати оглядів аппаратної компоненти.

Результатом виконання етапу є сформовані в електронному вигляді списки компонентів та вузлів електронної схеми, яка розробляється.

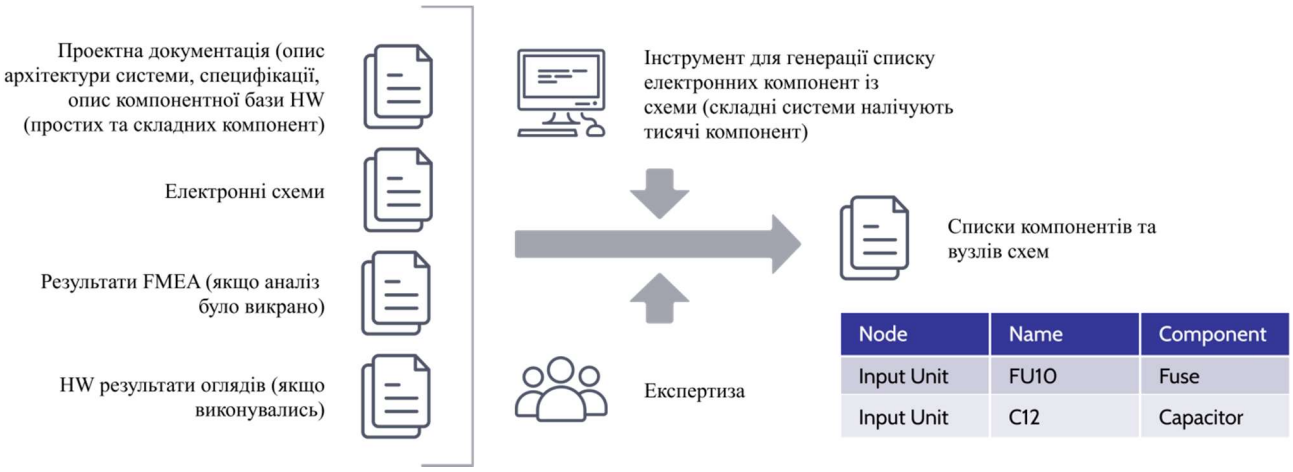


Рис. 6.3 Інформаційні процеси етапу 1 FMEDA

Етап 2. Виконати експертне -заповнення анкет вибору режимів відмов із електронної бази режимів відмов, що сформована за допомогою існуючих баз даних режимів відмов.

Вхідні дані етапу: результати етапу 1.

Результатом виконання етапу є сформований список режимів відмов для всіх компонент. Інформаційні процеси етапу 2 зображено на рисунку 6.4.

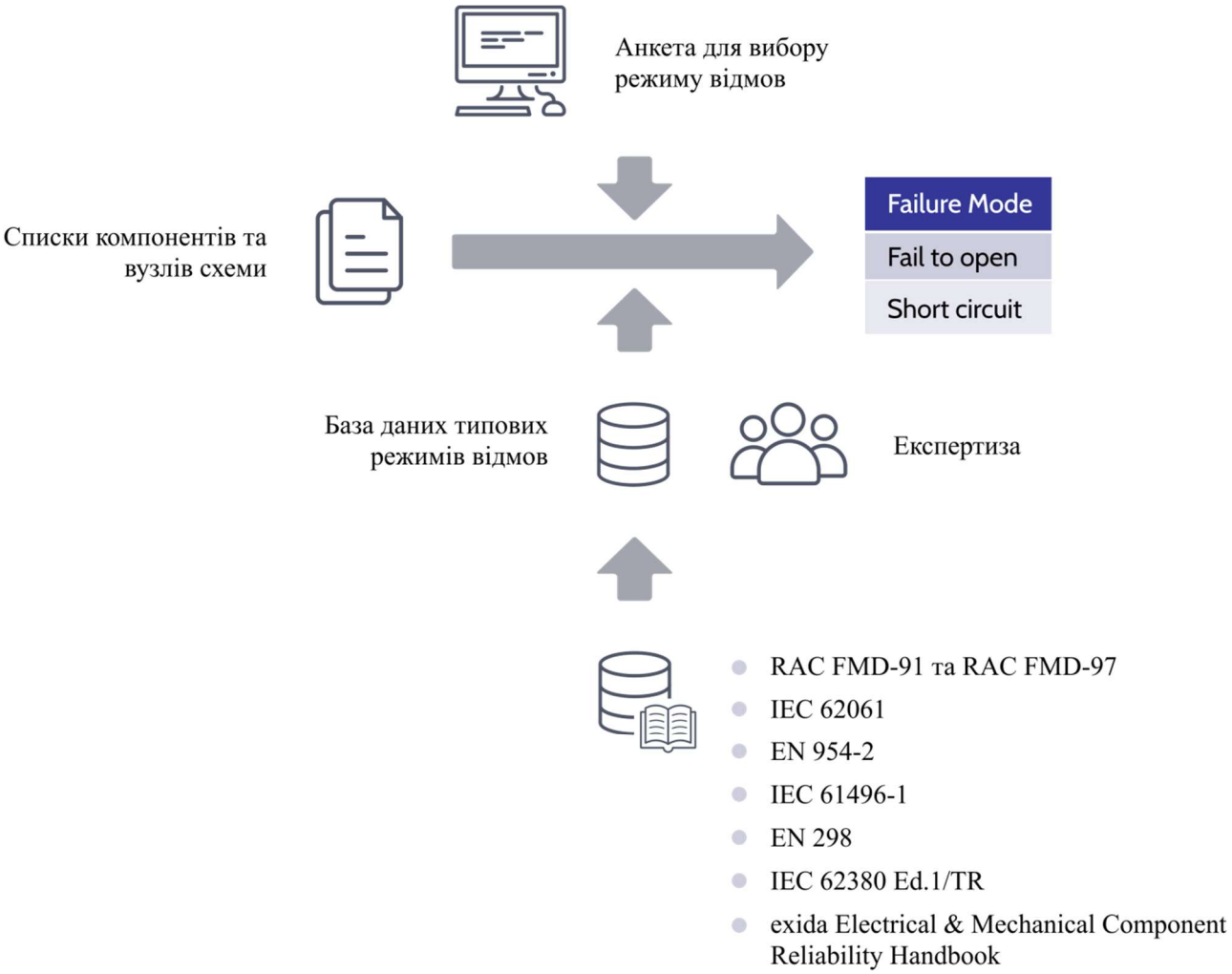


Рис. 6.4 Інформаційні процеси етапу 2 FMEDA

Етап 3. Застосувати інструмент обчислення інтенсивностей відмов електронних компонент.

Вхідні дані етапу: результати етапу 1,2.

Результатом виконання етапу є розраховані значення інтенсивностей відмов електронних компонент плати, що розробляється.

Етап 4. Виконати експертну оцінку впливу режимів відмов на функційну

безпечність (можливість виконання системою запиту на виконання функції безпеки за умови виникнення даного режиму відмови).

Вхідні дані етапу - результати виконання попередніх етапів.

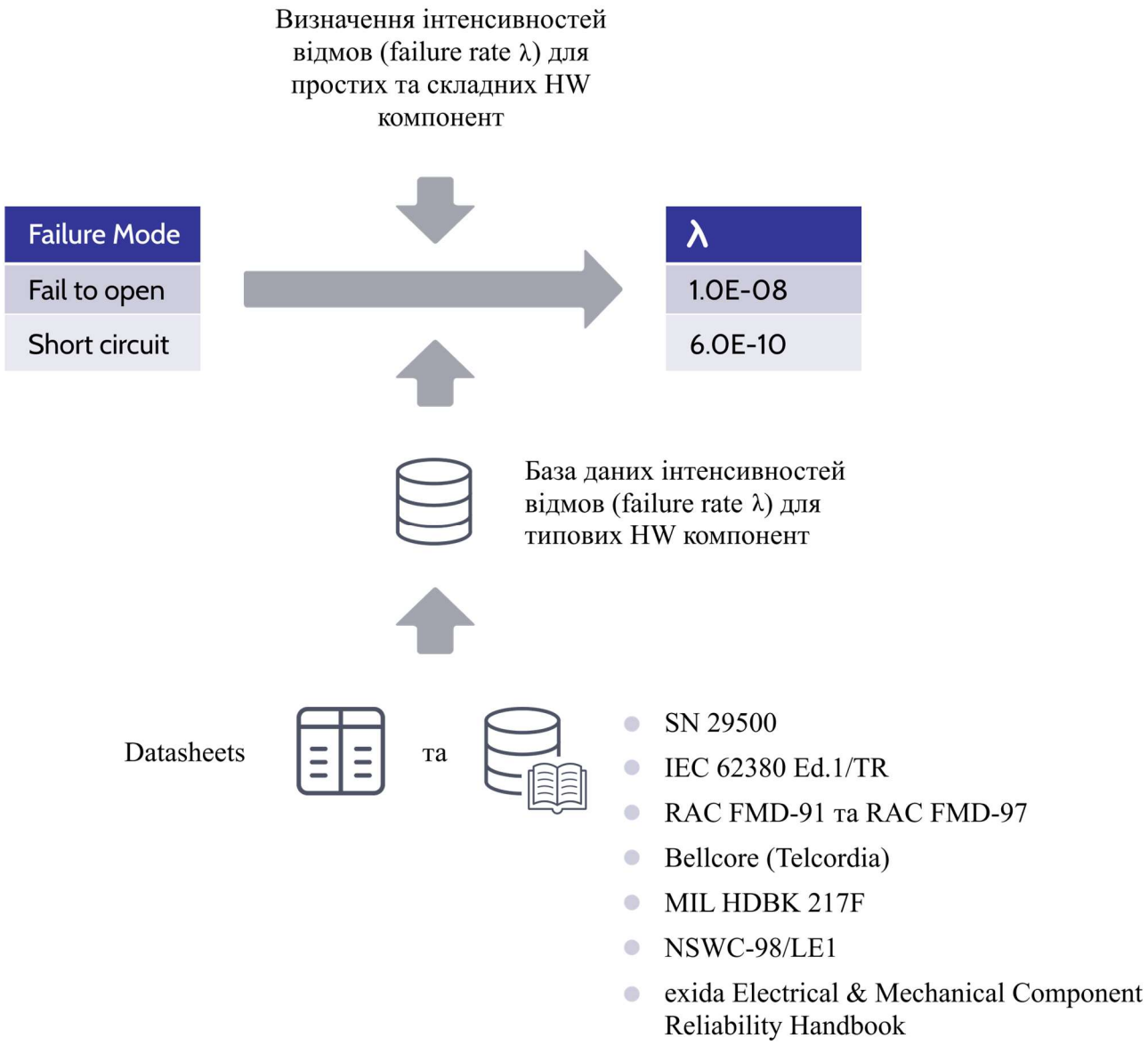


Рис. 6.5 Інформаційні процеси етапу 3 FMEDA

Результатом виконання етапу є експертна оцінка режимів відмов на підставі аналізу значень інтенсивностей відмов та огляду проектних рішень платі, що розробляється. Кожному режиму дається оцінка безпечно/небезпечно (Safety/ Dangerous).

Етап 5. Виконати експертне оцінювання можливості детектування режиму відмови засобами вбудованої самодіагностики.

Вхідні дані етапу - результати виконання попередніх етапів.

Рис. 6.6 Інформаційні процеси етапу 4 FMEDA

Результатом виконання етапу є оцінка діагностичного покриття схеми, що розробляється (Diagnostic Coverage).

Рис. 6.7 Інформаційні процеси етапу 5 FMEDA

Етап 6. Розробка фінального звіту FMEDA.

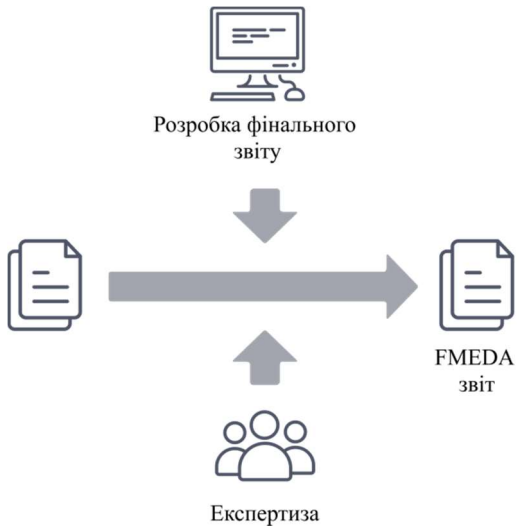


Рис. 6.8 Інформаційні процеси етапу 6 FMEDA

Фрагмент (приклад) фінального звіту FMEDA Report наведено в таблиці 6.4.

Таблиця 6.4

Фрагмент FMEDA Report

	A	B	C	D
1	LISTS OF FIT TESTS PER PHYSICAL MODULE 2013-11-21/11:12:06 AM			
2				
3	MODULE	MODULE	MODULE	MODULE
4	LM	AIM	DIM	DOM
5				
6	[LM.PS 3.3v lost *IT]	[IO.INPUT LOSS OF COMM *IT]	[IO.INPUT LOSS OF COMM *IT]	[IO.PS VCCINT 1.2V lost]
7	[LM.PS 5.0v lost *IT]	[IO.PS VCCINT 1.2V lost]	[IO.PS VCCINT 1.2V lost]	[IO Communcations fault]
8	[LM.PS VCC_GXB 1.1v lost]	[IO Communcations fault]	[IO Communcations fault]	[IO Clock A failure]
9	[LM.PS VCC_GXB 1.5v lost]	[IO Clock A failure]	[IO Clock A failure]	[IO Clock B failure]
10	[LM.PS VCC 0.9v lost]	[IO Clock B failure]	[IO Clock B failure]	[IO Clock C failure]
11	[LM.PS VCCIO 2.5v lost]	[IO Clock C failure]	[IO Clock C failure]	[IO FPGA package failure]
12	[LM loss of comm to FPGA2]	[IO FPGA package failure]	[IO FPGA package failure]	[IO FPGA CONFIG HARD FAILURE]
13	[LM loss of comm to each IOM *IT]	[IO FPGA CONFIG HARD FAILURE]	[IO FPGA CONFIG HARD FAILURE]	[IO FPGA USER LOGIC GATES RAM HARD FAULTS]
14	[LM clock A fault]	[IO FPGA USER LOGIC GATES RAM HARD FAULTS]	[IO FPGA USER LOGIC GATES RAM HARD FAULTS]	[IO FPGA CONFIG SOFT FAULTS]
15	[LM clock B fault]	[IO FPGA CONFIG SOFT FAULTS]	[IO FPGA CONFIG SOFT FAULTS]	[IO FPGA USER RAM SOFT FAULTS]
16	[LM clock C fault]	[IO FPGA USER RAM SOFT FAULTS]	[IO FPGA USER RAM SOFT FAULTS]	[IO.PS 3.3v Lost *IT *ETT]
17	[LM.FPGA1 pkg fault]	[IO.PS 3.3v Lost *IT *ETT]	[IO.PS 3.3v Lost *IT *ETT]	[IO.PS 3.3v Low]
18	[LM.FPGA1 config RAM hard fault]	[IO.PS 3.3v Low]	[IO.PS 3.3v Low]	[IO.PS 3.3v High]
19	[LM.FPGA1 config memory soft fault]	[IO.PS 3.3v High]	[IO.PS 3.3v High]	[IO.PS 5.0v Lost]
20	[LM.FPGA1 user RAM soft fault]	[IO.PS 5.0v Lost]	[IO.PS 5.0v Lost]	[IO.PS 5.0v Low]
21	[LM.PS 3.3v low]	[IO.PS 5.0v Low]	[IO.PS 5.0v Low]	[IO.PS 5.0v high]
22	[LM.PS 3.3v high]	[IO.PS 5.0v high]	[IO.PS 5.0v high]	[IO.PS VCCA 2.5v lost]
23	[LM.PS 5.0v low]	[IO.PS VCCA 2.5v lost]	[IO.PS VCCA 2.5v lost]	[IO.PS VCCA 2.5v low]
24	[LM.PS 5.0v high]	[IO.PS VCCA 2.5v low]	[IO.PS VCCA 2.5v low]	[IO.PS VCCA 2.5v high]
25	[LM.PS VCCL_GXB 1.1v lost]	[IO.PS VCCA 2.5v high]	[IO.PS VCCA 2.5v high]	[IO.PS 2.5v BANKS lost]
26	[LM.PS VCCL_GXB 1.1v low]	[IO.PS 2.5v BANKS lost]	[IO.PS 2.5v BANKS lost]	[IO.PS 2.5v BANKS low]
27	[LM.PS VCCL_GXB 1.1v high]	[IO.PS 2.5v BANKS low]	[IO.PS 2.5v BANKS low]	[IO.PS 2.5v BANKS high]
28	[LM.PS VCCL_GXB 1.5v lost]	[IO.PS 2.5v BANKS high]	[IO.PS 2.5v BANKS high]	[IO.PS VCCINT 1.2v low]
29	[LM.PS VCCL_GXB 1.5v low]	[IO.PS VCCINT 1.2v low]	[IO.PS VCCINT 1.2v low]	[IO.PS VCCINT 1.2v high]
30	[LM.PS VCCL_GXB 1.5v high]	[IO.PS VCCINT 1.2v high]	[IO.PS VCCINT 1.2v high]	[DOU HL switch stuck on]
31	[LM.PS VCC 0.9v low]	[AIU ADC A/B comparison]	[DIU SHORTED FIELD CONTACT]	[DOU LL switch stuck on]
32	[LM.PS VCC 0.9v high]	[AIU +12V RAIL LOW]	[DIU OPEN CCT FIELD LOOP *ETT]	[IO.OUTPUT LOSS OF COMM *IT]
33	[LM.PS VCCIO 2.5v low]	[AIU -12V RAIL LOW]	[DIU HL SENSE STUCK ON]	[IO.OUTPUT 3.3v lost]
34	[LM.PS VCCIO 2.5v high]	[AIU +12V RAIL HIGH]	[DIU HL SENSE STUCK OFF *ETT]	[IO.OUTPUT 5.0v lost]
35	[LM.PS clock B fault]	[AIU -12V RAIL HIGH]	[DIU LL SENSE STUCK ON]	
36	[LM.FPGA1 Logic gate RAM hard fault]	[AIU FB A/B comparison]	[DIU LL SENSE STUCK OFF *ETT]	
37	[LM.DIU LL SENSE STUCK ON]	[AIU A/D Valid Range Check *LE]	[DIU LVL TEST SW STUCK ON]	
38	[LM.DIU LVL TEST SW STUCK ON]	[AIU A/D Valid Range Check]	[DIU LVL SW STUCK OFF *ETT]	
39	[LM.DIU Loss of 24v *ETT]		[DIU SOURCE ON TEST SW STUCK OFF *ETT]	
40	[LM.DIU Low 24v *ETT]		[DIU Loss of 24v *ETT]	
41	[LM.DIU Loss of 3.3v *IT]			

В таблицю включено режими відмов, які в ході аналізу віднесено до небезпечних і які є обов’яковими для перевірки методом внесення дефектів до

апаратної компоненти перспективної цифрової інформаційно-керуючої платформи (ЦІКП) RadICS виробництва: логічного модуля (LM- Logic Module); модуля аналогових входів (AIM- Analog Inputs Module), модуля цифрових входів (DIM - Discrete Inputs Module), модуля цифрових виходів (DOM - Discrete Outputs Module).

Відповідно до FMEDA техніки визначено рівні внесення дефектів:

- на рівні VHDL кода (саботажник, аналог ДП ПЗ) для окремих програмних компонент і електронного проекту в цілому, де під саботажником розуміється фрагмент додаткового коду, який ін'єктується в програмний компонент для симуляції і перевірки впливу визначеного режиму відмови;

- дефект фізичний на рівні Chip (для ЦІКП RadICS це ПЛІС) ;

- дефект фізичний на рівні юнітів (вузлів) та окремого модуля в цілому;

- дефекти фізичні одночасно в різні модулі (мультидефекти);

- дефекти взаємодії (зовнішні впливи - навмисні і ненавмисні);

- дефекти рівня даних конфігурування системи (на рівні програмного забезпечення, яке відповідає за конфігурування системи);

- дефекти рівня IDE (Integrated Development Environment).

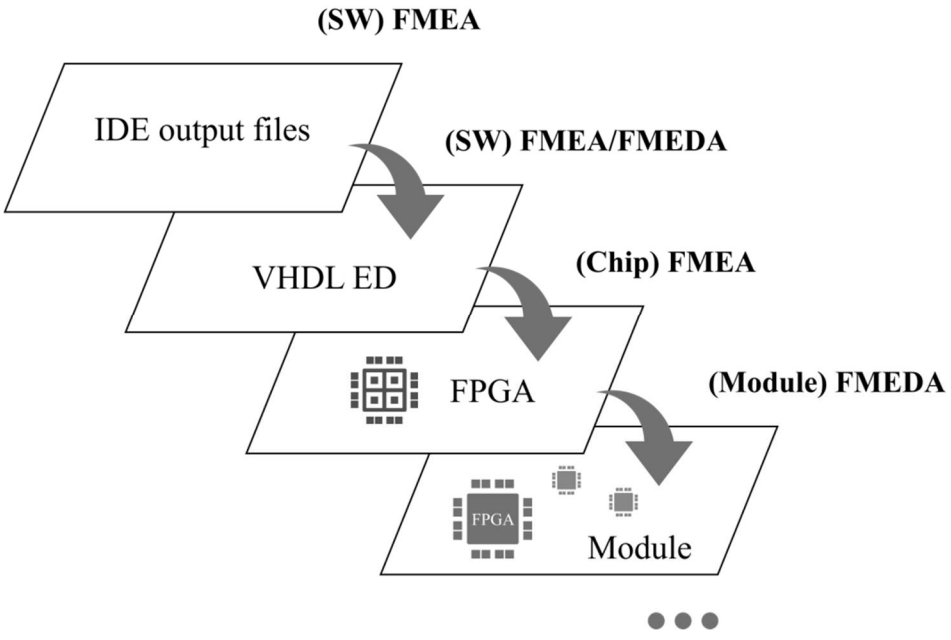


Рис. 6.9 Рівні внесення дефектів (FMEA/FMEDA and HW/SW FIT процедури для FPICS)

6.1.2 Модифікована процедура FIT

Атрибути надійності та функційної безпечності зазнали декілька етапів еволюції, основними з яких були:

- I – етап: (1950-1960-ті роки): синтез цифрових автоматів з мінімальною кількістю елементів. На цьому етапі було визначено основні вимоги, що стосуються спрощення систем та забезпечення надійності [284];

II – етап: (1970-1990-ті роки): розроблено методи синтезу самоперевіряємих цифрових автоматів та відмовостійких систем, сформульовано основні вимоги до здатності до перевірки та реконфігурування;

III – етап: (2000–2010-ті роки): розроблено методи синтезу легко перевіряємих та безпечних цифрових автоматів, новою додатковою вимогою до критично важливих доменів безпеки є забезпечення безпеки та демонстрація необхідного рівня безпеки при розробці, верифікації, валідації та експлуатації.

У цьому випадку можна говорити про здатність компонент та системи в цылому до перевірки як важливий атрибут I&C (FIT – ability. англ. Придатність системи до ін’єктування дефектів).

На рисунку 6.9 схематично зображено основні етапи еволюції атрибутів надійності і функційної безпечності.

Таким чином, методи синтезу перевіряємих та безпечних цифрових автоматів третього етапу еволюції надійності та функційної безпечності для забезпечення безпеки та демонстрації необхідного рівня безпеки при розробці, верифікації, валідації та експлуатації ПТК мають бути доповнено додатковими етапами.

В основу етапу тестування з ін’єктуванням дефектів покладено придатність електричної схеми, окремих її компонент та вбудованого ПЗ до ін’єктуванням дефектів.

Визначення 6.1

FIT (Fault insertion testing)- придатність - це придатність до ін’єктування

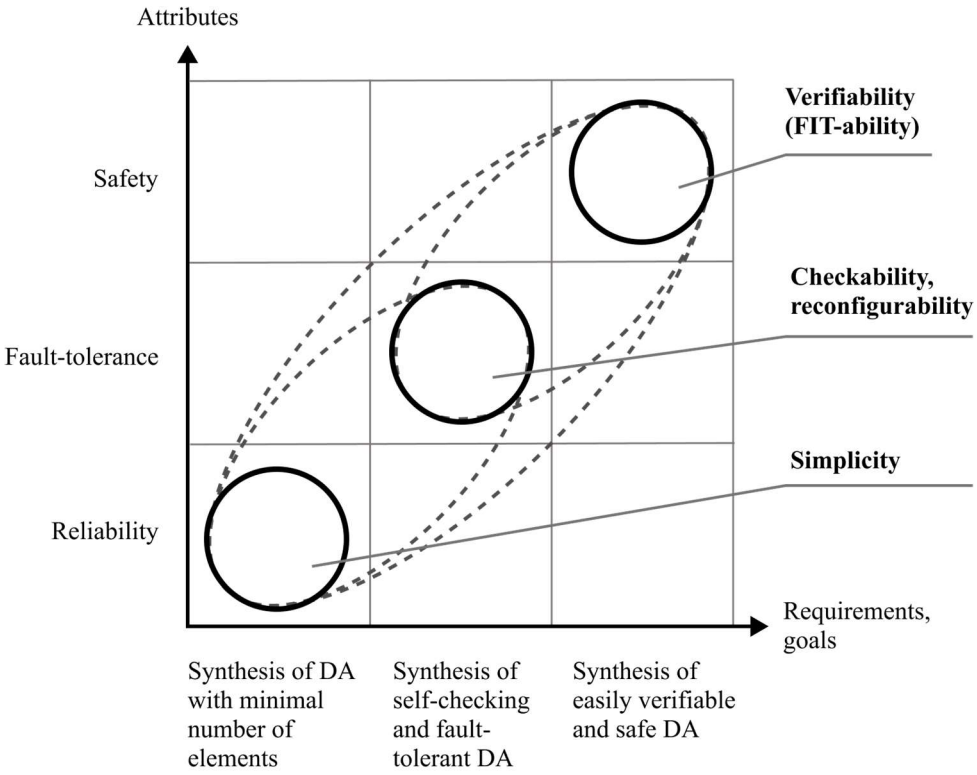


Рис. 6.9 Етапи еволюції атрибутів надійності та функційної безпечності

дефектів у електричні схеми та окремі компоненти ї схеми (HW FIT-здатність) або програмного коду (SW FIT-здатність).

Для SIL-орієнтованого процесу сертифікації ICS концепція SW&HW FIT-здатності може бути визначена як здатність виконати тест на введення (ін'єкцію) за результатами FMEA або FMEDA на різному рівні ієрархії системи: (модуль системи, юніт модуля, електронний проєкт, система в цілому) FMEDA; системний SW, реалізований з кодом HDL (Chip) - FMEDA; програми SW - конфігураційні файли, що генеруються інтегрованим середовищем розробки) – FMEA.

Метою виконання модифікованої процедури FIT – є перевірка: здатності діагностичних підсистем виявляти різнотипні дефекти HW та помилки в даних конфігурації для вбудованого SW і ініціювати запуск захисних дій на рівні системи відповідно до типу виявленого дефекту (помилки); підтвердження рівня надійності та функційної безпечності системи; стійкості системи до зовнішніх вторгнень; збільшення діагностичного покриття on-line тестування.

6.1.3 Теоретичні аспекти HW та SW FIT –придатності

Опишемо схему S_{FIT}, яка є об'єктом процедури HW FIT, вона може бути представлена парою:

$$S_{FIT} = <G = \{A, B\}, T_{FMEDA} >, \quad (6.3)$$

де $G = \{A, B\}$ – граф, що описує схему S_{FIT}, який складається з набору вузлів (елементів схеми), $A = \{a_x\}$ і набору ребер $B = \{b_y\}$; $T_{FMEDA} = \{f_i, m_i, e_i, d_i, c_i\}$ - набір (таблиця FMEDA), що складається з підмножини типів дефектів f_i, режимів відмов m_i, ефектів відмов e_i, діагностичних атрибутів d_i, що визначають можливість (виявлення) дефекту f_i, та критичності дефектів c_i, i = 1,…, F. Таким чином в таблиці FMEDA представлений перелік симптомів, які слід перевірити в ході виконання тестування з ін'єктуванням дефектів.

Для HW FIT у відповідності до рисунка 6.9. маємо:

$$FMEDA=(Chip)FMEDA \cup (Module)FMEDA \cup (Cabinet)FMEDA \cup \cup (System)FMEDA, \quad (6.4)$$

де *(Chip)FMEDA* - виконаний аналіз для ПЛІС (FPGA), *(Module)FMEDA* – виконаний аналіз для модуля ПЛК, *(Cabinet)FMEDA* - виконаний аналіз для набора модулів, що уможливлює виконання процедури мульті - FIT (одночасне внесення двох і більше дефектів), *(System)FMEDA* – виконаний аналіз для системи в цілому (як часний випадок для FPICS).

Наступним завданням є визначення позиції (точки схеми) pf_i та засобів mf_i внесення для всіх дефектів f_i. Загалом pf_i і mf_i - це множини $pf_i = \{pf_ij\}$, $mf_i = \{mf_{ik}\}$, j = 1,…, npf_i; k = 1,…, nmf_i і тоді маємо:

$$\exists i,v,\ i \neq v: pf_i \cap pf_v \neq \varnothing,\ mf_i \cap mf_v \neq \varnothing. \quad (6.5)$$

Повний простір FIT покриття для дефекта f_i (Full FIT covered space - $FFCSf_i$), є множина, яка є декартовим добутком:

$$FFCSf_i = pf_i \, x \, mf_i.. \tag{6.6}$$

Повний простір FIT покриття дефектів для схеми (Full FIT covered space of scheme (FFCS)) є об'єднання:

$$FFCSS = \cup FFCSf_i, \, , \, i = 1,...,F. \tag{6.7}$$

Тривіальний простір FIT покриття дефектів (Trivial FIT of f_i ($TFCS_i$)) є:

$$\begin{gathered} \forall pf_{ij} \;\; \exists! \, mf_{ij}, \; Card \; TFCS_i = npf_i; \\ TFCS = \cup TFCSf_i, \; TFCS_{i,} \subseteq FFCSf_i, \\ TFCS \subseteq FFCSf. \end{gathered} \tag{6.8}$$

Імплементований простір покриття для схеми (Implemented FIT covered space of scheme (IFCS)) є підмножиною *FFCS* і визначається*:*

$$IFCS \subseteq FFCS \text{ (and } TFCS \subseteq IFCS) \tag{6.9}$$

та має бути розроблений у відповідності до множини обмежень(restrictions) виконання процедури $FITR = \{r_z\}$ для різних рівнів системи. Маємо наступні обмеження на виконання HW FIT:

r1 - параметри елементів не змінюються при температурних та механічних впливах;

r2 - введення дефекту для елемента $a_x \in A$ (у просторі елементів a_x) не спричиняє новий дефект або неприйнятну зміну параметрів інших елементів a_q;

r3 - будь-який елемент $a_x \in A$ повинен бути технологічно прийнятним для внесення дефекту;

r4 – внесений дефект видаляється без додаткових доробок системи і працездатність відновлюється.

Отже:

$$IFCS = FITR \blacklozenge FFCS, \tag{6.10}$$

де $\blacklozenge$ -операція фільтрації набору FFCS набором FITR. IFCS описується наборами позицій $Ipf_i = \{Ipf_{ij}\}$ і значень вносимого дефекту $Imf_i = \{Imf_{ik}\}$, j = 1,…, $Inpf_i$; k = 1,…, nmf_i. Зрозуміло, що $\forall Ipf_{ij} \subseteq pf_{ij}$, $\forall Imf_{ik} \subseteq mf_{ik}$.

Тоді, як приклад, функцію покриття тестами HW FIT можливо записати для вузла (юніта) схеми як:

$$\Phi_{HW\ FIT} = (p1m11 \vee p2m11 \vee \ldots \vee p_i m11) \wedge (p1m21 \vee p2m21 \vee \ldots \vee p_i m21) \wedge \ldots \wedge (p1m_{ik} \vee \ldots \vee p_i m_{ik}) \tag{6.11}$$

Початковими даними для виконання SW FIT - є результати FMEA. Під час FMEA виконується аналіз джерел ризиків, які можуть виникнути під час роботи з IDE (Integrated Development Environment) та формування файлів конфігурації FPICS. Ці результати є типами відмов.

Основними завданнями виконання фази тестування SW FIT є наступні:

- перевірка здатності діагностичної підсистеми логічного модуля FPICS виявляти помилки в конфігураційних даних і перевірка готовності системи до виконання захисних дій відповідно до типу виявленого дефекту;

- перевірка здатності он-лайн-компонентів IDE виявляти помилки в даних конфігурації перед їх завантаженням в FPICS;

- перевірка здатності підсистем діагностування елементів систем відображення (моніторингу стану сигналів) виконувати пом'якшувальні (захисні заходи) при зміні параметрів настройки логіки користувача.

Для SW FPICS маємо:

$$FMEA = \cup (SW\ Components) FMEA, \tag{6.12}$$

де *SW Components* – окремі компоненти комплексу програмного забезпечення, такими комплексами є більшість IDE, CAD – системи. Для кожної окремої компоненти визначається підмножина режимів відмов (дефектів) та ефекти їх впливу на працездатність ПЗ та FPICS в цілому. Кількість підмножин відповідає кількості тестованих компонентів SW. Тоді F = $\{f_i\}$ - це повний набір SW-дефектів, а SWComp = $\{SWComp_i\}$ - множина протестованих компонентів SW. Тоді можна встановити відображення набору SW компонентів на набір дефектів:

$$f: SWComp \rightarrow F \tag{6.13}$$

Наступним завданням виконання процедури, за аналогією HW FIT, для кожної пари f_i - $SWComp_i$ є встановлення положення (точка внесення) pf_i і значення mf_i вставки. Загалом pf_i and mf_i є множини $pf_i = \{pf_{ij}\}$, $mf_i = \{mf_{ik}\}$, $j = 1,\ldots, npf_i$; $k = 1,\ldots, nmf_i$, і ідповідно повний простір SW FIT покриття дефектів (SW FIT covered space of f_i (FF_SWCSf_i)) є декартовим добутком:

$$FF\_SWCSf_i = pf_i \times mf_i. \tag{6.14}$$

Відповідно повний простір SW FIT покриття SW (FF_SWCS) є об'єднання всієї множини FF_SWCSf_i:

$$FF\_SWCS = \cup FF\_SWCSf_i, , i = 1,\ldots,F. \tag{6.15}$$

Реалізований простір покриття для програмного компонента (IF_SWCS - Implemented SW FIT covered space of component) - є підмножиною FF_SWCS,. IF_SWCS слід розробляти з урахуванням основного обмеження SW FITR - введення несправності SW для SWComp повинно бути технологічно прийнятним.

Тоді, як приклад, функцію покриття тестами SW FIT можливо записати для програмного компонента як:

$$\Phi_{SW\,FIT} = (p1m11 \vee p2m11 \vee ..... \vee p_i m11) \wedge (p1m21 \vee p2m21 \vee ..... \vee p_i m21) \wedge .... \wedge (p1m_{ik} \vee ..... \vee p_i m_{ik}) \quad (6.16)$$

6.1.4 HW та SW FIT – методи

Етапи HW FIT – метода наступні.

Етап 1. Одержання наборів $FFCSf_i$, FFCSS та відповідних таблиць (Таблиця 6.5). Особливістю цього етапу є необхідність вірного розуміння та технологічної інтерпретації симптому на основі FMEDA.

Таблиця 6.5

Таблиця встановленого списку дефектів і відповіних ним точок та значень внесення і виконання HW FIT

Дефекти, f_i	Атрибути внесення дефектів	
	Точки внесення, pf_i	Значення внесення, mf_i
f_1	pf_1	mf_1
…	…	…
f_F	pf_F	mf_F

Етап 2. Побудова IFCS у відповідності з встановленими обмеженнями FITR:

r1 - параметри елементів не змінюються при температурних та механічних впливах;

r2 - введення дефекту для елемента $a_x \in A$ (у просторі елементів a_x) не спричиняє новий дефект або неприйнятну зміну параметрів інших елементів a_q;

r3 - будь-який елемент $a_x \in A$ повинен бути технологічно прийнятним для внесення дефекту;

r4 – внесений дефект видаляється без додаткових доробок системи і працездатність відновлюється.

Таблиця 6.6

Таблиця IFCS

Дефекти, f_i	Атрибути внесення дефектів	
	Точки імплементації дефекта, Ipf_i	Значення імплементації дефекта, Imf_i
f_1	Ipf_1	Imf_1
…	…	…
f_F	Ipf_F	I mf_F

Етап 3. Для обраних точок (Ipfi) та засобів внесення дефектів (Imfi) слід визначати методи HW FIT з урахуванням, встановлених обмежень.

Етап 4. Внесення дефектів в обрані точки та встановленими і розробленими засобами.

Етап 5. Документування результатів тестування (оформлення звітів розробленого зразку). За умови виявлення дефектів, інформування розробників, усування дефектів та проведення регресійного тестування.

Етапи SW FIT – метода наступні.

Етап 1. Поділ множини типів відмов на підмножини, розроблення таблиці 6.6.

Таблиця 6.7

Таблиця відповідності типу дефекту програмній компоненті

Типи дефектів, f_i	SW Components		
	SW Com_1	…..	SW Com_M
f_1	+		+
…			+
f_F	+		

Етап 2. Одержання множин FF_SWCSf_i, FF_SWCS та відповідних таблиць. Особливістю цього етапу є необхідність правильного розуміння та технологічної інтерпретації відмов на основі FMEA.

Таблиця 6.8

Таблиця FF_SWCS

Підмножина дефектів SW компоненти, f_i	Атрибути внесення SW дефектів	
	Точки внесення, pf_i	Значення, mf_i
f_1	pf_1	mf_1
…	…	…
f_z	pf_j	mf_F

Етап 3. Побудова IF_SWCS у відповідності з встановленими обмеженнями FITR для кожної підмножини дефектів:

Таблиця 6.9

Таблиця IF_SWCS

Підмножина дефектів SW компоненти, f_i	Атрибути внесення SW дефектів	
	Точки внесення, Ipf_i	Значення, Imf_i
f_1	Ipf_1	Imf_1
…	…	…
f_z	Ipf_j	Imf_F

Етап 4. Для обраних точок (Ipf_i) та значень внесення SW дефектів (Imfi) слід визначити методи внесення (техніки внесення) SW FIT та SW FIT інструменти (Tools), які повинні бути розроблені під час проектування тесту SW FIT.

Етап 5. Внесення дефектів обрані точки розробленими засобами.

Етап 6. Документування результатів виконання тестів. У випадку виявлення дефектів, інформування розробників, усунення дефектів та виконання регресійного тестування з повторним документуванням.

6.1.5 Метод верифікації та валідації модулів, платформ і ПТК

Запропоновані HW & SW FIT процедури покладено в основу метода верифікації та валідації програмовних платформ і програмно-технічних комплексів на їх основі, який базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов (FMEDA/FMECA(для SW)) та ін'єктування фізичних і програмних дефектів (HWFIT/SWFIT), що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності.

Основні етапи метода наступні:

Етап 1.

Виконується визначення HW та SW складових компонент системи, що розробляється.

Початкові дані етапу – документи груп розробки HW та SW компонент (специфікації вимог до системи і окремо HW та SW компонент, детальний дизайн HW&SW, алгоритми користувацької логіки та інш.)

Результатом виконання етапу є: списки простих та складних електронних компонент системи, схемотехнічні рішення на рівні юнітів, модулів, конструктивних елементів ПТК, тощо). Структура ПЗ (перелік, бібліотеки ПЗ вернього та нижнього рівнів та інш.).

Етап 2.

Аналіз складових системи

Початкові дані етапу – списки простих та складних електронних компонент системи, схемотехнічні рішення на рівні юнітів, модулів, конструктивних елементів ПТК, тощо). Структура ПЗ (перелік, бібліотеки ПЗ вернього та нижнього рівнів та інш.).

Результатом виконання етапу є звіти за результатами огляду документів дизайну відповідно HW та SW компонент.

Етап 3.

Виконання аналізу FMEDA та задіяння метода HW Fault Insertion Testing.

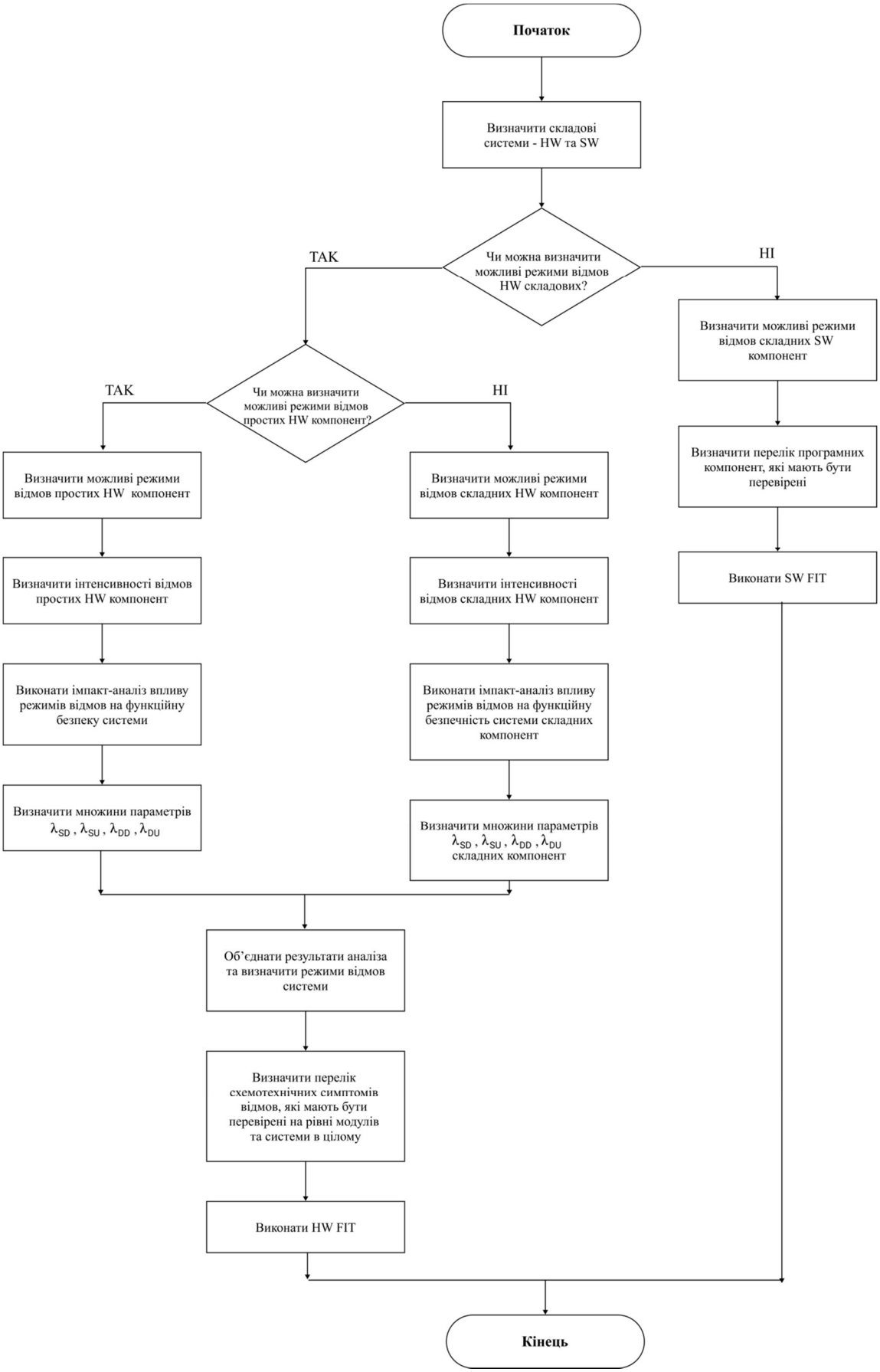


Рис. 6.10 Алгоритм методу верифікації та валідації програмовних платформ і ПТК на їх основі

Етап 4.

Виконання аналізу FMEA та задіяння метода SW Fault Insertion Testing.

Етап 5. Аналіз результатів верифікації та валідації. Оформлення звітів з тестування.

У випадку знаходження дефектів АК або ПК, в звіт включається таблиця із списком дефектів та передається групам розробки для аналізу. Групи розробки аналізують виявлені дефекти та приймають рішення щодо їх усунення або обгрунтовують відмову від усунення.

Після завершення усунення дефектів виконується регресійне (повторне вибіркове) тестування з повторним оформленням звітів в частині перетестованих компонент.

6.2 Метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні платформ і ПТК інформаційно-керуючих систем

6.2.1 Вимоги та особливості оцінювання та забезпечення функціональної безпеки при розробленні та ліцензуванні

Прийняття концепції "життєвого циклу безпеки" (Safety Life Cycle - SLC) є загальним для всіх сучасних стандартів, пов'язаних з функціональною безпечністю. У стандартах IEC використовуються моделі SLC, які охоплюють повний термін експлуатації продукту безпеки або системи безпеки, або повну систему I&C (відповідно до IEC 61513).

На рисунку 6.11 представлено концепцію розроблення продукції у відповідності до SLC у відповідності до стандарту IEC 61513. Затінені деталі стосуються розробки системи, конкретного пристрою або програмного забезпечення.

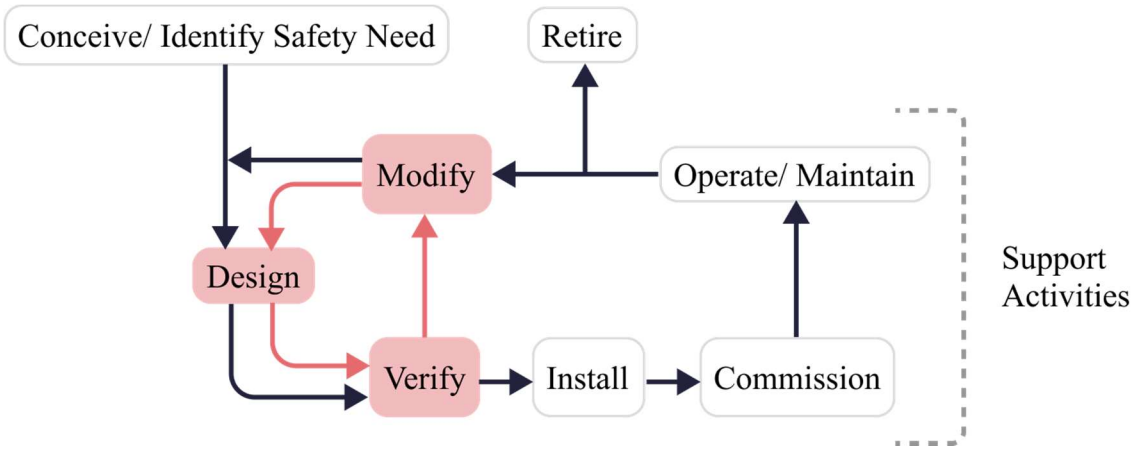


Рис. 6.11 Життєвий цикл безпеки відповідно до IEC 61513

IEC 61508 представляє життєвий цикл безпеки. До кожного етапу життєвого циклу наведено вимоги, які необхідно на ньому виконати. Прикладом імплементації концепції життєвого циклу безпеки системи та наведеного життєвого циклу безпеки є розроблена та реалізована V-модель у відповідності до активностей якої, розроблено, верифіковано та ліцензовано перспективну цифрову інформаційно-керуючу платформу RadICS, рисунок.12.

Представлена модель дає опис загального та локальних процесів розроблення та верифікації і валідації сучасної ЦІКП RadICS. «Ліва» гілка моделі описує послідовний процесс розроблення та верифікації проєктних документів, основними з них є наступні: англ. Product Concept Document (PCD) - концепція продукту; FPGA-based Safety Controller System Requirements Specification (FSC SRS)– специфікація системних вимог; Product Architecture Document (PAD) – архітектура безпечного ПЛК; Static Code Analysis Code Review Report та інші. «Права» гілка моделі описує послідовність процесів виконання валідаційних процедур (тестування коду, інтеграція системи, в тому числі виконання процедури тестування з внесенням дефектів, валідація системи). Інтеграційні тести присвячено перевірці вимог до архитектури ПЛК, валідаційні - тестуванню системних вимог. Горизонталні зв’язки вказують на взаємозв’язок проєкнтих процесів та артефактів між гілками моделі. Зв’зяки, що вказують зворотні напрямки виконання проєктних завдань вказують на те, що модель передбачає повернення процесів на попередні етапи у випадку

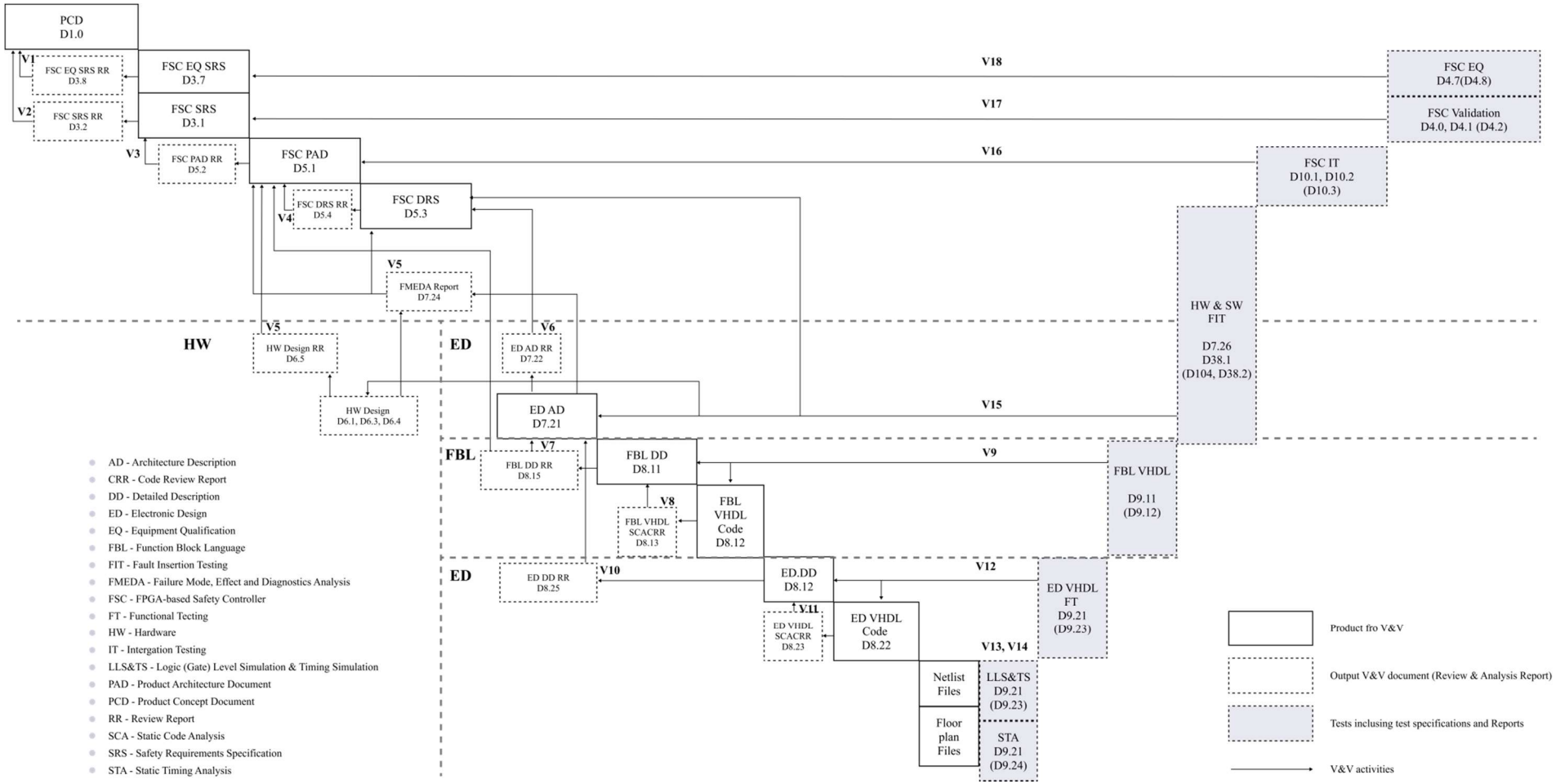


Рис. 6.12 V-модель життєвого циклу активностей розроблення та верифікації і валідації ЦІКП RadICS

виникнення проблем на поточному етапі роботи. Одним із основних результатів розроблення і застосування даної моделі є досягнення безпечним ПЛК ЦІКП RadICS рівня функційної безпечності SIL-3 згідно всіх вимог IEC 61508 [314-317].

6.2.2 Алгоритм метода

Розроблені та запропоновані методи покладено в основу підсумкового метода оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах.

Основні етапи метода наступні:

Етап 1.

Застосування послідовності оцінювання надійності ПЗ шляхом комплексування моделей надійності програмних засобів та урахування їх вторинних дефектів.

Початкові дані етапу – Аналіз вимог до системи (System Requirements Specification, Software Requirements Specification, Software Detailed Design and Implementation). Аналіз етапів ЖЦ (етапи дизайну та тестування), статистичні дані про ДП ПЗ, лінія регресії, рівняння лінії регресії, коефіцієнт кореляції.

Результатом виконання етапу є: обчислені значення функції ризику λ_d (t) та величини її зміни $\Delta\lambda_d$ (t) на основі обраних та модифікованих МНПЗ.

Етап 2.

Застосування метода оцінювання надійності та функційної безпечності ПТК зі структурно-версійною надмірністю.

Початкові дані етапу – специфікація системних вимог (опис системних функцій, опис сценаріїв функціонування, функціональні вимоги,вимоги до інтерфейсів, вимоги до продуктивності, вимоги до оточующого середовища, вимоги до інформаційноЇ безпеки, вимоги до надійності), специфікація вимог

до Software, специфікація вимог до Hardware, архітектурні вимоги до ПТК, детальний дизайн SW та HW

Результатом виконання етапу є: обчислені прогнозні значення показників надійності та функціональної безпеки ПТК за обраною архітектурою.

Етап 3.

Застосування метода забезпечення надійності та функційної безпечності ПТК на самодіагностовних програмовних платформах шляхом використання різних варіантів надмірності (диверсності.)

Початкові дані етапу – специфікація системних вимог (опис системних функцій, опис сценаріїв функціонування, функціональні вимоги, вимоги до інтерфейсів, вимоги до продуктивності, вимоги до оточующого середовища, вимоги до інформаційноЇ безпеки, вимоги до надійності), специфікація вимог до Software, специфікація вимог до Hardware, архітектурні вимоги до ПТК, детальний дизайн SW та HW, результати Етапу 2, результати тестування ПЗ

Результатом виконання етапу є:

Етап 4.

Застосування метода верифікації та валідації ПТК на програмовних платформах

Початкові дані етапу – детальний дизайн SW та HW, результати Етапу 2, результати тестування ПЗ

Результатом виконання етапу є: результати виконання SW та HW Fault Insertion Testing (висновки щодо якості технічних рішень щодо побудови системи вбудованої програмної та апаратної діагностики).

Етап 5. Виконання порівняння уточнених значень показників надійності та функційної безпечності із тими, що вимагає технічне завдання на систему.

$$\text{ПН\&ПФБ} \in \text{Н\&ПФБ} \geq (\text{ПН\&ПФБ})^{\text{Вим}}.$$

Запропоновано основні контрольні точки задіяння метода (рисунок 6.15):

Р1 – після завершення етапу розроблення множини специфікацій вимог до системи та її апаратної і програмної складових;

Р2 – Після завершення етапу верифікації та тестування програмної компоненти (компонент) системи;

Р3 – Після виконання інтеграційних тестів системи;

Р4 – Після виконання кваліфікаційних тестів системи;

Р5 – Після виконання підсумкових валідаційних тестів системи.

Основними контрольними очками (точками задіяння) метода в ході реалізації V-моделі життєвого циклу розроблення та верифікації і валідації продукту є наступні:

- необхідно прогнозно виконати оцінювання надійності та функційної безпечності системи після закінчення розроблення всіх специфікацій (системної, програмної та апаратної компонент). За умови не виконання вимог до надійності та функційної безпечності необхідно корегувати специфікації щодо архітектурних вимог тощо. Контрольна точка після етапу Software Requirements Specification;

- після розроблення програмного забезпечення і його тестування необхідно уточнити показники його надійності та далі їх використовувати для оцінювання та забезпечення рівня показників надійності та функційної безпечності системи. Контрольна точка після етапу Software Verification;

-в ході виконання етапу інтеграційного тестування (Integration), коли здійснюється перевірка архітектурних вимог, можливі ситуації прояву дефектів взаємодії апаратної та програмної компонент. Після цього етапу необхідно виконати контрольну перевірку (оцінювання) рівня показників надійності та функційної безпечності;

- заключними етапами уточнення шуканих показників є контрольні точки після виконання кваліфікаційних випробувань та валідаційних, коли методом функціональних тестів встановлюється відповідність розробленої системи всьому переліку системних вимог.

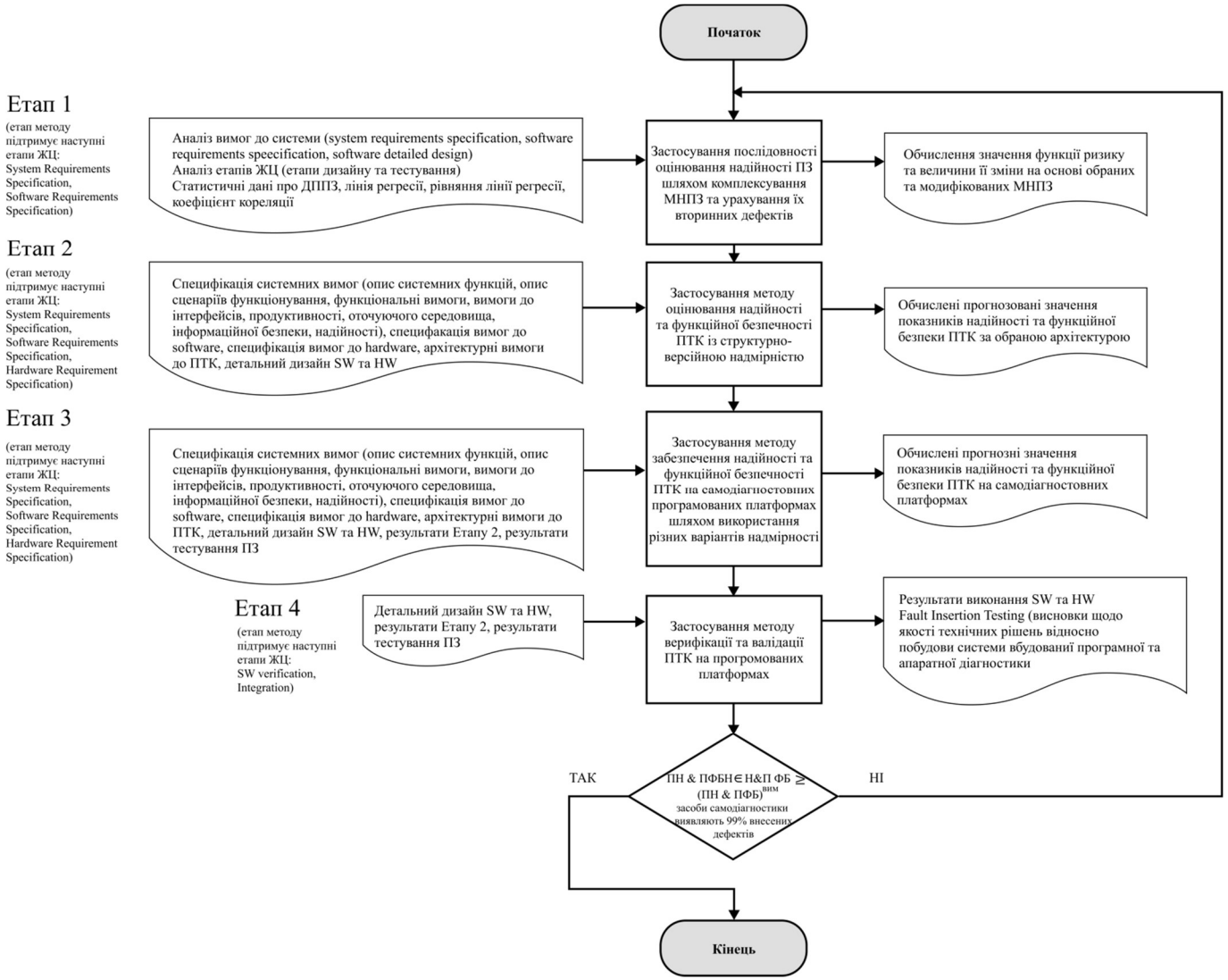


Рис. 6.14 Алгоритм метода оцінювання та забезпечення НіФБ ПТК при розробленні та ліцензуванні модулів і платформ для ІКС ПЛІС

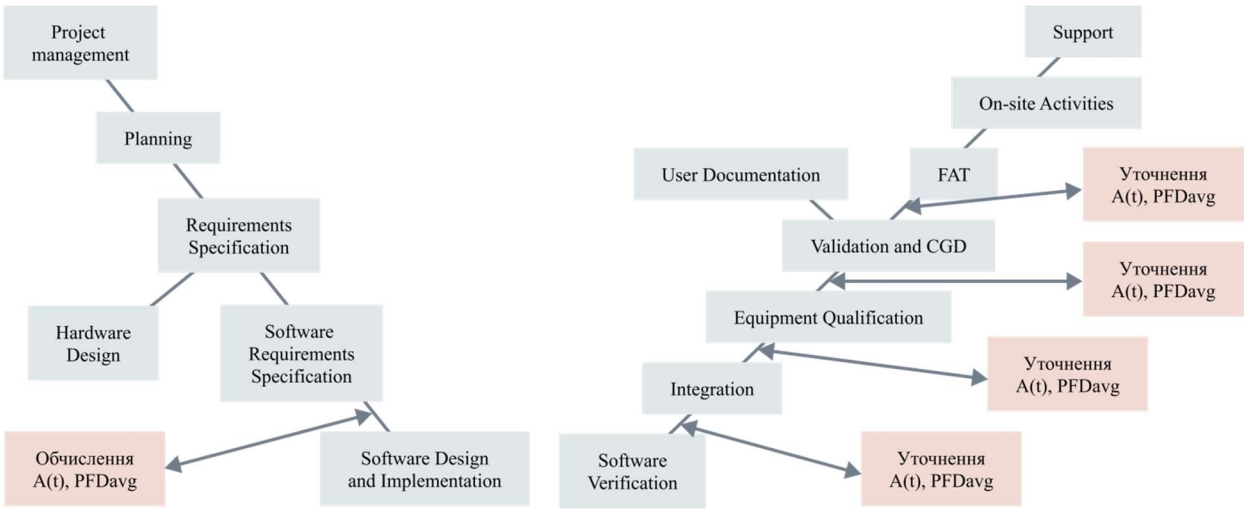
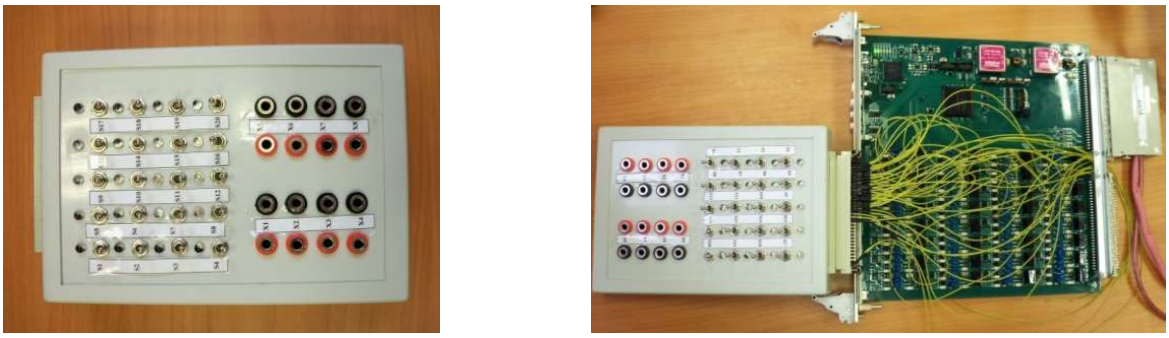


Рис. 6.15 Контрольні точки задіяння метода на V-моделі ЖЦ

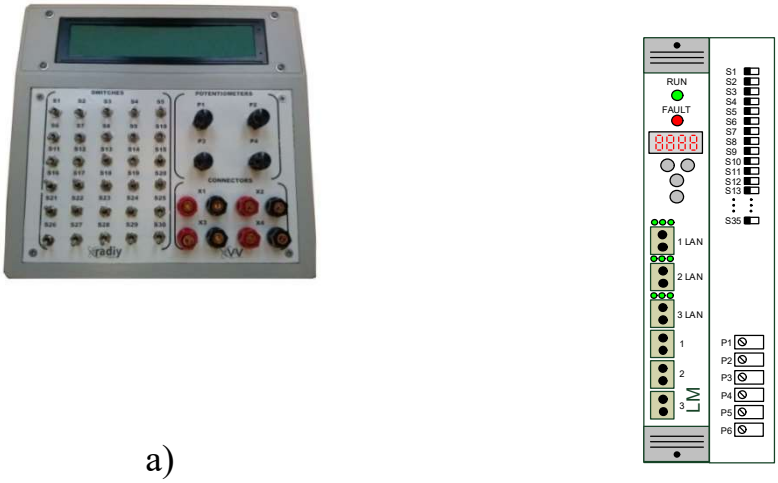
6.3 Інструментальні програмно-апаратні засоби підтримки виконання HW FIT

Прикладами апаратної підтримки виконання HW FIT є розроблені тестові панелі, які зазнали декілька етапів еволюції у відповідності до зростаючого функціоналу. Тестова панель (рис.6.16 а) дозволяє виконувати замикання окремих ланцюгів юнітів окремого модуля. Тестова панель (рис.6.17 а) додатково дозволяє виконувати тести з можливістю зміни електричних параметрів схеми (підвищення, зменшення опору). Панель (рис.6.17 б) за функціоналом співпадає але з V2.0 але монтується безпосередньо на модуль, що дозволяє виконувати тести для окремого модуля у складі повноцінно діючої платформи (разом з іншими модулями) та розширює можливості виконання Multi HW FIT. Де під Multi HW FIT розуміємо можливість одночасного внесення двох і більше дефектів.



а) б)

Рис. 6.16 а) тестова панель v1.0, б) тестова панель v1.0 під’єднана до модуля



а) б)

Рис. 6.17 а) тестова панель V2.0, б) тестова панель V3.0

Прикладами програмних засобів виконання SW FIT є наступні:

1. RPCT outputs Fault Insertion Tool (RFIT) – програмний засіб внесення дефектів.

Основними функціями RFIT є:

а) відкриття та аналіз вихідних файлів IDE RPCT;

б) редагування вмісту вихідних файлів RPCT тестувальником;

в) перерахунок контрольної суму CRC5 для команд, які редагуються;

г) перерахунок контрольної суми CRC64 для кадрів даних, які були відредаговані;

д) збереження вихідні файли RPCT, які містять внесені дефекти.

2. FOTIP Fault Insertion Tool (TFIT) – мережевий програмний засіб внесення дефектів

Основними функціями TFIT є:

а) мережева робота з компонентами платформи, які оснащені інтерфейсами LAN;

б) формування та надсилання в інтерфейси LAN кадрів пропрієтарного протоколу RUP, які містять вставлені дефекти;

3. Спеціальна програма тестування (Test Software program – TSP) розроблено за допомогою програмного забезпечення LabView. Основними функціями TSP є:

а) встановлення сигналів на вхідних модулях;

б) контроль сигналів на модулях виходів;

в) автоматичне створення звітів із архівуванням даних.

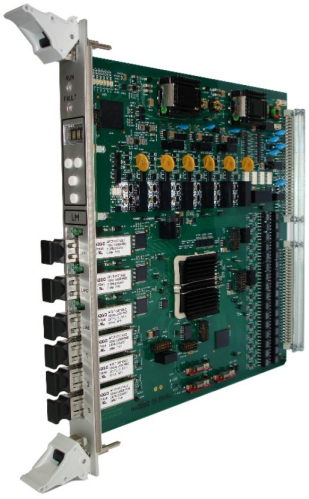
6.3.1 Застосування модифікованої процедури Hardware Fault Insertion Testing в ході ліцензування цифрової інформаційно-керуючої платформи RadICS

Модифіковану процедуру HW Fault Insertion Testing було застосовано в ході виконання етапу тестування з внесенням дефектів в ході ліцензування цифрової інформаційно-керуючої платформи RadICS розробки і виробництва ТОВ НВП Радій м. Кропивницький (Україна) на відповідність вимогам всіх частин стандарту IEC61508. Встановлено рівень функційної безпечності платформи за даним стандартом SIL-3 в одному каналі.

Мінімальна канальна конфігурація інформаційно-керуючих систем безпеки, заснованих на платформі RadICS, складається з 1 логічного каналу, який містить логічний модуль (Logic Module (LM)) (виконує функції логічної обробки, управління та діагностики), що покращує безпеку і надійність платформи, і до 14 інших модулів (вхідних / вихідних і оптичних зв'язків) в будь-який їх комбінації. Основний комплект типів вхідних / вихідних модулів

містить модуль аналогових входів (Analog Inputs Module (AIM)), модуль дискретних входів (Discrete Inputs Module (DIM)), модуль дискретних виходів (Discrete Outputs Module (DOM)) і модуль аналогових виходів (модуль управління силовими приводами) (Analog Outputs Module (AOM)). Також є вхідний модуль входу спеціального призначення для прийому сигналів з ультранизьким рівнем струмів - модуль вимірювання нейтронного потоку (Analog Inputs for (neutron) Flux Measure)). Модуль оптичного зв'язку може бути використаний для розширення систем до конфігурації, що включає в себе множину шасі. Крім того, можливе забезпечення міжканальних зв'язків між 2, 3 або 4 каналами ІКС за допомогою оптоволоконних зв'язків безпосередньо між логічним модулем або утворених за допомогою модулів оптичного зв'язку. Логічний модуль збирає вхідні дані від модулів входів відповідно до сконфігурованої користувачем логікою, оновлює величини керуючих сигналів для модулів виходів, збирає діагностичні дані і дані про загальний стан працездатності системи від всіх модулів входів / виходів і від другого логічного модуля, встановлених в тому ж шасі. Модулі входів / виходів забезпечують інтерфейси з іншими пристроями (наприклад, детекторами, сенсорами, приводами, пристроями сигналізації). Функціональність кожного модуля визначається логікою, запрограмованої в відповідної FPGA.

Рис. 6.18 Цифрова інформаційно-керуюча платформа RadICS



а) Логічний модуль (Logic Module (LM)

б) Модуль вимірювання нейтронного потоку (Analog Inputs for (neutron) Flux Measure)

в) Модуль вхідних дискретних сигналів Discrete Inputs Module (DIM)

г) Модуль вихідних дискретних сигналів Discrete Outputs Module (DOM)

д) Модуль вхідних аналогових сигналів Analog Inputs Module (AIM)

е) Модуль вихідних аналогових сигналів Analog Outputs Module (AOM)

Рис. 6.19 Ліцензовані модулі платформи RadICS за рівнем функційної безпечності SIL-3 (IEC 61508)

Етап 1. Виконання процедури FMEDA в повному обсязі.

Етап 2. Аналіз режиму відмови – визначення типів HW дефектів, які може бути фізично внесено до схеми (Means,mf_i), визначення точок на схемі, куди можуть бути внесені дефекти (Points, pf_i).

Приклад списку симптомів, які одержано в ході виконання FMEDA процедури наведено в таблиці А.1

Значення стовбців таблиці наступне:

FIT ID – ідентифікатор тесту.

Test descriptor detectable symptom – режим відмови, який має бути перевіреним.

Chassis config'n – модуль, який має бути протестованим.

Insertion required – ідентифікатор, який визначає, чи буде модуль модифіковано.

Module's mode – режим роботи модуля під час виконання тесту.

Modified module – ідентифікатор, який вказує на можливу зміну продуктивності модуля.

Mod'd vhdl – ідентифікатор вказує на те, що модифікація VHDL модуля потрібна для запуску несправності для певного фізичного стану.

Auto'd test – ідентифікатор режиму тестування (ручний чи автоматичний)

Для визначених режимів відмови заповнюється таблиця імплементованого простору покриття для схеми (Implemented FIT covered space of scheme (IFCS)).

Визначаємо функцію покриття із аналізу таблиці:

$$\begin{gathered} \Phi = (p3m11 \vee p4m11 \vee p6m12) \wedge (p1m21 \vee p2m21 \vee p5m22) \wedge \\ (p9m31 \vee p7m32) \wedge (p10m41 \vee p8m42) = p3m11 \wedge p1m21 \wedge p9m31 \wedge \\ p10m41 \vee p4m11 \wedge p1m21 \wedge p9m31\, p10m41 \vee p6m12 \vee p1m21 \wedge p9m31 \\ \wedge p10m41 \vee \ldots \vee p6m12 \vee p5m22 \wedge p7m32 \wedge p8m42 \end{gathered} \tag{6.17}$$

Таблиця 6.10

Фрагмент списку симптомів для перевірки в ході виконання HW FIT модуля DIM платформи RadICS

Test Case RID	Unit	Test descriptor detectable symptom	Chassis config'n	Insertion required	IT	Module's MODE	Modified module	Mod'd vhdl	Auto'd Test
FIT.DIM.13	PS	IO.PS 3.3v lost.	DIM	inc.R	1	RUN, STARTUP	mod. H/W	std VHDL	manual
FIT.DIM.18	PS	IO.PS VCCA 2.5v lost.	DIM	open cct	1	RUN, STARTUP	mod. H/W	std VHDL	manual
FIT.DIM.21	PS	IO.PS 2.5v BANK5 lost	DIM	open cct	1	RUN, STARTUP	mod. H/W	std VHDL	manual
FIT.DIM.24	PS	IO.PS VCCINT 1.2v lost	DIM	inc.R	1	RUN, STARTUP	mod. H/W	std VHDL	manual

Таблиця 6.11

Таблиця імплементованого простору покриття для визначених дефектів (режимів відмов), які потрібно перевірити в ході FIT

Дефекти, f_i	**Значення імплементації дефектів, m_{ij}**	**Точки імплементації дефектів, Ipf_i**									
		Ipf_1	**Ipf_2**	**Ipf_3**	**Ipf_4**	**Ipf_5**	**Ipf_6**	**Ipf_7**	**Ipf_8**	**Ipf_9**	**Ipf_{10}**
f_2, PS.2,5v BANKS lost	m_{11}, stuck off	0	0	1	1	0	0	0	0	0	0
	m_{12}, out&GND	0	0	0	0	0	1	0	0	0	0
f_3 , PS.2,5v VCCA lost	m_{21}, stuck off	1	1	0	0	0	0	0	0	0	0
	m_{22}, out&GND	0	0	0	0	1	0	1	0	0	0
f_4, PS.1,2v VCCINT lost	m_{31}, stuck off	0	0	0	0	0	0	0	0	1	0
	m_{32}, out&GND	0	0	0	0	0	0	1	0	0	0
f_5, PS.3,3v BANKS lost	m_{41}, stuck off	0	0	0	0	0	0	0	0	0	1
	m_{42}, out&GND	0	0	0	0	0	0	0	1	0	0

Маємо 36 варіантів внесення дефектів:

irIFCS = {irIFCS$_1$={(p_3, m_{11}),(p_1, m_{21}),(p_9, m_{31}),(p_{10}, m_{41})},…, irIFCS$_{36}$={(p_6, m_{12}),(p_5, m_{22}),(p_7, m_{32}),(p_8, m_{42})}}.

Етап 3. Розробка спеціалізованих інструментів для реалізації HW FIT.

Внесення дефектів (що реалізують визначені до тестування симптоми (режими відмов) здійснюється методом впаювання в окремі ланцюги вузлів (юнітів) модулів. Місця впаювання відповідно визначаються на етапі 2 виконання процедури.

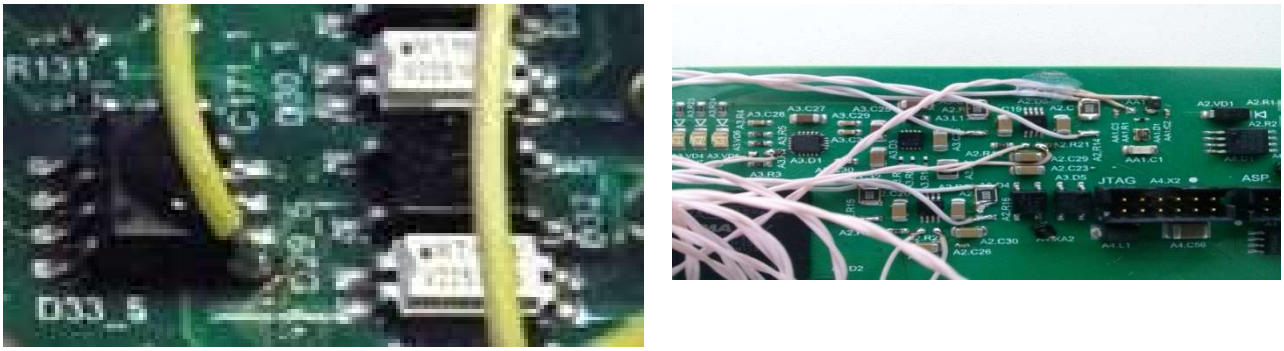


Рис. 6.20 Фото з прикладами впаювання дефектів в окремі ланцюги модулів

Місця впаювання з’єднуються проводами з входами спеціально розроблених тестових пристроїв внесення дефектів (тестових панелей).

Основний функціонал тестових панелей наступний:

- втрата живлення модуля або окремих його вузлів. Реалізація таких тестових випадків проводиться шляхом впайкі тумблерів, які розмикають відповідні ланцюги. Особливістю здійснення даних тестів є те, що цілісність плати не порушується, і модуль повертається в початковий стан шляхом замикання ланцюга тумблером;
- збільшення / зменшення рівня напруги в ланцюгах блоків живлення модулів. Для реалізації даних тестів виконується впаювання провідників до відповідних точки ланцюга і виведення їх на вхідні інтерфейси тестової панелі (рисуноки6.21, 6.22). До тестової панелі підключається зовнішнє джерело живлення для відтворення, а потім зміни напруги живлення в ланцюзі. За допомогою прецизійного джерела напруга живлення змінюється (збільшується

або зменшується) і при досягненні граничних значень система діагностики модуля повинна виявити факт виникнення дефекту;

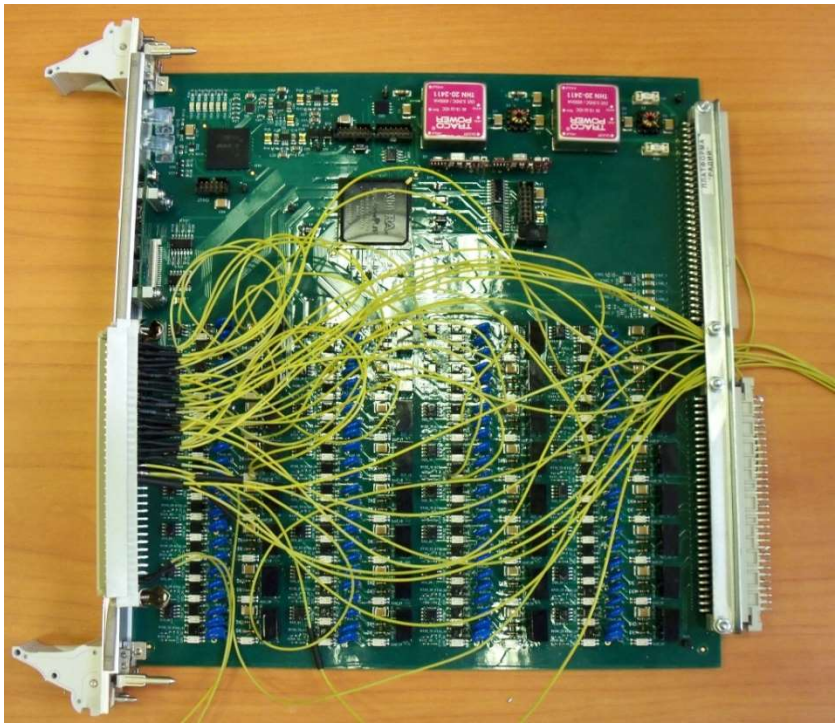


Рис 6.21 Модуль DIM з внесеними HW дефектами

Рис. 6.22 Тестова панель V2.0 під’єднана до модуля DIM

- порушення (втрата) сигналів синхронізації в ланцюгах мікросхем FPGA і блоку живлення. Реалізацію даних дефектів необхідно проводити шляхом відключення живлення на кварцових генераторах відповідних ланцюгів. Відключення живлення проводиться тумблером на тестовій панелі;
- «залипання» логічного «0» або «1».Оскільки, наприклад, цифрова оптопара фізично «залипнути» (в стійке положення логічного «0» або «1») не може, здійснюється імітація даного процесу шляхом примусового встановлення рівня логічного «0» або «1» в необхідних ланцюгах схем модуля . Установка сигналів в «0» або «1» реалізується за допомогою тумблерів, замикаючих певні лінії проходження сигналів на «землю».

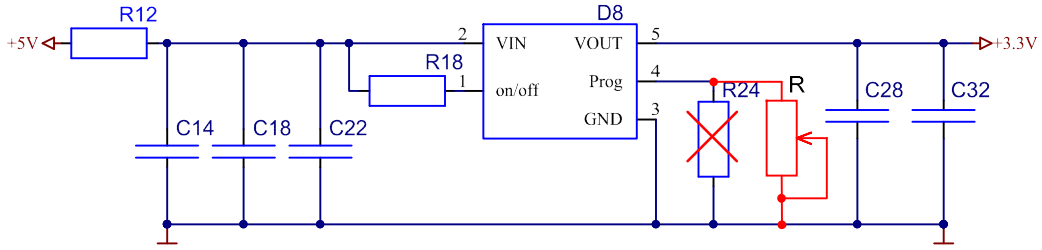
Етап 4. Розроблення специфікації тестів. До складу специфікації має бути включено весь встановлений та визначений до тестування перелік дефектів (симптомів). Симптоми визначено на етапі FMEDA. Опис окремого тесту має назву тест-кейса (Test Case). Кожний Test Case включає наступну інформацію:

- Розділи, які чітко ідентифікують даний Test Case (Test Case ID);
- опис тесту (вхідні дані) (Test Case Description);
- Склад, конфігурацію обладняння для виконання даного тесту (Test Bench);
- дата розроблення тесту та прізвище розробника із складу групи тестувальників (Test Designed by, Test Designed date);
- - опис будь-яких початкових умов і / або вимог (при необхідності наводиться опис будь-яких спеціальних обмежень на процес тестування (Requirements are related to the test, Pre-conditions);
- покрокова інструкція по виконанню кожного теста (Test Case Steps);
- розділ, в якому описано результат, що очикується (Expected result);
- умови завершення тесту.

В таблиці 6.12 наведено приклад опису Test Case FIT.DIM.13, із складу тест-кейсів специфікації тестів HW FIT модуля DIM ЦІКП RadICS виробництва ТОВ «НВП «Радій» м.Кропивницький.

Таблиця 6.12

Опис тест-кейсу FIT.DIM.13

Test Case RID	FIT.DIM.13	**Test Case TID**	DIM.13.01
Test Case TN	[IO.PS 3.3v Low]		
Test Case description	Test: IO.PS 3.3v Low Tracing: D7.24.X		
Test Designed by		**Test Designed date**	
SUT Configuration	SUT.DIM.01	**TB Configuration**	TB.01
Requirements are related to the test			
DIM ED DD	DIM_ED.01, DIM_ED.02, DIM_ED.03		
PSWD ED DD	PSWD_ED.01, PSWD_ED.02, PSWD_ED.04.		
FBL DD	DDC.04, DDC.05, DDC.07, IBUC.01, IBUC.02, IBUC.03, IBUC.04, IBUC.04a, IBUC.04b.		
Test			
Pre-conditions	1. Replace the resistor A2.R24 by the potentiometer R 5 kOhm (Figure DIM.13.01.01). 2. Activate SUT (DIM in the RUN mode). 3. Activate TB (MATS and NI equipment with LabVIEW). 4. FIT control panel for DIM is set in accordance with Appendix B.		
 Figure DIM.13.01.01 – Symptom realization			
Test Case Steps	1. No fault. Register state of all I/O modules in Chassis using LabVIEW software and MATS. 2. Insert fault (change the resistance of R from initial value of A2.R24 to +10%). Register state of all I/O modules in Chassis using LabVIEW software and MATS. 3. Check the state of DIM. Register the error code/codes on the IBU/PSWD LEDs of DIM (if it/they exist). 4. Register the error code/codes on the IBU of LM (if it/they exist). 5. Check if changing the normal command signal leads to output following the commands (if it is applicable). 6. Check commands (SOR) that will try to put the channel into the safe state (if it is applicable). 7. Check the accuracy of border value. 8. Remove fault (change the resistance of R to initial value of A2.R24). Register state of all I/O modules in Chassis using LabVIEW software and MATS.		

Продовження таблиці 6.12

Expected results	1. DIM is in FAULTED MODE (LED FAULT is ON, LED RUN is OFF). 2. Expected DIM's PSWD LED binary code: 001000. 3. Expected DIM's IBU code/codes: #006. 4. Expected border value not less than 3.135 VDC. 5. Expected LM's IBU code/codes: lost communication with module, which installed in appropriate slot. 6. Platform forces the safe state (DOs and AOs are in RUN SAFE).
Post-conditions	Module was returned to the initial state after testing (DIM in the RUN mode).
Note	Fault was detected in accordance with DIM ED DD, PSWD ED DD and FBL DD.

Етап 5. Покрокове виконання та документування результатів тестування. Склад таблиць звіту викоанання тестів наступний:

- Розділи, які чітко ідентифікують даний Test Case (Test Case ID);
- опис тесту (вхідні дані) (Test Case Description);
- Склад, конфігурацію обладняння для виконання даного тесту (Test Bench);
- дата виконання тесту та склад групи тестувальників (Date of test execution, Names of testers);
- результати покрокового виконання тестів;
- розділ, в якому описано результат, що очикується (Expected result);
- розділ, в якому зафіксовано одержаний результат (Actual result);
- висновок щодо одержаного результату (Pass/Fail). Висновок Fail встановлюється у випадку коли результат одержаний не співпадає з очикуваним;
- критерій приймання теста (Acceptance criterion);
- розділ опису встановленої аномалії (Summary of all test anomalies);
- розділи реакції розробників на встановлену аномалію (Justification from designer) та висновок верифікатора про результати усунення аномалії (Justification from verifier).

Частина звіту про виконання HW FIT модуля DIM платформи RadICS

наведено в таблиці 6.13.

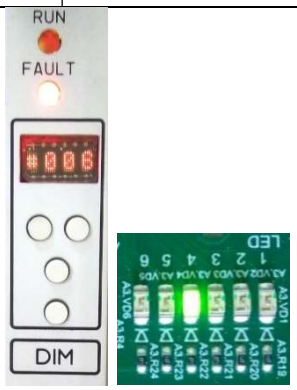
Таблиця 6.13

Звіт виконання тест-кейсу FIT.DIM.13

Test Case RID	FIT.DIM.13	**Test Case TID**	DIM.13.01
Test Case TN	[IO.PS 3.3v Low]		
Test Case description	Test: IO.PS 3.3v Low Tracing: D7.24.X		
Date of test execution		**Names of testers**	
SUT Configuration	SUT.DIM.01	**TB Configuration**	TB.01

No Fault [Step 1, 7]				
Expected result		**Actual result**		**Pass/Fail**
LM#1	RUN	**LM#1**	RUN	Pass
DIM#1	RUN	**DIM#1**	RUN	Pass
DOM#1	RUN	**DOM#1**	RUN	Pass
AIM#1	RUN	**AIM#1**	RUN	Pass
AOM#1	RUN	**AOM#1**	RUN	Pass
OCM#1	RUN	**OCM#1**	RUN	Pass
LM#2	RUN	**LM#2**	RUN	Pass
OCM#2	RUN	**OCM#2**	RUN	Pass
DOUs of DOM#1	In accordance with UAL	**DOUs of DOM#1**	In accordance with UAL (See	Pass
DACUs of AOM#1	In accordance with UAL	**DACUs of AOM#1**	In accordance with UAL (See)	Pass
DOUs of LM#1	In accordance with UAL	**DOUs of LM#1**	In accordance with UAL (See	Pass
Fault was inserted [Step 2, 6]				
Expected result		**Actual result**		**Pass/Fail**
LM#1	RUNS	**LM#1**	RUNS	Pass
DIM#1	FAULTED	**DIM#1**	FAULTED	Pass
DOM#1	RUNS	**DOM#1**	RUNS	Pass
AIM#1	RUN	**AIM#1**	RUN	Pass
AOM#1	RUNS	**AOM#1**	RUNS	Pass
OCM#1	RUN	**OCM#1**	RUN	Pass
LM#2	RUN	**LM#2**	RUN	Pass
OCM#2	RUN	**OCM#2**	RUN	Pass
DOUs of DOM#1	Open	**DOUs of DOM#1**	Open (See)	Pass

Продовження таблиці 6.13

DACUs of AOM#1	0 VDC / 0 mA	**DACUs of AOM#1**	0 VDC / 0 mA (See)	Pass
DOUs of LM#1	Open	**DOUs of LM#1**	Open (See)	Pass
DIM state [Step 3] (See Figure FIT.DIM.13.01.01)				
Expected result		**Actual result**		**Pass/Fail**
LED "RUN"	OFF	**LED "RUN"**	OFF	Pass
LED "FAULT"	ON	**LED "FAULT"**	ON	Pass
PSWD LEDs	001000	**PSWD LEDs**	001000	Pass
IBU state	#006	**IBU state**	#006	Pass
 Figure FIT.DIM.13.01.01				
LM state [Step 4] (See Figure FIT.DIM.13.01.02)				
Expected result		**Actual result**		**Pass/Fail**
LED "RUN"	ON	**LED "RUN"**	ON	Pass
LED "FAULT"	Flashing	**LED "FAULT"**	Flashing	Pass
IBU state	#014	**IBU state**	#014	Pass
 Figure FIT.DIM.13.01.02				
DIM border value [Step 5] (Checking of low level of 3.3 VDC of PSWD (x =3.3 VDC))				
Expected result		**Actual result**		**Pass/ Fail**
Inaccuracy x±(VDC)	**Code of errors on IBU**	**Inaccuracy x±(VDC)**	**Code of errors on IBU**	

Продовження таблиці 6.13

x-0.000	No error	x-0.000	No error	Pass
x-0.033	No error	x-0.033	No error	Pass
x-0.066	No error	x-0.066	No error	Pass
x-0.099	No error	x-0.099	No error	Pass
x-0.132	No error	x-0.132	No error	Pass
x-0.135	No error	x-0.135	No error	Pass
x-0.138	No error	x-0.138	No error	Pass
x-0.141	No error	x-0.141	No error	Pass
x-0.145	No error	x-0.145	No error	Pass
x-0.148	No error	x-0.148	#006	Pass
x-0.151	No error	x-0.151	#006	Pass
x-0.155	No error	x-0.155	#006	Pass
x-0.158	No error	x-0.158	#006	Pass
x-0.161	No error	x-0.161	#006	Pass
x-0.165	#006	x-0.165	#006	Pass
Border value				
Expected result		**Actual result**		**Pass/ Fail**
Not less than (VDC)	3.135	**Not less than (VDC)**	3.155	Pass
Acceptance criterion	1. "Pass" – when all values from expected result is equal all values from actual result; 2. Test successful when all values are Pass. Else – test unsuccessful.			
Summary of Test Results (Pass/Fail)	Test successfully PASSED.			
Summary of all test anomalies and the CRs raised	Anomalies are not detected.			
Justification unresolved bugs				
Justification from designer		Justification from verifier		

Таким чином маємо загальний алгоритм виконання процедури HW FIT

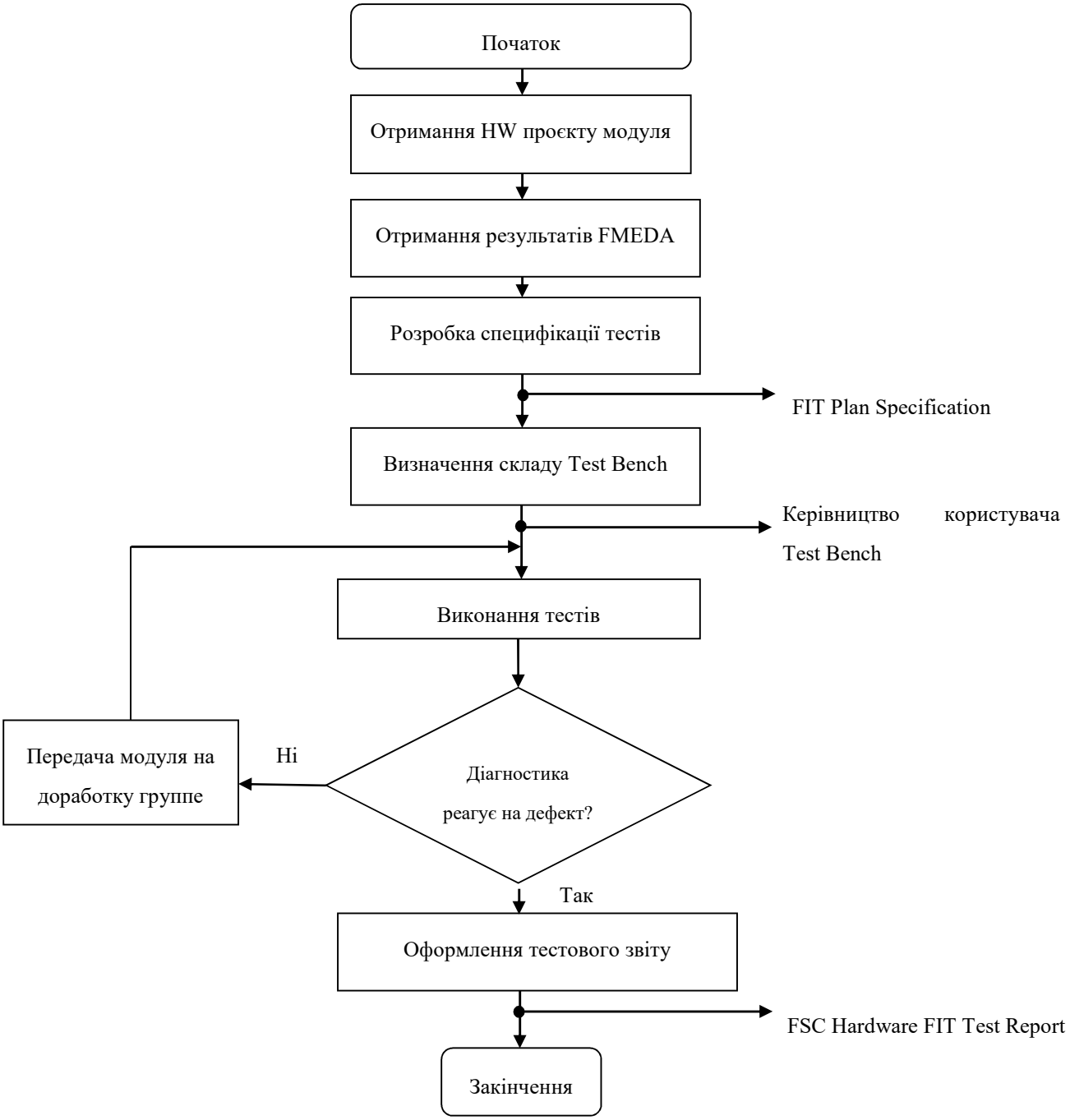


Рис. 6.23 Загальний алгоритм виконання HW Fault Insertion Testing

6.3.2 Застосування модифікованої процедури Software Fault Insertion Testing в ході ліцензування цифрової інформаційно-керуючої платформи RadICS

Застосування модифікованої процедури SW Fault Insertion Testing в ході ліцензування ЦІУП RadICS складається із наступних етапів.

Етап 1. Формування вихідних даних для виконання FMEA. Прикладом таких даних є:

- типи даних, які застосовуються: блок User Application Logic (UAL) подає вхідні дані, очікувані як FP32 (Float point 32), але які насправді є SI32 (Signed Integer 32), або навпаки, де UAL – користувацька логіка, що розробляється. Значення SI32 може бути інтерпретовано блоком як «денормалізоване значення», + ∞, + ∞, NaN (немов прийшли дані в FP32). Оскільки SI32 і FP32 мають однакову довжину, в онлайн-системі немає вбудованої захисту для виявлення неправильного з'єднання, і така умова потенційно небезпечна і для безпеки непередбачувана.
- Loopbacks: блок UAL може отримати дані від блоку, який повинен виконуватися після нього (петля).
- Елементи AFB (Application Fanction Block) і компоненти AFB: дизайнер UAL бачить один об'єкт в RPCT і отже IDE повинна правильно встановити параметр, який використовується компонентом для виконання операції, необхідної конкретним елементом. Помилки тут можуть бути результатом помилок в описах XML-елементів AFB або в коді підсумкового BUILDa UAL - проєкту. Помилка може привести до виконання UAL не специфікованої функції (наприклад, компонент MATH виконує ADD замість SUBTRACT), та інш.

Етап 2. Виконання FMEA аналізу та складання таблиці.

Таблиця 6.13

FMEA (Failure Mode Effect Analysis)

FMEA ID	Режим відмови програмного компоненту	Очикуване проявлення під час тестування	Вимоги до тесту	Критичність відмови (вплив на роботу системи)	Вплив відмови на безпеку	Необхідні дії щодо пом'якшення наслідків

Приклад такої таблиці в ході тестування програмних компонент IDE RPCT платформи RadICS (таблиця 6.14).

Таблиця 6.14

RPCT BUILD/UPLOAD FMEA

FMEA ID	Type of failure	Expected Detection during Normal Development Testing	Development Testing Required	Detection during Normal Use	Impact on PLC and Safety	Mitigation Action Required
RUF.01.1	Creates a command call to the wrong kind of block, but block type is valid to the UAL controller	May be blocked by the "compiler" if the argument list structure is different. Would be detected by a test of all AFB items (checking use on a schema to upload file).	Integrated test from items on a schema to the M1 tool output covering all blocks.	Subtle errors may not be detected.	This is potentially dangerous.	Use independent tool to generate an EU-readable assembly listing 1:1 with the upload file(s), and require the EU to review it for safety projects.

Етап 3. Формування множин дефектів у відповідності до кількості компонент IDE і побудова таблиці відповідності типу дефекту програмній компоненті.

Таблиця 6.15

Таблиця відповідності типу дефекту програмній компоненті

Типи дефектів, f_i	SW Components		
	SW Com_1	…..	SW Com_M
f_1	+		+
…			+
f_F	+		

Етап 4. Технологічна інтерпретація відмов на основі FMEA та визначення

точок і засобів внесення дефектів

Таблиця 6.16

Таблиця відповідності підмножин дефектів SW атрибутам внесення SW дефектів (точкам внесення та значенням внесення)

Підмножина дефектів SW компоненти, f_i	Атрибути внесення SW дефектів	
	Точки внесення, pf_i	Значення, mf_i
f_1	pf_1	mf_1
…	…	…
f_z	pf_j	mf_F

Приклад реалізації наведено в таблиці 6.19 для FMEA ID RUF.01.1 таблиці 6. (Creates a command call to the wrong kind of block, but block type is valid to the UAL controller - створити виклик команди для неправильного типу блоку, але тип блоку є дійсним для ПЛК).

Для того, щоб внести визначену підмножену дефектів $\mathbf{fsw_1}$ із значенням Imf_{ij} у обрані точки (Ipfi), розробник тестів повинен виконати наступне:

а) визначити в даних UAL точку вставки дефекту (певна команда та певне поле даних у команді).

б) змінити вірне значення даних на невірне.

с) перерахувати і змінити контрольні суми, що захищають дані UAL від пошкодження.

У таблиці 6.19 показано застосування вищеописаних етапів для розглянутого прикладу.

Таблиця 6.17

Таблиця відповідності підмножини дефектів fsw_1 атрибутам внесення SW дефектів (точкам внесення - Ipf_1 та значенням внесення - Imf_{11})

Subset types of failure, fsw_i	Points, Ipf_i	Means, Imf_{ij}
fsw_1 Logic AFB was configured to perform a wrong function	**Ipf_1** Function code field within assembler command	**Imf_{11}** Function code is WRONG and INVALID: - Function Code ≠ Function Code specified in the UAL project - Function Code is out of the legal range - Function Code = 4
		Imf_{12} Function code is WRONG and INVALID: - Function Code ≠ Function Code specified in the UAL project - Function Code is out of the legal range - Function Code = 0
		Imf_{13} Function code is WRONG but VALID: - Function Code ≠ Function Code that was specified in the UAL project - Function Code is within the legal range [1..3] - Function Code = 2 instead of 1 (OR instead of AND)

Таблиця 6.18

Значення дефектів, що вносяться у поле даних UAL

	Hex Code	Mnemocode
Init. command	128100020001	WRFBC LB.0, **funct_code <= 1**
Imf_{11}	AA8100020004	WRFBC LB.0, **funct_code <= 4**
Imf_{12}	D28100020000	WRFBC LB.0, **funct_code <= 0**
Imf_{13}	7A8100020002	WRFBC LB.0, **funct_code <= 2**

Етап 5. Розробка при необхідності спеціалізованого ПЗ для виконання SW тестів.

Етап 6. Планування тестів (розробка плана та специфікації тестів). Фрагмент планової таблиці проведення SW FIT IDE RPCT складової платформи RadICS наведено таблицею 6.19.

Таблиця 6.19

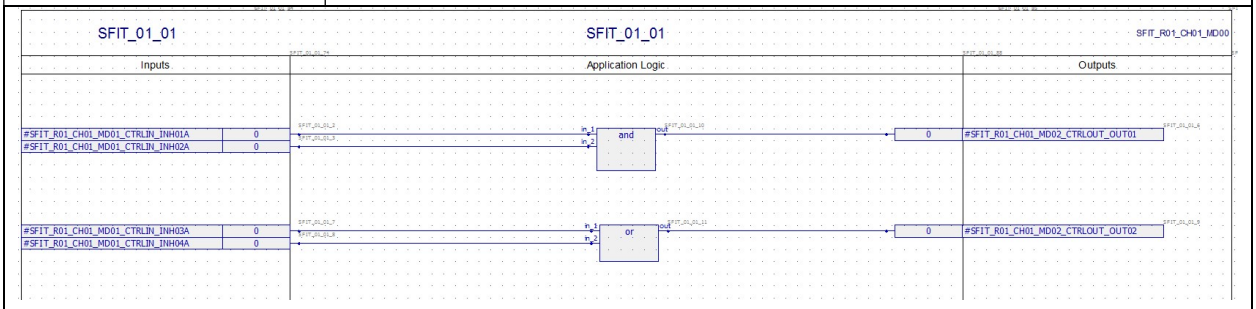
Фрагмент планової таблиці плана проведення SW FIT IDE RPCT складової платформи RadICS

[T/RUF]	Test descriptor	[T\SFIT]	Test description	FIT technique	Component	TD techniques	FSC mode	System Under Test	Test Bed	Note
RUF.01.1	Creates a command call to the wrong kind of command, block or block implementation, but command number, block type or implementation number is valid to the UAL controller. [/]	SFIT.01	To test SUT behavior if Command Parameters are WRONG but VALID for UAL Controller or particular UAL project. [/]	FITT.01	BTS	PWT.01	RUN	SUT.SFIT.01	STB.01	11 test cases.

Таблиця 6.20

Фрагмент специфікації SW FIT

Test Case RID	SFIT.01	**Test Case TID**	SFIT.01.01
Test Case TN	[Test valid but wrong command code, RDFBB <= WRFBB]		
Test Case description	To test SUT behavior if Command code is WRONG but VALID for UAL Controller. Command length is EQUAL to the correct command length. Correct Command Code = RDFBB (12) Inserted Command Code = WRFBB (11)		
SUT Configuration	SUT.SFIT.01	**TB Configuration**	STB.01
Test Case UAL	SFIT_01 (see Appendix C)		
Test Case was Designed by		**Test Case design version and date**	V1R0 December 19, 2017
Test Case was Changed by		**Test Case design version and date**	V1R1 July 11, 2018
Pre-condition preparation, initial data, setup	1. Perform static analysis of the UAL project SFIT_01_PART2 by ROVT. 2. Upload to the LM#1 configuration file of the UAL project SFIT_01_PART2 (Figure SFIT.01.01 shows fragments of the ALS diagram (a), SFIT.01 BTS before (b) and after (c) error seeding). 3. Set LM#1 jumpers configuration as (HEX): 0x6141. 4. Activate SUT. 5. Reset SOR to LM and all output modules. 6. All modules in Chassis#1 are in RUN mode.		



a) SFIT.01.01 ALS


```
{
  "bts_before_error_seeding": [
            {
      "z_description_channel_01": {
        "desc00000085":          "1;true;00C9;4B010014B4030001;RDFBB                                    46083[1],
OR.0[20];#SFIT_R01_CH01_MD02_CTRLOUT_OUT02 <= or.out"
```

Продовження таблиці 6.20


```
        },
        "z_frame_0003": {
          "data0000": "f440 00b7 0180 b400 ffff 5341 0016 00cf b600 b400 0000 cb42 0003 0067 7600 b400",
          "data0010": "0001 5b43 000e 00d0 1e00 b400 0002 7b44 0009 006a de00 b400 0003 7345 000b 006a",
          "data0020": "ce00 b400 0004 f346 0015 006b 0e00 b400 0005 bb47 0005 0068 6600 b400 0006 7b48",
          "data0030": "0026 0067 a600 b400 0007 2349 0025 0067 4600 b400 0008 bb4a 000c 006f 8600 b400",
          "data0040": "0009 334b 0015 0070 ee00 b400 000a 2b4d 000e 0068 3e00 b400 000c 134e 0010 006c",
          "data0050": "fe00 b400 000d 8b50 000d 0003 5600 b400 000f b100 e1b8 b400 0180 b400 ffff 1351",
          "data0060": "001d 0006 b600 b400 0000 cb54 0010 0005 de00 b400 0003 4355 0008 0001 ce00 b400",
          "data0070": "0004 b356 000f 0004 0e00 b400 0005 2357 000e 0007 6600 b400 0006 c359 001f 0003",
          "data0080": "4600 b400 0008 335a 001c 0005 8600 b400 0009 2b5b 0016 0004 ee00 b400 000a 135c",
          "data0090": "000b 0000 2e00 b400 000b e100 e1b9 b400 0180 b400 ffff 1100 e1ba b400 0180 b400",
          "data00a0": "ffff 4100 e1bb b400 aa81 0040 0002 9281 0041 0001 6281 0042 0001 da81 0000 0002",
          "data00b0": "e281 0001 0001 7a81 0002 0002 60c0 61c0 b402 0000 0000 89c0 b402 0001 0001 9ac1",
          "data00c0": "0003 0076 0002 2ac1 0004 0076 0003 7881 0000 4b01 0014 b403 0001 bac1 0043 0076",
          "data00d0": "0000 0ac1 0044 0076 0001 0881 0040 1301 0054 b403 0000 7180 b400 0000 5bc0 b400",
          "data00e0": "0075 0000 93c0 b400 0075 0101 e3c0 b400 0075 0202 2bc0 b400 0075 0303 cbc0 b400",
          "data00f0": "0076 0400 03c0 b400 0076 0501 73c0 b400 0076 0602 bbc0 b400 0076 0703 03c0 b400",
          "data0100": "0a75 0800 cbc0 b400 0a75 0901 f100 d2c4 b400 5140 d2c5 b403 0001 7180 b400 0000",
          "data0110": "e3c0 b400 b403 0000 2bc0 b400 b403 0101 2900 0a00 b400 a180 e1b6 0000 60c0 0000",
          "data01f0": "0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 b3f1 a164 cfca 7949",
          "frameIndex": 3
        }
      }
        ],
    "bts_after_error_seeding": [
            {
        "z_description_channel_01": {
          "desc00000085":          "1;true;00C9;22C10014B4030001;WRFBB                                                    46083[1],
OR.0[20];#SFIT_R01_CH01_MD02_CTRLOUT_OUT02 <= or.out"
        },
        "z_frame_0003": {
          "data0000": "f440 00b7 0180 b400 ffff 5341 0016 00cf b600 b400 0000 cb42 0003 0067 7600 b400",
          "data0010": "0001 5b43 000e 00d0 1e00 b400 0002 7b44 0009 006a de00 b400 0003 7345 000b 006a",
          "data0020": "ce00 b400 0004 f346 0015 006b 0e00 b400 0005 bb47 0005 0068 6600 b400 0006 7b48",
          "data0030": "0026 0067 a600 b400 0007 2349 0025 0067 4600 b400 0008 bb4a 000c 006f 8600 b400",
          "data0040": "0009 334b 0015 0070 ee00 b400 000a 2b4d 000e 0068 3e00 b400 000c 134e 0010 006c",
          "data0050": "fe00 b400 000d 8b50 000d 0003 5600 b400 000f b100 e1b8 b400 0180 b400 ffff 1351",
          "data0060": "001d 0006 b600 b400 0000 cb54 0010 0005 de00 b400 0003 4355 0008 0001 ce00 b400",
```

Продовження таблиці 6.20


```
        "data0070": "0004 b356 000f 0004 0e00 b400 0005 2357 000e 0007 6600 b400 0006 c359 001f 0003",
        "data0080": "4600 b400 0008 335a 001c 0005 8600 b400 0009 2b5b 0016 0004 ee00 b400 000a 135c",
        "data0090": "000b 0000 2e00 b400 000b e100 e1b9 b400 0180 b400 ffff 1100 e1ba b400 0180 b400",
        "data00a0": "ffff 4100 e1bb b400 aa81 0040 0002 9281 0041 0001 6281 0042 0001 da81 0000 0002",
        "data00b0": "e281 0001 0001 7a81 0002 0002 60c0 61c0 b402 0000 0000 89c0 b402 0001 0001 9ac1",
        "data00c0": "0003 0076 0002 2ac1 0004 0076 0003 7881 0000 22c1 0014 b403 0001 bac1 0043 0076",
        "data00d0": "0000 0ac1 0044 0076 0001 0881 0040 1301 0054 b403 0000 7180 b400 0000 5bc0 b400",
        "data00e0": "0075 0000 93c0 b400 0075 0101 e3c0 b400 0075 0202 2bc0 b400 0075 0303 cbc0 b400",
        "data00f0": "0076 0400 03c0 b400 0076 0501 73c0 b400 0076 0602 bbc0 b400 0076 0703 03c0 b400",
        "data0100": "0a75 0800 cbc0 b400 0a75 0901 f100 d2c4 b400 5140 d2c5 b403 0001 7180 b400 0000",
        "data0110": "e3c0 b400 b403 0000 2bc0 b400 b403 0101 2900 0a00 b400 a180 e1b6 0000 60c0 0000",
        "data01f0": "0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 bc93 4c82 6440 519c",
        "frameIndex": 3
      }
    }
  ]
}
```


Figure SFIT.01.01 – Error Seeding Implementation

Test Case Steps

1. Perform review of ROVT reports.
2. Register state of all modules in Chassis#1.
3. Set the following sequence of input signals and check output signals for each input signals combination.

Module	Signal	[Step 3.1]	[Step 3.2]	[Step 3.3]
DIM#1	*INH01A	1	1	1
DIM#1	*INH02A	1	1	1
DIM#1	*INH03A	0	1	1
DIM#1	*INH04A	0	0	1
DOM#1	*OUT01			
DOM#1	*OUT02			

Продовження таблиці 6.20

<table>
<tr><td>Expected results</td><td>1. [Step 1]. Expected ROVT message: ROVT shall report an ERROR - the wrong MD5 checksum of LM#1 BTS file.
2. [Step 2]. All modules in Chassis#1 are in RUN MODE.
3. [Step 3]
<table>
<tr><td>Module</td><td>Signal</td><td>[Step 3.1]</td><td>[Step 3.2]</td><td>[Step 3.3]</td></tr>
<tr><td>DIM#1</td><td>*INH01A</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>DIM#1</td><td>*INH02A</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>DIM#1</td><td>*INH03A</td><td>0</td><td>1</td><td>1</td></tr>
<tr><td>DIM#1</td><td>*INH04A</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td>DOM#1</td><td>*OUT01</td><td>1</td><td>1</td><td>1</td></tr>
<tr><td>DOM#1</td><td>*OUT02</td><td>0</td><td>0</td><td>0</td></tr>
</table></td></tr>
<tr><td>Post-conditions</td><td>-</td></tr>
<tr><td>Note</td><td></td></tr>
</table>

Етап 7. Виконання SW FIT тестування та документування результатів

Таблиця 6.21

Фрагмент звіту виконання SW FIT

<table>
<tr><td>Test Case RID</td><td>SFIT.01.01</td><td>Test Case TID</td><td>SFIT.01.01</td></tr>
<tr><td>Test Case TN</td><td colspan="3">[Test valid but wrong command code, RDFBB <= WRFBB]</td></tr>
<tr><td>Test Case description</td><td colspan="3">To test SUT behavior if Command code is WRONG but VALID for UAL Controller. Command length is EQUAL to the correct command length.
Correct Command Code = RDFBB (12)
Inserted Command Code = WRFBB (11)</td></tr>
<tr><td>Date of test execution</td><td colspan="3">December 10, 2019</td></tr>
<tr><td>SUT Configuration</td><td>SUT.SFIT.01</td><td>TB Configuration</td><td>STB.01</td></tr>
<tr><td>Test Case UAL</td><td colspan="3">SFIT_01</td></tr>
<tr><td colspan="4">No Fault
Fault was inserted into LM#1 configuration file (BTS) during test design.
LM#1 configuration files were uploaded into LM#1 during test setup.
SOR were reset for LM and all output modules.</td></tr>
<tr><td colspan="4">Review of the ROVT report [Step 1] (See Figure SFIT.01.01.01 and Appendix B)</td></tr>
<tr><td colspan="2">Expected result</td><td colspan="1">Actual result</td><td>Pass/Fail</td></tr>
<tr><td colspan="2">ROVT shall report an ERROR – wrong MD5 checksum of LM#1 BTS file.</td><td colspan="1">ROVT reports an ERROR – wrong MD5 checksum of LM#1 BTS file.</td><td>PASS</td></tr>
</table>

Продовження таблиці 6.21

==========
Analysis summary
Summary entity name
Build status
Time and date stamp
Number of errors in build.xml analysis
WARNING: RPCT compilation log contains warning messages.
==========
ERROR: \sfit_01-000034.bts expected and obtained MD5 checksums mismatch.
==========

Figure SFIT.01.01.01

SUT state [Step 2] (See Figure SFIT.01.01.01)

LM#1	RUN	**LM#1**	RUN	PASS
DIM#1	RUN	**DIM#1**	RUN	PASS
DOM#1	RUN	**DOM#1**	RUN	PASS
AIM#1	RUN	**AIM#1**	RUN	PASS
AOM#1	RUN	**AOM#1**	RUN	PASS
WAIM#1	RUN	**WAIM#1**	RUN	PASS
TIM#1	RUN	**TIM#1**	RUN	PASS
RIM#1	RUN	**RIM#1**	RUN	PASS
OCM#1	RUN	**OCM#1**	RUN	PASS

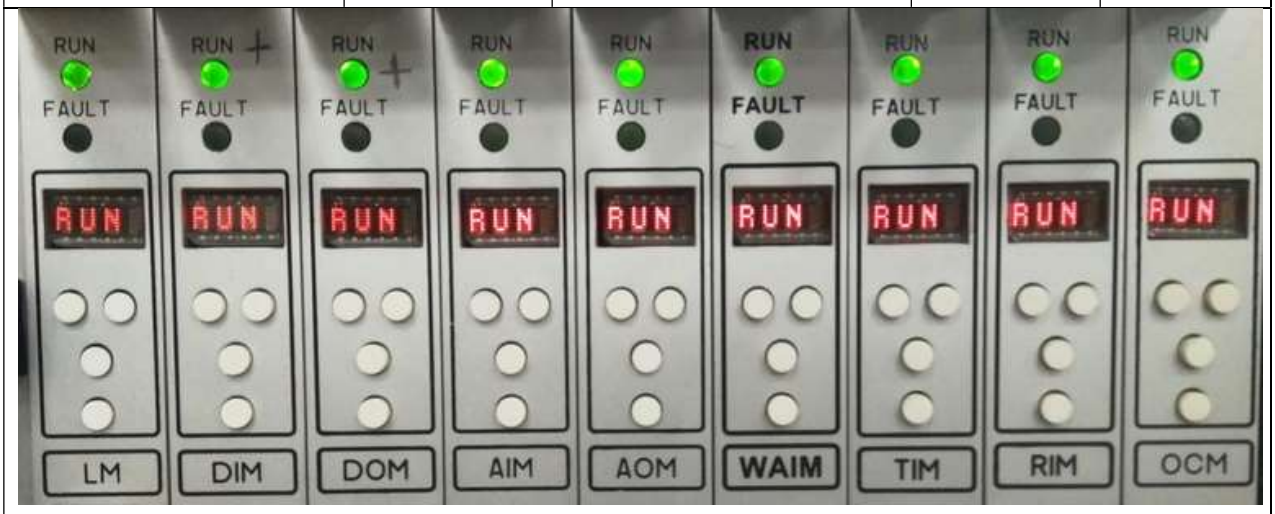


Figure SFIT.01.01.02

Exercise UAL [Step 3.1] (See Figure SFIT.01.01.03)

Module	Signal	[Step 3.1]			Module	Signal	[Step 3.1]	
DIM#1	*INH01A	1			DIM#1	*INH01A	1	
DIM#1	*INH02A	1			DIM#1	*INH02A	1	
DIM#1	*INH03A	0			DIM#1	*INH03A	0	PASS
DIM#1	*INH04A	0			DIM#1	*INH04A	0	
DOM#1	*OUT01	1			DOM#1	*OUT01	1	
DOM#1	*OUT02	0			DOM#1	*OUT02	0	

Figure SFIT.01.01.03

Продовження таблиці 6.21

Exercise UAL [Step 3.2] (See Figure SFIT.01.01.04)

Module	Signal	[Step 3.2]
DIM#1	*INH01A	1
DIM#1	*INH02A	1
DIM#1	*INH03A	1
DIM#1	*INHL4A	0
DOM#1	*OUT01	1
DOM#1	*OUT02	0

Module	Signal	[Step 3.2]
DIM#1	*INH01A	1
DIM#1	*INH02A	1
DIM#1	*INH03A	1
DIM#1	*INH04A	0
DOM#1	*OUT01	1
DOM#1	*OUT02	0

PASS

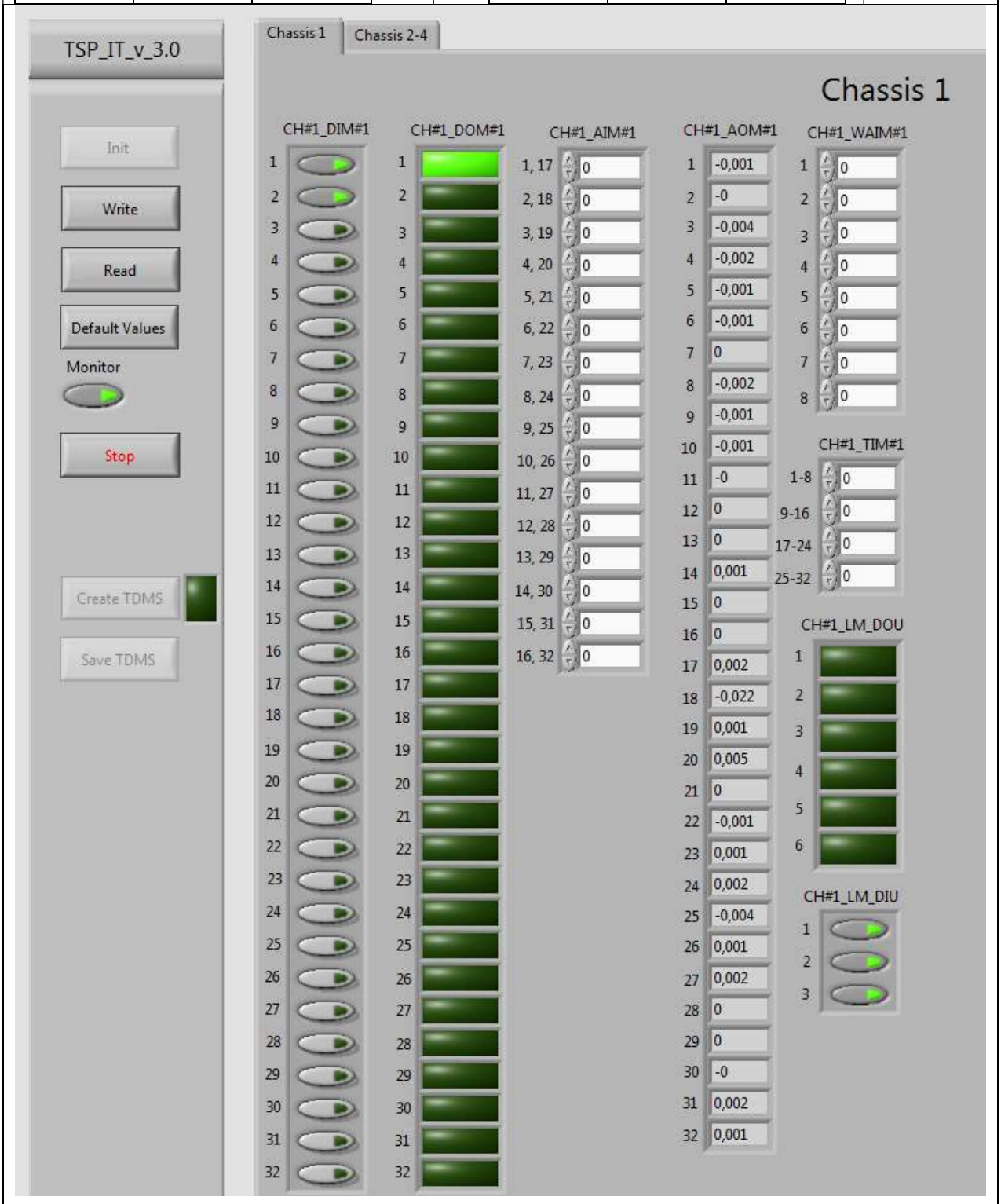


Figure SFIT.01.01.03

Продовження таблиці 6.21

Exercise UAL [Step 3.2] (See Figure SFIT.01.01.04)								
Module	Signal	[Step 3.2]			Module	Signal	[Step 3.2]	
DIM#1	*INH01A	1			DIM#1	*INH01A	1	PASS
DIM#1	*INH02A	1			DIM#1	*INH02A	1	
DIM#1	*INH03A	1			DIM#1	*INH03A	1	
DIM#1	*INHL4A	0			DIM#1	*INH04A	0	PASS
DOM#1	*OUT01	1			DOM#1	*OUT01	1	
DOM#1	*OUT02	0			DOM#1	*OUT02	0	
Exercise UAL [Step 3.3] (See Figure SFIT.01.01.05)								
Module	Signal	[Step 3.3]			Module	Signal	[Step 3.3]	
DIM#1	*INH01A	1			DIM#1	*INH01A	1	
DIM#1	*INH02A	1			DIM#1	*INH02A	1	
DIM#1	*INH03A	1			DIM#1	*INH03A	1	PASS
DIM#1	*INHL4A	1			DIM#1	*INH04A	1	
DOM#1	*OUT01	1			DOM#1	*OUT01	1	
DOM#1	*OUT02	0			DOM#1	*OUT02	0	

Acceptance criterion	1. "Pass" – when all values from expected result is equal all values from actual result; 2. Test successful when all values are Pass. Else – test unsuccessful.
Summary of Test Results (Pass/Fail)	Test PASSED.
Summary of all test anomalies and the CRs raised	

Justification unresolved bugs	
Justification from designer	Justification from verifier

Етап 8. Задіяння процедури усунення виявлених дефектів (за умови виявлення). Де в цьому випадку під дефектом розумієм не співпадання результату виконання тесту з очикуваним.

6.4 Висновки за розділом

1. В розділі упереше 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, а саме:

- метод засіву апаратних дефектів, який відрізняється від відомих процедурою оптимізації таблиць покриття, що забезпечує достатнє тестове покриття та зменшує затрати часу на виконання тестування;

- метод засіву програмних дефектів, який базується на техніці FMEA і відрізняється від відомих процедурою оптимізаціїї таблиць покриття, що забезпечує необхідний рівень тестового покриття і зменшує затрати часу на виконання тестування.

Набув подальшого розвитку 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.

Дані результати отримано на виконання вимог державних та міжнародних стандартів, які встановлено до процесів розроблення, тестування ПТК ІКС критичного застосування

2. Модифікація метода FMEDA базується на аналізі еволюції техніки оцінки надійності FMEA (англ. Failure Mode Effect Analysis – аналіз режимів та наслідків відмов) до FMEDA (англ. Failure Modes, Effects, and Diagnostic analysis – аналіз режими відмов, наслідків та діагностичного охоплення), а також проєктного досвіду використання FMEDA. В результаті аналіза було

встановлено, існуюча техніка FMEDA має ряд суттєвих недоліків, а саме: вимагає багато рутинної та складної роботи для простих і складних електронних компонент системи; нові компоненти (наприклад, типу FPGA) мають специфічні (не проаналізовані) режими відмов; не існують нормативні документи, які описують FMEDA та визначають вимоги до її продуктивності для різних типів систем; не враховує ненадійність, що вноситься програмною компонентою. Здійснена модифікація дозволила автоматизувати найбільш трудомісткі етапи техніки та за рахунок впровадження FMEA для програмних компонент врахувати ненадійність програмної компоненти. Все це знизило в два рази часові затрати на виконання FMEDA та підвищило точність оцінювання функційної безпечності системи в цілому до 5%.

3. Модифіковна процедура FIT є результатом аналізу етапів еволюції атрибутів надійності та функційної безпечності складних систем, а саме простоти (simplicity), здатності до перевірки (checkability), здатності до реконфігурування (reconfigurability), верифікуємості (verifiability) та результатів проєктного впровадження результаів виконання техніки FMEDA (встановлених режимів відмов). Перевірка встановлених режимів відмов базується та техніці FIT (Fault insertion testing), а саме техніці тестування апаратних і програмних компонент із внесенням дефектів в компоненти системи. Як результат виконання цієї техніки встановлено новий атрибут надійності та функційної безпечності, а саме FIT (Fault insertion testing) - придатність. Де FIT - придатність_- це придатність до ін’єктування дефектів у електричні схеми та окремі компоненти ї схеми (HW FIT-здатність) або програмного коду (SW FIT-здатність). Модифікована FIT процедура була застосована для SIL-орієнтованого процесу сертифікації платформи RadICS і дозволила виконати тести на введення (ін'єкцію) за результатами FMEA або FMEDA на різному рівні ієрархії системи: (модуль системи, юніт модуля, електронний проєкт, система в цілому) FMEDA; системний SW, реалізований з кодом HDL (Chip) - FMEDA; програми SW -конфігураційні файли, що генеруються інтегрованим

середовищем розробки) – FMEA, що сприяло визначенню рівня функційної безпечності системи SIL-3.

4. Особливостями процедур є можливість урахування всіх встановлених режимів відмов, визначення для них атрибутів внесення дефектів (точок внесення та значень внесення), що дозволило досягти необхідного рівня тестового покриття для повної впевненості в позитивному результаті тестів діагностичних підсистем.

5. Метод верифікації і валідації дозволяє об’єднати переваги модифікованих процедур: FMEDA; ін’єктування апаратних та програмних компонент, що дозволяє встановлювати реальний рівень діагностичного покриття засобами підсистем самодіагностування АК та ПК. Використання даних процедур дає основний висновок щодо рівня функційної безпечності (Safety Integrity Level) на відповідність станадартам із функційної безпечності і зокрема IEC 61508 ПТК, які розробляються, тестуються та вводяться в експлуатацію.

6. Метод оціювання та забезпечення надійності і функційної безпечності програмно-технічних комплексів іформаційно-керуючих систем критичного застосування акумулює всі попередні наукові результати та їх переваги. Він дозволяє виконувати комплексне оцінювання вказаних властивостей враховуючи: розширення поняття технічного стану системи до інформаційно-технічного; розширену множину компонентів (апаратних, прогрманих, програмовни); розширену множину дефектів (фізичні дефекти АК, дефекти проєктування, дефекти взаємодії); множини відмов (критичні, некритичні); розширену множину змінних параметрів тощо. Метод застосовується на протязі життєвого циклу системи, який описується V-моделлю після наступних етапів: Software Requirements Specification (розробки множини специфікацій, системної, АК та ПК); Software Verification – верифікації компонент ПЗ та комплексу ПЗ; інтеграційного тестування; кваліфікаційного тестування та валідаційного тестування. Це дає змогу уточнювати системні вимоги та вимоги

до АК і ПК компонент системи, формулювати рекомендації щодо архітектури побудови системи, уточнювати ітогові значення показників надійності і функційної безпечності систем, які розробляются, тестуються та вводяться в експлуатацію. Сумарний ефект щодо підвищення оцінювання точності показників, в результатів застосування даного метода, досягає 10%. Застосування окремих складових метода, наприклад модифікованих процедур FMEDA, SW FIT, HW FIT знижує часові і відповідно фінансові витрати на виконання процесів ліцензування і сертифікації ПТК ІКС критичного застосування.

7. Програмно-апаратні засоби виконання тестування реалізують розроблені теоретині положення і є основою частини впровадженої системи менеджмента якості підприємства, яка визначає умови та послідовність виконання робот (активностей) верифікації та валідації програмовних платформ та програмно-технічних комплексів інформаційно-керуючих систем критичного використання на програмовних логічних інтегральних схемах, які розробляються на їх основі. Основні положення розділу викладені у публікаціях автора [235, 237, 247, 248, 250, 251, 254, 262, 263, 275, 276, 280, 281, 282, 283, 293, 294].

ВИСНОВКИ

1. У дисертаційній роботі вирішена актуальна науково-прикладна проблема 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 вразливост ями програмних і апаратних засобів (включаючи відмови з загальної причини), а також зміни параметрів потоків їх відмов і відновлень, що полягає у вирішенні об'єктивного протиріччя, а саме в усунені невідповідності між встановленою розширенною множиною причин порушення працездатності програмно-технічних комплексів інформаційно-керуючих систем атомних станцій, аерокосмічних комплексів та інших індустріальних об’єктів критичного застосування внаслідок фізичних і проєктних дефектів їх апаратних, програмних і програмовних компонентів, зміною параметрів потоків відмов і відновлень з одного боку, і рівнем розвитку концептуальних засад, сучасних методів і засобів оцінювання та забезпечення надійності та функційної безпечності, які не повно враховують причини і характеристики відмов і порушень ПТК, - з іншого боку.

2. У дисертації одержані наступні нові наукові результати:

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 програмових 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. В рамках методології сформульована концепція комплексного оцінювання й забезпечення надійності та функційної

безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного застосування, яка є розвитком концепції синтезу надійних систем із ненадійних компонентів, яку запропонував Джон фон-Нейман, яка розвивається стосовно ПТК ІКС критичного застосування шляхом їх комплексного оцінювання і забезпечення надійності і функційної безпечності. Концепція базується на принципах:

- аналізу інформаційно-технічного стану та варіантів його порушення, який відрізняється тим, що дозволяє урахувати системні властивості і ознаки як технічного, так і інформаційного характеру, які притаманні системі в певний момент часу;

- визначення змінних параметрів потоків відмов за різними ознаками й відновлень компонентів і систем, який відрізняється тим, що дозволяє виконувати оцінювання надійності і функційної безпечності ПТК ІКС критичного застосування з урахуванням змінності параметрів потоків відмов і відновлень їх програмно-апаратних компонент, спираючись на аналіз опису: системних функцій; сценаріїв функціонування системи; вимог до оточуючого середовища, вимог до інформаційної безпеки; вимог до надійності і функційної безпечності; архітектури системи; детального дизайну програмно-апаратних компонент ПТК;

- комплексування моделей та методів оцінювання апаратних, програмних і програмовних компонент, який відрізняється тим, що дозволяє поєднувати переваги розроблених моделей і методів з метою більш точного оцінювання надійності і функційної безпечності ПТК ІКС критичного застосування;

- використання процесно-продуктивної диверсності при створенні систем, який відрізняється тим, що дозволяє застосовувати різні продуктові (програмно-апаратні) і процесні засоби для реалізації ідентичних функцій з метою розробки ПТК, які є стійкими дефектів різної природи, завдяки: застосуванню в резервованих каналах системи різних програмно-апаратних версій, що знижує імовірність відмови за загальною причиною; застосуванню

диверсних незалежних процесів і засобів проєктування і тестування.

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

3. 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, а також обгрунтувати вимоги до них.

4. Результати досліджень впроваджено в процесі:

- оцінювання надійності і функційної безпечності перспективної цифрової інформаційно-управляючої платформи RadICS в процесі її SIL-3 сертифікації на відповідність вимогам стандарту IEC 61508 («Науково-виробниче підприємство «Радій» (м. Кропивницький));

- розроблення процедур і інструкцій системи менеджменту якості підприємства і виконання низки міжнародних проєктів із розроблення відповідних інформаційно-керуючих систем (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) (Товариство з обмеженою відповідальністю «Науково-виробниче підприємство «Радікс» (м. Кропивницький);

- розроблення 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 (Державне науково-виробниче підприємство «Об’єднання «Комунар» СКБ «Полісвіт»);

- розроблення структур і вимог нормативних документів до ПТК ІКС АЕС, що надало змогу покращити повноту оцінювання і якість відповідних документів (Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки»);

- 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 (Приватному підприємстві ЛітСофт);

- виконання 5 науково-дослідних робіт за держзамовленням, 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» (Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»).

5. Виконана в дисертації кількісна оцінка ефективності запропонованих методів, підтверджена результатами практичного впровадження, свідчить про їх переваги, порівняно з існуючими методами, а саме вдосконалено процеси розроблення, верифікації та валідації СДПП і систем, які будуються на їх

основі, що забезпечло досягнення системами рівня функційної безпечності SIL-3 і зменьшило відповідно часові і фінансові затрати на ці процеси до 10%; підвищена точність оцінювання та значення показників надійності і функційної безпечності з урахуванням різних типів дефектів і відмов програмно-апаратних засобів бортових ІКС літаків АН-70, АН-148 до 5%; підвищена ефективність тестування (число виявлених дефектів) до 10%.

6. Достовірність нових наукових положень і висновків дисертаційної роботи підтверджується:

− збігом з результатами, отриманими з використанням відомих моделей і методів теорії надійності; обґрунтованістю припущень, прийнятих при розробленні моделей і методів, виходячи з досвіду експлуатації ПТК ІКС;

− працездатністю та ефективністю апаратних рішень та інструментальних засобів, отриманих із застосуванням запропонованих методів і моделей, підтвердженою на низці підприємств;

− результатами практичного використання розроблених моделей, методів та інструментальних засобів при створенні, сертифікації та експлуатації ПТК на програмовних платформах та ІКС різного призначення.

7. Основні положення і результати дисертації можуть бути використані державними та закордонними підприємствами, що виконують розробку, тестування, супроводження і експлуатацію програмно-технічних комплексів інформаційно-керуючих систем критичного застосування.

8. Подальші дослідження слід проводити в наступних напрямках:

- вдосконалення інструментальних засобів виконання процедури аналізу видів, наслідків і критичності відмов з урахуванням ненадійності, що вносять програмні компоненти;

- вдосконалення інструментальних засобів автоматизації процеса прийняття рішень при розробці ПТК ІКС КЗ, а також створення інформаційних технологій підтримки експлуатації систем, важливих для безпеки, атомних

станцій, аерокосмічних комплексів та інших індустріальних об’єктів критичного застосування на всіх етапах життєвого циклу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безопасность атомных станций: Информационные и управляющие системы /Ястребенецкий М.А. и др.; под ред. М.А. Ястребенецкого. Київ, Техніка, 2004. 472 с.

2. Системы управления и защиты ядерных реакторов / Ястребенецкий М.А. и др.; под ред. М.А. Ястребенецкого. Киев, Основа-Принт, 2011.768 с.

3. Ястребенецкий М.А. Автоматика АЭС Украины после Чернобыльской аварии. *Ядерна та радіаційна безпека*. 2011. Т. 14, №1. С. 47–52.

4. Копчинский Г.А., Штейнберг Н.А. Чернобыль: О прошлом, настоящем и будущем:монография. Киев: Основа, 2011. 224 с.

5. Либман Ж. О ядерной безопасности. Фонтене-о-Роз, Франция: Институт по ядерной и радиационной безопасности, 1997. 690 с.

6. НП 306.5.02/2.068-2000. Требования к порядку и содержанию работ по продлению срока эксплуатации информационных и вычислительных систем, важных для безопасности атомных станций. Киев.:Гос. Администрация ядерного регулирования, 2000.

7. НП 306.5.02/3.035-2000.Требования по ядерной и радиационной безопасности к информационным и управляющим системам, важным для безопаснотси атомных станций. Киев.: Гос. Администрация ядерного регулирования, 2000.

8. СОУ-Н НКАУ 0060:2010. Гарантоздатність програмно-технічних комплексів критичного призначення. [Чинний від 2010-02-08]. Київ, 2010. 60с.

9. IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Published. 2010 – 04. IEC Standards, 2010. 594 p.

10. IEC 61513: 2011. Nuclear power plants – instrumentation and control for systems important for safety – general requirements for systems. Published. 2011 – 08 – 25. IEC Standards, 2011. – II, 86 p.

11. IEC 61226.Ed.2. Nuclear power plants- Instrumentation and control systems important for safety-Classifcation of instrumentation and control systems.-2005.

12. IEC 60880:2006. Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A function. Published 2006 – 05 – 09. – IEC Standards, 2006. 211 p.

13. IEC 62138:2018 Nuclear power plants- Instrumentation and control systems important for safety-Software aspects for computer-based systems perfoming category A or C functions.

14. IEC 60987.Ed.2.1. Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems. 2013.

15. IEC 60300-3-1:2003. Dependability management. Part 3-1: Application guide. Analysis techniques for dependability. Guide on methodology. – Published 2004 – 09 – 29. – IEC Standards, 2004. 50 p.

16. IEC 61165:2008. Application of Markov techniques. – Published 2008 – 07 – 28. IEC Standards, 2008. 27 p.

17. ISO 12207:2008 System and software engineering – Software life cycle processes.

18. ISO/IEC 25010:2011 Systems and software engineering – SQuaRE (Final draft) –System and software quality models // International Organization for Standardization.

19. ISO/IEC TR 9126-2:2003 «Software engineering – Product quality. Part 2: External metrics».

20. ISO/IEC TR 9126-3:2003 «Software engineering – Product quality – Part 3: Internal metrics».

21. ISO 9126:2000. Information technology. Software product quality [Text]. – Published 2012 – 09 – 13. IEC Standards, 2012. 25 p.

22.ISO 9001:2015. Системи управління якістю. Вимоги. 2015. 33с.

23.IEEE 1012:2004 Standard for Software Verification and Validation.

24.IEEE 1008:1987 (R2002) Standard for Software Unit Testing.

25.IEEE 829:2008 Standard for Software Test Documentation.

26. IEEE 1016:2009 Standard for Information technology – Systems Design – Software Design Descriptions.

27. IEEE 7-4.3.2-2016. IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations.

28. IAEA. The safety of nuclear installations// IAEA safety series №110.Vienna, 1993.

29. IAEA NS-R-1. Safety of nuclear power plants:design// Safety requirements.-Vienna, 2000.

30. IAEA NS-G-1.3. Insrtumentation and control systems important to safety in nuclear plants // Safety guide.-Vienna, 2002.

31. IAEA NS-G-1.1. Software for computer based systems important to safety in nuclear power plants // Safety guide.-Vienna, 2000.

32. IAEA NS-R-2. Safety of nuclear power plants:operation// Safety requirements.-Vienna, 2000.

33. IAEA NS-G-2.4 The operation organization for nuclear power plants// Safety guide.-Vienna, 2001.

34. ДСТУ ISO 9001:2015: Системи управління якістю. Вимоги (ISO 9001:2001).[Чинний від 2015-01-01]. Київ. 2015. 39с.

35. ДСТУ IEC 60880: Атомні електростанції. Інформаційні та керувальні системи, важливі для безпеки. Програмні аспекти комп’ютерних систем, які виконують функції категорії А. [Чинний від 2008-01-01].Київ. 2008. 90с.

36. ДСТУ 2860-94: Надійність техніки. Терміни та визначення. [Чинний від 1996 – 01 – 01]. Київ. 1995. 92с.

37. ДС'ТУ 2861-94:Надійність техніки. Аналіз надійності. Основні положення.[Чинний від 1996-01-01].Київ, 1995. 10 с.

38. ДСТУ 2862-94: Надійність техніки. Методи розрахунку показників надійності. Загальні вимоги. [Чинний від 1996-01-01]. Київ: 1994. 40 с.

39. ДСТУ 3524-97 (ГОСТ 27.205-97). Надійність техніки. Проектна оцінка надійності складних систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення. [Чинний від 1997-01-01]. Київ, 1997. 52 с.

40. ДСТУ 2850-94. Програмні засоби ЕОМ. Показники та методи оцінки якості [Текст]. – Введ. 1994 – 01 – 01. – К. : Держспоживстандарт України, 1994. – 33 с.

41. ДСТУ ISO/IEC TR 13335-1:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції та моделі безпеки ІТ. [Чинний від 2003-01-01]. Київ, 2003. 22 с.

42. ДСТУ ISO/IEC TR 13335-2:2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ. [Чинний від 2003-01-01]. Київ, 2003. 20 с.

43. Military handbook. Electronic reliability design handbook: MIL-HDBK-338B. –Washington: DoD, 1998. 1046 p.

44. Нейман, Дж.Фон. Теория самовоспроизводящихся автоматов/ Дж. Фон Нейман. Москва.: Изд. «Мир», 1971. 383с.

45. Отказобезопасные информационно–управляющие системы на программируемой логике / Бахмач Е.С. и др. ; под ред. В.С. Харченко, В.В. Скляра. Харків, Национальний аэрокосмический университет «ХАИ», НПП «Радий», 2008. 380 с.

46. Основы теории и расчета надежности / Половко А.М. др.; под ред. А.М. Половко. Ленинград: изд. Судпромгиз, 1959 г.

47. Mathematical Theory of Reliability. Richard E. Barlow and Frank Proschan. With contributions by Larry C. Hunter. Wiley, New York, 1965, 256 pp.

48. Гнеденко Б.В., Беляев Ю.К, Соловьев А.Д. Математические методы в теории надежности. Серия: «Физико-математическая библиотека инженера». Москва., 1965 г., 1965., 524 с.

49. Соловьев А.Д. Основы математической теории надежности. Москва.:Знание, 1975. 129 с.

50. Сорин Я. М. Физическая сущность надежности. Издательство стандартов. Москва, 1969 г. 82с.

51. Бусленко Н.П. Моделирование сложных систем. Главная редакция физико-математической литературы издательства «Наука», Москва., 1968, 356 с.

52. Бусленко В. Н. Автоматизация имитационного моделирования сложных систем. Москва.: изд. Наука, 1977. 239 с.

53. Баруча Р.А. Элементы теории марковских процессов и их приложения. Москва.: изд. Наука, 1969. 511 с.

54. Метод статистических испытаний (метод Монте-Карло) / Бусленко Н.П. и др.; под ред. Ю.А Шрейдера. Москва.: изд. Физматгиз, 1962. 331 с.

55. Герцбах И.Б. Модели профилактики. Москва.: изд. Сов. Радио, 1969. 214с.

56. Герцбах И.Б., Кордонский Х.Б. Модели отказов. Москва.: изд. Сов. радио, 1966. 166с.

57. Половко А.М., Гуров С.В. Основы теории надежности.-2-изд.перераб. и доп.. Санкт-Петербург: изд. БХВ-Петербург, 2006. 704с.

58. Надежность технических систем: Справочник/ Ю.К. Беляев, В.А. Богатырев, В.В. Болотин и др.; под ред. И.А. Ушакова. Москва.: Радио и связь, 1985. 608 с.

59. Рябинин И.А. Надежность и безопасность структурно-сложных систем. Санкт-Петербург: изд. Санкт-Петербургского университета, 2007. 276 с.

60. Черкесов *Г.Н.* Надежность технических систем с временной избыточностью. Москва.:Сов.радио, 1974. 296с.

61. Дружинин Г. В. Процессы технического обслуживания автоматизированных систем. Москва.: Энергия, 1973. 226 с.

62. Управление эксплуатацией летательных комплексов: учеб. пособие / Л. И. Волков. Москва.: Высш. Школа, 1981. 368 с.

63. Надежность и эффективность в технике: Справочник: В 10 т./Ред.совет: В.С. Авдуевский (пред.) и др. Москва.: Машиностроение, 1986.

64. Основи надійності цифрових систем: підручник. / Харченко В.С. та ін.; за ред. В.С. Харченка, В.Я. Жихарева.Харків, Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2004. 572 с.

65. Диллон Б., Сингх Ч. Инженерные методы обеспечения надежности систем: Пер. с англ. Москва.:Мир, 1984. 318с.

66.Антонов А.В. Системный анализ. Москва.: Высшая школа, 2004. 454 с.

67. Советов Б.Я., Яковлев Б.Я. Моделирование систем: Учебник для вузов. Москва.: Высш. Шк., 1985. 271 с.

68. Уемов А.И. Системный подход и общая теория систем. Москва. Мысль, 1978. 272 с.

69. Садовский В.Н. Системный подход и общая теория систем: статус, основные проблемы и перспективы. Москва.: Наука, 1980. 234 с.

70. Носовский, А.В. Особенности безопасности ядерной енергетики. *Ядерная и радиационная безопасность*. 2003. Т. 6, № 2. С. 29–39.

71. Введение в безопасность ядерных технологий /Носовский А.В. и др.; под ред. А.В. Носовского. Київ: Техніка, 2006. 360с.

72. Федоров Ю.Н. Справочник инженера по АСУ ТП: Проектирование и разработка. Москва.: Инфра–Инженерия, 2008. 928 с.

73. Федоров Ю. Н. Основы построения АСУ ТП взрывоопасных производств. Москва. : СИНТЕГ, 2006. 720 с.

74. Smith, D. Functional Safety. A Straightforward Guide to applying IEC 61508 and Related Standards / D. Smith, K. Simpson. – Elsevier Butterworth-Heinemann, Oxford, UK, 2004. 263 p.

75. Medoff, M. Functional Safety – An IEC 61508 SIL 3 Compatible Development Process / M. Medoff, R. Faller. – exida.com L.L.C., Sellersville, PA, USA, 2010. 281 p.

76. Guzman–Miranda, H. Coping With the Obsolescence of Safety– or Mission–Critical Embedded Systems Using FPGAs / H. Guzman-Miranda, L. Sterpone, M. Violante, M. A. Aguirre, M. Gutierrez–Rizo // IEEE Trans. on Industrial Electronics. 2011. V. 58, N. 3. P. 814–821.

77. Нарушения в работе АЭС вследствие отказов информационных и управляющих систем по общей причине / О.Н. Бутова, В.В. Инюшев, Л.И. Спектор, М.А. Ястребенецкий. *Радіоелектронні і компьютерні системи. Науково-технічний журнал. Національний аерокосмічний університет «ХАІ».* 2008. № 5. С. 45–54.

78. Мухин В.И. Исследование систем управления. Москва.: Издательство Экзамен, 2003. 384 с.

79. Комп'ютерна програма «MSMC-Method selector for Markov chains». Свідоцтво про реєстрацію авторського права на твір №57120.-Дата реєстрації 05.10.2014.

80. Одарущенко О.Н., Харченко В.С Моделирование и оценивание функциональной безопасности программно-технических комплексов в контексте стандарта IEC 61508. Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013. Чернігів-Жукин, 2013. С. 339-339.

81. Скляр В. В. Методология и информационные технологии обеспечения функциональной безопасности информационно-управляющих систем: дис. д-ра техн. наук: 05.13.06 /Национальный аэрокосмический университет им. М. Е. Жуковского «ХАИ». Харьков, 2011. 444 с.

82. FPGA–based NPP Instrumentation and Control Systems: Development and Safety Assessment/ E.S. Bakhmach, A.D. Herasimenko, V.A. Golovyr, V.S. Kharchenko, Yu.V. Rozen, A.A. Siora, V.V. Sklyar, V.I. Tokarev, S.V.

Vinogradskaya, M.A. Yastrebenetsky. – National Aerospace University “KhAI”, 2008. 188 p.

83. Romanovsky, A. A looming fault tolerance software crisis? ACM SIGSOFT Software Engineering Notes. ACM, 2007. V. 32(2). P. 1–4.

84. Конорев Б.М., Федорович О.Е., Манжос Ю.С. Нормативная база программной инженерии в разработке систем с интенсивным использованием программного обеспечения. Харьков, Нац. аэрокосмический ун-т «ХАИ», 2001. 162 с.

85. Конорев Б.М., Харченко В.С., Чертков Г.Н.. Концепция и принципы реализации интегрированной инструментальной системы для поддержки экспертизы и независимой верификации критического программного обеспечения (SAVExpert–System). Государственный комитет ядерного регулирования Украины, Государственный центр регулирования качества поставок и услуг, Сертификационный центр АСУ, 2003. 60с.

86. Littlewood B., Popov P.,. Strigini L. Modelling the effects of combining diverse software fault removal techniques. IEEE Trans. on Software Engineering. 2000. – SE–26(12). P. 1157–1167.

87. Зеленая ИТ-инженерия.В 2-х томах. Том 1. Принципы, компоненты, модели /Харченко В.С., Андрейченко Д.К., Антощук С.Г., Дрозд М.А., Одарущенко О.Н., Бульба Е.Н., Стрюк А.Ю., Ивасюк А.О. и др. // Под ред. Харченко В.С. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ».- 2014.-594с.

88. Littlewood B., Strigini L. Redundancy and diversity in security. European Symposium on Research in Computer Security (ESORICS’2004): proceedings of 9th Symposium. Sophia Antipolis, France, 2004. P. 117–126.

89. Popov P., Strigini L. Conceptual models for the reliability of diverse systems – new results. *International Symposium on Fault–Tolerant Computing (FTCS–28)*: proceedings of 28th International Symposium. Munich, Germany, 1998. P. 80–89.

90. Estimating bounds on the reliability of diverse systems / Popov P., Strigini L., May J., Kuball S. IEEE Trans. on Software Engineering. 2003. V. 29. P. 345–359.

91. Popov P., Strigini L. The Reliability of Diverse Systems: a Contribution using Modelling of the Fault Creation. *International Conference on Dependable Systems and Networks: proceedings of International Conference*. Sweden, Goteborg, 2001. P. 5–14.

92. Popov P., Strigini L., Romanovsky A .Diversity for Off–The–Shelf Components. *International Conference on Dependable Systems and Networks: proceedings of Conference*. Goteborg, Sweden, 2001. P. 61–67.

93. Харченко В.С., Скляр В.В., Аль–Тарази А.Х. Вероятностная модель оценки состояний отказобезопасных информационных и управляющих систем энергетических комплексов. *Вісник Харківського державного технічного університету сільського господарства. Проблеми енергозабезпечення та енергозбереження в АПК України*. Вип. 27, Т.2., Харків, 2004. С. 210-213.

94. Головир В.А., Скляр В.В., Харченко В.С. Методы внесения и оценки версионной избыточности при разработке информационно–управляющих систем на базе ПЛИС. *Вісник Хмельницького національного університету*. 2005. Т. 1,Ч. 1, № 4. С. 94–97.

95. Модели безотказности и готовности встроенных мультидиверсных систем / В.С. Харченко, В.В. Скляр, А.А. Сиора, Ю.А. Белый. Авиационно–космическая техника и технология. 2008. №1(48). С. 64-69.

96. Kharchenko V., Siora A., Sklyar V. Design and Testing Technique of FPGA–Based Critical Systems. *The Experience of Designing and Application of CAD Systems in Microelectronics: proceedings of the X International Conference*. Ukraine, Lviv–Polyana, 2009. P.305–314.

97. Certification of FPGA–based Safety Instrumentation and Control Platform in Accordance with IEC 61508 / A. Andrashov, V. Kharchenko, A. Siora, V. Sklyar, A. Volkoviy. *Critical Infrastructure Safety and Security (CrISS–DESSERT*

2011): proceedings of the First International Workshop. – Kharkiv, 2011. V. 1. P.148 – 152.

98. Розенберг Е.Н., Шубинский И.Б. Методы и модели функциональной безопасности технических систем /Москва.: ВНИИАС, 2004. 188 с.

99. Functional Safety of Safety–Related Systems. Manual for Plant Engineering and Maintenance/ A. Basilio, F. Landrini, G. Novelli, G. Landrini, M. Baldrigh. G.M. International S.r.l, Villasanta, Italy, 2008. 388 p.

100. Banerjee N. Utilization of FMEA concept insoftware lifecycle management. *Conference on Software Quality Management: proceedings of the Conference*. Göteborg, Sweden, 1995. P. 219–230.

101. Bluvband Z., Zilberberg E. Knowledgebase approach to integrated FMEA. Annual Quality Congress: proceedings of the 52nd Congress. Philadelphia, PA, USA, 1998. P.535–545.

102. Бабешко Е.В., Кривоносов А.И., Харченко В.С. Анализ возможностей современных ПЛК для построения отказоустойчивых АСУ ТП. *Інформаційні інфраструктури та технології*. 2007. №2. – С.37-41.

103. Pekka P. Human reliability analysis methods for probabilistic safety assessment. Technical research centre of Finland, 2000. 67 p.

104. Александровская Л.Н., Афанасьев А.П., Лисов А.А. Современные методы обеспечения безотказности сложных технических систем. Москва. Логос, 2001. 208 с.

105. Weightman M. Japanese earthquake and tsunami: Implications for the Nuclear Industry. Interim Report. Merseyside, UK, Office for Nuclear Regulation, 2011. 106 p.

106. Надежность технических системы: справочник/ Ю.К. Беляев, В.А. Богатырев, В.В. Болотин и др.; под ред. И.А.Ушакова. Москва. Радио и связь, 1985. 608 с.

107. Каштанов В.А., Медведев А.И. Теория надежности сложных систем. Москва. : Изд–во Европейский центр по качеству, 2002. 469 с.

108. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. Москва.: Наука, 1970. 720 с.

109. Кемени Дж., Снелл Дж. Конечные цепи Маркова. Москва. Наука, 1970. 273 с.

110. Procedures for Performing a Failure Mode, Effects and Criticality Analysis. U.S. Department of Defense: MIL-P-1629. 1980. 42 p.

111. Ушаков, И.А. Курс теории надежности систем. Учебное пособие. Москва.: Дрофа, 2008. 239 с.

112. Vsely, V.E. Fault Tree Handbook. NUREG–0492/ V.E. Vsely, F.F. Goldberg, N.H. Roberts, D.F. Haasl. – U.S. Nuclear Regulatory Commission, Washington D.C., USA, 1981. 209 p.

113. Walker, J.S. Three Mile Island. A Nuclear Crisis in Historical Perspective. University of California Press, 2006. 314 p.

114. Садчиков П.И., Приходько Ю.Г. Методы оценки надежности и обеспечения устойчивости функционирования программ. Москва. Знание, 1983. 102 с.

115. Портенко Н.И., Скороходов А.В., Шуренков В.М .Марковские процессы. Москва. ВИНИТИ, 1989. 246 с.

116. Барлоу Р., Прошан Ф. Статистическая теория надежности и испытания на безотказность. Москва.: Наука, 1984. 156 с.

117. Безопасность критических инфраструктур:математические и инженерные методы анализа и обеспечения/ Одарущенко О.Н. и др.; под. ред. В.С. Харченко. Харьков, 2011.641с.

118. Иыуду К.А. Надежность, контроль и диагностика вычислительных машин и систем. Москва.: Высшая школа, 1989. 216 с.

119. Федухин А.В., Сеспедес Гарсия Н.В. Математические машины и системы. 2013. № 2. С. 195-201.

120. Федухин А.В., Пасько В.П. Моделирование надежности систем. Методы менеджмента качества. 2012. № 3. С. 50-55.

121. Математичні моделі та методи аналізу надійності радіоелектронних, електротехнічних та програмних систем: монографія / Ю. Я. Бобало та ін.; Львів.:Львівська політехніка, 2013. 300 с.

122. Черкесов Г.Н. Надежность аппаратно-программных комплексов. Учебное пособие. Санкт-Петербург.: Питер. 2005. 479с.

123. Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Selecting mathematical software for dependability assessment of computer systems described by stiff Markov chains. *ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer. ICTERI 2013. Procceding of the 9th International Conference.* (June 19-22, 2013). Kherson, Ukraine, P. 146 – 162.

124. Одарущенко О.Н., Харченко В.С. Модель информационно-технического состояния информационной системы. *Системи обробки інформації. Збірник наукових праць НАНУ, ПАНМ, ХВУ*. 2008. Вип 7(74). С.128-130.

125. Одарущенко О.Н., Харченко В.С. Информационно-технические состояния компьютеризированных систем: модель событий и показатели гарантоспособности. *Системи управління, навігації та зв'язку: Державне підприємство «Центральний науково-дослідний інститут навігації і управління»*. 2009. Вип.3(11). С.156-159.

126. Одарущенко О.Н., Живило С.В. Методология оценки гарантоспособности на основе фактического информационно-технического состояния. Материалы междунар одной научно-практической конференции «Информационные технологии и информационная безопасность в науке, технике и образовании (ИНФОТЕХ -2011). Севастополь, 2011. С.38-39.

127. Odarushchenko O., Kharchenko V., Popov P., Zhadan V. Empirical evaluation accuracy of mathematical software used for availability assessment of fault-tolerant computer systems. *Electronic Jornal Reliability & risk Analysis: Theory & Applications*. 2012. 3(26).Vol.7. P.85-97.

128. Odarushchenko O., Kharchenko V., Butenko V. Metric-based analysis of Markov models for computer systems availability assessment / *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ»*. Вип.5(64). 2013. С.214-220.

129. Харченко В.С., Асидех Ф.А., Лысенко И.В.Марковские модели готовности восстанавливаемых STRATUS-систем. *Системи обробки інформації : зб. наук. пр. Харк. ун-т Повітряних Сил ім. Івана Кожедуба*. Харків, 2004. Вип. 4. С. 216-226.

130. Арушанян О.Б., Залеткин С. Ф. Численное решение обыкновенных дифференциальных уравнений на Фортране. М.: Изд.МГУ, 1990. 336 с.

131. Markov Analysis ITEM ToolKit Module [Electronic source]. URL: http://www.itemuk.com/markov.html (дата звернення: 19.03.2021).

132. Reliasoft (Blocksim) [Electronic source]. URL: http://www.reliasoft.com/ BlockSim/features2.htm (дата звернення: 19.03.2021).

133. Щербовських С.В., Мандзій Б.А. Математична модель надійності для аналізу причин непрацездатності системи із роздільним заміщувальним резервом. *Радіотехнічні й комп'ютерні системи*. 2014. – №5 (69). С. 114 – 118.

134. Надійнісна модель відмовостійкої програмно-апаратної системи на основі мажоритарної структури з ковзним резервуванням та автоматичним перезавантаженням програмного забезпечення / Волочій Б.Ю., Озірковський Л.Д., Муляк О.В., Змисний М.М. *Радіоелектронні й комп'ютерні системи*. 2013. № 5 (64). С. 221 – 226.

135. Barge, W. S., Stewart W. J. Autonomous solution methods for large Markov chains. Pennsylvania State University CiteSeerX Archives. 2002. P. 1 – 17.

136. Липаев *В.В.* Обеспечения качества программных средств. Методы и стандарты. Москва.: СИНТЕГ, 2001.380 с.

137. Липаев В.В. Функциональная безопасность программного обеспечения. Москва.: Синтез, 2004. 281 с.

138. Майерс Г. Надежность программного обеспечения. Москва: Мир, 1980. 360 с.

139. Канер С., Фолк Д.,. Нгуен К Тестирование программного обеспечения. Москва.: DiaSoft, 2001. 544 с.

140. CASE-оценка критических программных систем. В 3-х томах. Том 1. Качество / Мищенко В.О. и др.; под ред. Харченко В.С. Х.: Нац. аэрокосмический ун-т «Харьк. авиац. ин-т», 2012. 201 с.

141. Поночовный Ю.Л., Одарущенко Е.Б. Моделирование надежности обновляемых программных средств нерезервированных информационно-управляющих систем постоянной готовности. *Радіоелектронні і комп'ютерні системи*. 2004. №4(8). С. 93-97.

142. Гласс Р. Руководство по надежному программированию. Москва: Финансы и статистика, 320 с.

143. B. Randell. System Structure for Software Fault Tolerance. IEEE Transactions on Software Engineering. 1975. Vol.1. P. 220-232.

144. Liu Y., Levendel H., Trivedi K. S. Modeling and Analysis of Software Rejuvenation in Cable Modem Termination System // ISSRE. 2002. Vol. 12, № 17. P. 159-170.

145. Lyu M.R. Handbook of Software Reliability Engineering. – Washington: McGraw-Hill Company, 1996. 805 p.

146. Теоретические основы дефектоустойчивых систем с версионной избыточностью. В.С. Харченко. Монография, МОУ, 1996, 506с.

147. Одарущенко О.Н., Руденко А.А., Руденко З.Н., Мельник М.А. Метод оценивания надежности программных средств с учетом вторичных дефектов. Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013. Тези доповідей. Чернігів-Жукин, 2013. С. 336-339.

148. Оценка и обеспечение качества программных средств космических систем / Под ред. Харченко В.С., Конорева Б.М. – Национальное космическое

агенство Украины, Государственный центр регулирования качества, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2007. 244 с.

149. Полонников Р.И., Никандров А.В. Методы оценки показателей надежности программного обеспечения. Санкт-Петербург.: Политехника – 1992. 78 с.

150. CASE-оценка критических программных систем. Надежность Т.2. / Одарущенко О.Н. и др.; под ред. В.С. Харченко, Харьков, 2012. 292с.

151. Терминологические аспекты теории надежности программных средств / О.Н. Одарущенко и др. *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ»*. 2006. Вип.6(18), С.61-70.

152. Модели оценки надежности программных средств с учетом недетерминированного числа вторичных дефектов / О.Н. Одарущенко и др. *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ»*. 2010. Вип.6(47), С.197-203.

153. Моделирование обслуживаемых компьютерных систем с учетом вторичных дефектов программных средств / О.Н. Одарущенко и др. *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ»*. 2009. № 7, С.245-249.

154. Учет вторичных дефектов в моделях надежности программных средств / О.Н. Одарущенко и др. *Математичні машини і системи. Інститут проблем математичних машин і систем НАН України*. 2010. Вип.1. С.205-217.

155. Анализ сценариев и определение параметров для оценки надежности программных средств с учетом вторичных дефектов / О. Н. Одарущенко и др. *Системи управління, навігації та зв'язку. Державне підприємство «Центральний науково-дослідний інститут навігації і управління»*. 2011.Вип.3(11), С.273-280.

156. Метод оценивания надежности программных средств с учетом

вторичных дефетков / О.Н. Одарущенко и др. *Радіоелектронні і комп'ютерні системи. Науково-технічний журнал. Національний аерокосмічний університет «ХАІ»*. 2012. Вип.7(59). С.313-318.

157. Одарущенко О.Н. Учет фактора вторичных дефектов при оценке надежности программных средств / О.Н. Одарущенко, В.С. Харченко, А.А. Руденко, Е.Б. Одарущенко. Научные ведомости Белгородского государственного университета. "История Политология Экономика Информатика". Научный рецензируемый журнал. №22(165). Выпуск 28/1, 2013 С.153-160.

158. Информационная технология оценки надежности программных средств с учетом вторичных дефектов / О.Н. Одарущенко , А.А. Руденко, Е.Б. Одарущенко. *Системи управління, навігації та зв'язку*. Полтавський національний технічний університет. Вип.1(33). Полтава, 2015. С.146-150.

159. Оцінювання кількості вторинних дефектів програмних засобів шляхом комплексування модифікованих моделей росту надійності Джелінські-Моранди і Шика-Волвертона / Одарущенко О.М. та ін. *Системи управління, навігації та зв'язку. Полтавський національний технічний університет*. 2020. Вип.1(59). С.97-100.

160. Одарущенко О.Н. О вопросе применения моделей надежности программных средств на этапе проектирования вычислительных устройств / О.Н. Одарущенко, Е.Б. Одарущенко, А.В. Харыбин// *Материалы 7-й Международной конференции «Теория и техника передачи, приема и обработки информации»*. – Харьков: ХТУРЭ, 2001. С. 319-320.

161. Одарущенко О.Н., Харыбин А.В. Анализ методических подходов к оценке надежности программного обеспечения телекоммуникационных систем. *Доклады 3-й научно-техн. конф. студентов, аспирантов и молодых специалистов стран СНГ "Техника и технология связи*". Одесса: УГАС им. А.С.Попова, 2001. С. 70-75.

162. Одарущенко О.Н., Руденко А.А. Модель Джелинского-Моранды с учетом недетерминированного числа вторичных дефектов. *Матеріали Третьої міжнародної науково-технічної конференції „Комп'ютерна математика в інженерії, науці та освіті*“ (CMSEE-2009), м. Полтава, 1-31 жовтня 2009 р. Київ: Видавництво НАН України, 2009. С. 49-50.

163. Одарущенко О.Н. Инвариантность простой экспоненциальной модели оценки надежности программного обеспечения при снятии допущения о невозможности внесения дефектов при восстановлении программных средств / О.Н. Одарущенко, А.А. Руденко // Четверта науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання систем (МОДС2'2009), 22-26 червня 2009 р., Київ. С.256-257.

164. Одарущенко О.Н. Модели оценки надежности программных средств с учетом вторичных дефектов как функции времени / О.Н. Одарущенко, А.А. Руденко, З.Н. Руденко // П'ята науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання систем. МОДС '2010''. Тези доповідей. Київ. 2010. 21-25 червня 2010 р. С. 226-228.

165. Одарущенко О.Н. Использование корреляционных зависимостей при прогнозировании числа вторичных дефектов программных средств / О.М. Одарущенко, А.А. Руденко // Матеріали Четвертої міжнародної науково-технічної конференції „Комп'ютерна математика в інженерії, науці та освіті“ (CMSEE-2010), м. Полтава, 1-31 жовтня 2010 р. Київ: Видавництво НАН України, 2010. С. 53-54.

166. Одарущенко О.Н. Определение параметров оценки надежности программных средств с учетом вторичных дефектов / О.Н. Одарущенко, А.А. Руденко // Шоста науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання систем. МОДС '2011''. Тези доповідей. Чернігів, 2010. 27-30 червня 2011 р. – С. 391-392.

167. Одарущенко О.Н. Использование многофрагментного моделирования для оценки надежности программных средств с учетом вторичных дефектов/ О.Н. Одарущенко, Е.Б. Одарущенко, А.А. Руденко, З.Н. Руденко// Сьома міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС ’2012’’. Тези доповідей. Чернігів-Жукин, 2012. 25-28 червня 2012 р. С. 344-346.

168. Одарущенко О.Н. Метод оценивания надежности программных средств с учетом вторичных дефектов / О. Н. Одарущенко, А.А. Руденко, З.Н. Руденко, М.А. Мельник// Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013. Тези доповідей. Чернігів-Жукин, 2013. 24-28 червня 2013 р. С. 336-339.

169. Антощук, С.Г., Маевский Д.А., Яремчук С.А. Проектирование количества ошибок на этапе эксплуатации адаптируемых учетных информационных систем. *Радіоелектронні і комп’ютерні системи*. 2010. № 6 (47). С. 204–210.

170. Одарущенко О.М., Одарущенко О.Б. Концепція і принципи оцінювання і забезпечення надійності та функціональної безпеки програмно-технічних комплексів.Сьома міжнародна науково-технічна конференція «Проблеми інформатизації». 2019. С.5.

171. Одарущенко О.М., Одарущенко О.Б. Метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах. Десята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління».2020. С.20.

172. Василенко Н.В., В.А. Макаров Модели оценки надежности программного обеспечения. *Вестник Новгородского государственного университета*. 2004. № 28. С. 126-132.

173. Гордеев А.А., Харченко В.С. Эволюция моделей качества программного обеспечения: методика и результаты анализа в контексте стандарта ISO 25010. *Системы обработки информации*. 2013. №6(113). С. 15-34.

174. Канер С.,Фолк Е., Нгуен К.Тестирование программного обеспечения. Москва.: DiaSoft, 2001. 544 с.

175. Коваль Г.И. Подход к прогнозированию надежности программного обеспечения при управлении проектом. *Проблемы программирования*. –2002. № 1 – 2. С. 282-290.

176. Лаврищева Е.М., Петрухин В.А. Методы и средства инженерии программного обеспечения: учебник. Московский физико-технический институт (государственный университет), 2006. 304 с.

177. Леффингуэлл Д, Уидриг Д. Принципы работы с требованиями к программному обеспечению. Унифицированный подход. Москва. Издательский дом «Вильямс», 2002. 448 с.

178. Липаев В.В. Обеспечение качества программных средств. Методы и стандарты. Москва. СИНТЕГ, 2001. 380 с.

179. Липаев В.В. Функциональная безопасность программного обеспечения. Москва. Синтез, 2004. 281 с.

180. Маевский Д.А., Яремчук С.А. Анализ моделей надежности программного обеспечения гарантоспособных информационных систем. *Електромашинобудування та електрообладнання*, *МНТК, Одесса, ОНПУ*, 2010 № 76, К:. Техніка, 2010 С. 68 -79.

181. Маевский Д.А. Моделирование надежности в теории динамики программных систем. *Электротехнические и компьютерные системы*. 2011. Вып. (04)80. С. 147-153.

182. Маевский Д.А., Яремчук С.А. Сравнительный анализ моделей надежности программного обеспечения на этапе эксплуатации. *Праці Одеського політехнічного університету*. 2011. Випуск 1 (35). С. 82-86.

183. Маєвський Д.А. Структурна динаміка програмних систем та прогнозування їх надійності при наявності вторинних дефектів. *Радіоелектронні і комп'ютерні системи*. 2010. №.3. С. 103-109.

184. Мороз Г.Б., Лаврищева Е.М. Модели роста надежности программного обеспечения. Киев. Препринт 92–38, 1992. 23 с.

185. Стандартизация разработки программных средств: учеб. пособие / В.А. Благодатских, В.А. Волнин, К.Ф. Поскакалов; под ред. О.С. Разумова. Москва.: Финансы и статистика, 2005. 288 с.

186. Фатуев В.П., Высоцкий В.И., Бушинский В.И. Надежность автоматизированных информационных систем: учебное пособие. Ташкент: ТГУ, 1998. 104 с.

187. Холстед М.Х. Начало науки о программах. Москва.: Финансы и статистика, 1981. 128 с.

188. Aital P., Sashikala P. Role of Software Reliability Models in Performance Improvement and Management. *Journal of Software Engineering and Applications*. 2012. № 5 P. 737-742.

189. A New Software Reliability Growth Model: Genetic-Programming-Based Approach. / Z. Al-Rahamneh, M. Reyalat, A.F. Sheta, S. Bani-Ahmad, S. Al-Oqeili . *Journal of Software Engineering and Applications*.– 2011. № 4. P. 476-481.

190. Performance Analysis of Software Reliability Models using Matrix Method. / R.P. Garg, K. Sharma, R. Kumar, R.K. Garg. *International Journal of Computer, Information, Systems and Control Engineering*. 2010. № 11. P. 31-38.

191. Goel A.L. Software reliability models: Assumptions, Limitations and Applicability . *IEEE Transactions on Software Engineering*, Vol. SE-11, № 12. 1985. P. 1411-1423.

192. Jelinski Z., Moranda P. Software reliability research. *Statistical computer performance evaluation W. Freiberger, Ed. Academic Pres*s. 1972. P. 465-484.

193. The Method of Software Reliability Growth Models Choice Using Assumptions Matrix / V.S. Kharchenko, O.M. Tarasyuk, V.V. Sklyar et al. *Proc. of 26th Annual Int. Computer Software and Applications Conference (COMPSAC). Oxford, England*, 2002. P. 541-546.

194. Lee C.H., Kim Y.T., Park D.H. S-Shaped Software Reliability Growth Models Derived from Stochastic Differential Equations. *IIE Transactions*. 2004. № 12. P. 1193-1199.

195. Lipow M. Model of Software Reliability. *Proceedings of the Winter Heeling of the Aerospase Division of the American Society of Mechanical Engineers, 1978*. 78-WA/Aero-18. P. 1-11.

196. Lyu M.R.. Handbook of Software Reliability Engineering. *IEEE Computer Society Press*., 1995. – 850 p.

197. Lyu M.R. Software Fault Tolerance. C*hichester, England: John Wiley and Sons, Inc.*, 1995. P. 109-138.

198. McCabe T.A. Complexity Measure. *IEEE Transactions on Software Engineering*. 1976. 4, N. SE-2. P. 308-320.

199. Maevsky D. A., Maevskaya A.A., Leonov H.D. Software reliability. Non-probabilistic approach. RT&A # 03 (26),2012. P. 8-20.

200. Mahapatra G.S., Roy P. Modified Jelinski-Moranda Software Reliability Model with Imperfect Debugging Phenomenon. *International Journal of Computer Applications*. 2012. № 18. P. 38-46.

201. Software Reliability Prediction Model Analysis / L. Mirtskhulava, M. Khunjgurua, N. Lomineishvili, K. Bakuria. *International Journal of Computer, Information, Systems and Control Engineering*. 2014. № 6. P. 927-932.

202. Moranda P.B. Event-Altered Rate Models for General Reliability Analysis. *IEEE Trans. on Reliability*. 1979. Vol. R-28, N 5. P. 376-381.

203. Musa J.D. A theory of software reliability and its application. *IEEE Trans. Rel*. 1979. Vol. R-28. P. 181-191.

204. Musa J.D., Okumoto K.A. Logarithmic Poisson Time Model for Software Reliability Measurement. *Proc. Sevent International Conference on Software Engineering*. Orlando, Florida. 1984. P. 230-238.

205. Musa J.D. Software Reliability. Measurement. Prediction. Application. USA: McGraw-Hill Company. 1987. 395 p.

206. Shick G.J., Wolverton R.W. An analysis of computing software reliability models. *IEEE Tras. Software Eng*. V. SE–4. № 2. 1978. P. 104-120.

207. Trivedi K.S. Analytical Models for Architectural-Based Software Prediction: A Unification Framework. IEEE Transactionson Reliability. 2006. № 4. P. 578-590.

208. Шафер Д, Фатрелл Р., Шафер. Л. Управление программными проектами: достижение оптимального качества при минимуме затрат. Москва. Вильямс, 2003. 1136 с.

209. Одарущенко О.Н., Одарущенко Е.Б., Поночовный Ю.Л. Сегментация многомерного пространства входных данных программного обеспечения. *Труды четвертой международной научно-практической конференции «Современные информационные и электронные технологии»*. Одесса:Одесский национальный политехнический университет, 2003. С.110.

210. Одарущенко О.Н., Поночовный Ю.Л. Надежность, как критерий качества программного обеспечения. *Матеріали Міжнародної науково-технічної конференції «Інтегровані комп'ютерні технології в машинобудуванні – ІКТМ-2003»*. Харків: Національний аерокосмічний університет «ХАІ», 2003. С.221.

211. Haapanen P., Helminen A.Failure Mode and Effects Analysis of Software–Based Automation Systems. *Radiation and Nuclear Safety Authority (STUK)*, Vantaa, Finland, 2002. P. 37.

212. Оценка и обеспечение качества программных средств космических систем / В.С. Харченко и др.; под ред. Харченко В.С. Харьков: Нац. аэрокосмический ун-т «ХАИ», 2007. 244 с.

213. Харченко В.С., Скляр В.В., Клименко О.М. Оценка точности матрично–графового метода выбора моделей надежности программных средств. *Электронное моделирование*. 2003. Т. 25, № 3. С. 59–72.

214. Харченко В.С., Скляр В.В., Бєлий Ю.О. Метод оцінки якості програмного забезпечення енергетичних комплексів з використанням операцій над графами. *Вісник Харківського державного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України*. Вип. 43, Том 2. Харків, 2006. С. –122.

215. Pullum, L. Software fault tolerance techniques and implementation. Artech House computing library, 2001. 343 p.

216. Trivedi K. S., Malhotra M., Muppala J. K. Stiffness-tolerant methods for transient analysis of stiff Markov chains. Microelectronic Reliability. 1994. № 34(11). P. 1825 – 1841.

217. Derisavi S., Hermanns H., Sanders W. H. Optimal state-space lumping in Markov chains. *Information Processing Letters*. 2003. №87(6). P. 309 – 315.

218. The Möbius state-level abstract functional interface. /S. Derisavi, P. Kemper, W. H. Sanders, T. Courtney. *In proc. of the 12th int. conf. on modelling techniques and tools for computer performance evaluation*. UK, London, 14 – 17 April, 2002. P. 31 – 50.

219. А.с. 57120 Комп`ютерна програма «MSMC – Method selector for Markov chains» / В. О. Бутенко, В. С. Харченко, Д. А. Бутенко, О. М. Одарущенко, О. Б. Одарущенко. № 57120; заявка 05.10.2014; реєстр. 17.11.2014. – 1 с.

220. Markov renewal theory applied to performability evaluation. / R. Fricks, M. Telek, A. Puliafito, K. S. Trivedi. *IEEE Explore: proc. Int. symp. on fault-tolerant computing (FTCS)*. USA, Wisconsin, Madison, June 15 – 18, 1999. P. 15 – 48.

221. Avizienis A. Fault–tolerance: the survival attribute of digital systems. *IEEE Trans. of Computers*. 1978. V. 66, N. 10. P. 1109–1026.

222. Basic concepts and taxonomy of dependable and secure computing. / *A.*

Avizienis, J.-C. Laprie, Randell, C. Landwehr. *IEEE Transactions on dependable and secure computing*. 2004. Vol. 1, № 1. P. 11-33.

223. Avizienis A., Lapri J.-C. Dependable Computing: From Concepts to Design Diversity. *Proceedings IEEE.* 1986. V. 74, N. 5. P. 8–21.

224. J.-C. Laprie. Dependability: Basic Concepts and Terminology. *Dependable Computing and Fault-Tolerant Systems*. 1992. Vol. 5. P. 265.

225. Achieving and assuring high availability / K. S. Trivedi, G. Ciardo, B. Dasarathy, M. Grottke, A. Rindos, B. Vashaw. *IEEE Explore: proc. of the 13th IEEE workshop on dependable parallel & distributed processing*. USA, Florida, Miami, 14 – 18 April, 2008. P. 1 – 7.

226. Archana S., Srinivasan R., Trivedi K. S. Availability models in practice. *IEEE Explore: proc. int. workshop on fault-tolerant control and computing.* Korea, Seoul, 22 – 23 May, 2001. P. 1 – 28.

227. Odarushchenko O., Kharchenko V., Odarushchenko V. Multi-fragmental availability models of critical infrastructures with variable parameters of system dependability, information & security. *Information and Security. An International Journal*. 2012. Vol. 28, № 2. P. 248 – 265.

228. Многоверсионные системы, технологиии, проекты. / В.С. Харченко и др.; под ред. В.С. Харченко. Харьков: Нац. аерокосмічний ун-т «ХАИ», 2003. 486 с.

229. Бабаков М. Ф., Попов А. В., Луханин М. И. Математические модели электронных аппаратов и систем: Учеб. пособие. Харьков: Нац. аэрокосмический университет «ХАИ», 2003. 109 с.

230. Markov renewal theory. Markov renewal theory applied to performability evaluation / Fricks R., Telek M., Puliafito A., Trivedi K.. Annual Int. Symp. Fault Tolerant Computing (FTCS). 1999. №6. P.15-48.

231. Технологии высокой готовности для программно-технических комплексов космических систем / Одарущенко О.Н и др.; под ред. В.С. Харченко, Б.М. Конорева. Харьков, 2010. 372с.

232. Безопасность критических инфраструктур:математические и инженерные методы анализа и обеспечения/ Одарущенко О.Н. и др.; под. ред. В.С. Харченко. Харьков, 2011.641с.

233. Оценка надежности программно-технических комплексов на основе многофрагментных марковских моделей / О.Н. Одарущенко и др. *Системи обробки інформації. Збірник наукових праць НАНУ, ПАНМ, ХВУ*. 2001. Вип 3(13), С.110-116.

234. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем / О.Н. Одарущенко и др. *Авіаційно-космічна техніка і технологія. Збірник наукових праць Національний аерокосмічний університет «ХАІ»*. 2002. Вип.35, С.187-191.

235. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов / О.Н. Одарущенко и др. *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ»*. 2006. Вип.5(17), С.62-70.

236. Одарущенко О.Н., Одарущенко Е.Б., Медведь Ю.Г. Методика разработки многофрагментных марковских моделей оценки надежности отказоустойчивых компьютерных систем. *Інформаційні технології та комп'ютерна інженерія. Міжнародний науково-технічний журнал. Вінницький національний технічний університет*. Вип.1(18). Вінниця, 2007. С.57-63.

237. Принципы анализа и управления безопасностью критических инфраструктур / О.Н. Одарущенко и др. *Вісник Хмельницького національного університету*. 2010. Вип.5. С.218-221.

238. Odarushchenko O., Kharchenko V., Odarushchenko V. Multi-fragmental availability models of critical infrastructures with variable parameters of system dependability, information & security. *Information and Security. An International Journal*. 2012. Vol. 28, № 2. P. 248 – 265.

239. Анализ архитектур отказоустойчивых серверов для оценки их надежности /О.Н. Одарущенко, Е.Б. Одарущенко, В.С. Харченко, С.В. Живило. *Радіоелектронні і комп'ютерні системи науково-технічний журнал*. Національний аерокосмічний університет «ХАІ». Вип.7(59).Харків, 2012. С.60-67.

240. Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Availability assessment of computer systems described by stiff Markov chains: case study. *Springer.CCIS (412)*. 2013. – P. 112 – 135.

241. Метрико-интервальные модели и инструментальные средства для оценивания готовности информационно-управляющих систем с использованием марковских процессов / О.Н. Одарущенко и др. *Системи обробки інформації. Науково-технічний журнал. Харківський університет Повітряних Сил імені Івана Кожедуба*. 2014. Вип 9(125). С.59-64.

242. Kharchenko V, Butenko V, Odarushchenko O., Sklyar V. Multi-fragmentation Markov Modeling of a Reactor Trip System. *Journal of Nuclear Engineering and Radiation Science (ASME_Journal_of_NE_&_RS (in prep)*. 2015. (10 pages).URL:https: // asmedigitalcollection.asme.org / nuclearengineering/articleabstract /1/3/031005/472772/Multifragmentation-Markov-Modeling-of-a-Reactor?redirectedFrom=fulltext (дата звернення: 25.02.2021).

243. The Imbedded Markovian Models of Computer Systems Taking into Account a Variation of Failure and Recovery Rates / O. Odarushchenko, V. Kharchenko, Olena. Odarushchenko, Y. Ponochovniy, E. Zaitseva, S. Zasukha // Management Science and Informatics in Žilina (FMSI) Special session on risk analysis and system reliability. *7th International Conference on digital technologies, circuits, systems and signal processing*. November 11-12 2010, Žilina - Slovak Republic ISBN: 9788055403045.

244. Odarushchenko, O., Kharchenko, V. Availability models of critical infrastructures with variable system dependability parameters. *Proceedings of the first International Workshop Critical Infrastructure Safety and Security. CrISS-*

DESSERT 2011. (May 11-13, 2011, Kirovograd). Kirovograd, Ukraine. P. 319-330.

245. Одарущенко О.Н., Харченко В.С., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем. Матеріали 1-ої Міжнар. науково-техн. конф. „Гарантоспроможні (надійні та безпечні) системи, сервіси та технології - DESSERT-2006". Полтава: Полтавський військовий інститут зв'язку, 2006. С. 12.

246. Одарущенко О.Н., Одарущенко Е.Б., Поночовный Ю.Л. Имитационное моделирование отказоустойчивых компьютерных систем с дискретно изменяющимися параметрами потоков отказов и восстановлений: принципы, алгоритмы, результаты. *Мат. 2-ої Міжнар. науково-техн. конф. „Гарантоспроможні (надійні та безпечні) системи, сервіси та технології - DESSERT-2007"*. Кіровоград: ЗАТ «Радій», 2007. С. 9.

247. Системы и технологии высокой готовности. Лекционный материал / Одарущенко О.Н. и др. под ред. О.Н. Одарущенко, В.С. Харченко: Харьков: Национальный аэрокосмический университет «ХАИ», 2013. 273с.

248. Системы и технологии высокой готовности. Практикум /Одарущенко О.Н. и др. под ред. О.Н. Одарущенко, В.С. Харченко. Харьков: Национальний аэрокосмический университетим. Н.Е. Жуковского «ХАИ», 2013. 96 с.

249. Комп'ютерна програма «MSMC-Method selector for Markov chains». Свідоцтво про реєстрацію авторського права на твір №57120.-Дата реєстрації 05.10.2014.

250. Selecting mathematical software for dependability assessment of computer systems described by stiff Markov chains / V. Kharchenko, O. Odarushchenko, V. Odarushchenko, P. Popov. *ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer : proc. of the 9th Int. Conf. ICTERI 2013*, Kherson, 19 – 23 June, 2013. K., 2013. P. 146 – 162.

251. Butenko V., Odarushchenko O., Kharchenko V. Analysis of markov chains for high availability systems: metric-based approach. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013*. (May 23-26, 2013). Sevastopol, Ukraine, 2013. P.16.

252. Odarushchenko, O., Kharchenko, V, Butenko, D, Butenko V. Assessment of the Reactor Trip System Dependability Two Markov Chains - based Cases. *Proceedings of the 10th International Conference on Digital Technologiesю.* (July 9-11, 2014, Zilina). Zilina, Slovakia, 2014. P. 103-109.

253. Butenko V., Kharchenko V., Odarushchenko O., Popov P., Sklyar V., Odarushchenko E. Markov's Model and Tool-Based Assessment of Safety-Critical I&C Systems: Gaps of the IEC 61508**.** *12-th International Conference on Probabilistic Safety Assessment and Modeling*. 2014. Proceeding of 12-th International conference on probabilistic safety assessment and modeling. USA. Hawaii. Honolulu. URL: http: // iapsam.org / psam12 / proceedings / paper /paper_455_1.pdf (дата звернення 17.02.2021).

254. Odarushchenko O., Kharchenko, V. Butenko V., Odarushchenko, E. Markov's Modeling of NPP I&C Reliability and Safety Optimization of tool-and-technique selection. *Proceeding of Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management* (February 15-18, 2016, Beer Sheva). Beer Sheva, Israel, 2016. P. 328 – 336.

255. Одарущенко О.Н., Одарущенко Е.Б., Яковлев В.И. Оценка надежности вычислительных систем с учетом изменения параметров отказов и восстановлений их программных средств. Материалы 8-й Международной конференции «Теория и техника передачи, приема и обработки информации» (Интегрированные информационные системы, сети и технологии). Харьков: ХНУРЭ, 2002. С. 269-271.

256. Mathematical software for modeling the computer systems described by stiff Markov chains: an empirical evaluation and choosing a solution /O.Odarushchenko, V. Kharchenko, V. Odarushchenko. *ICT in Education, Research*

and Industrial Applications: Integration, Harmonization and Knowledge Transfer : тез. доп. 9th Int. Conf. ICTERI 2013., 19 – 23 June, 2013. Kherson, 2013. P. 24.

257. Odarushchenko O., Kharchenko V., Butenko V., Odarushchenko E. Assessing of programmable system availability in context of the IEC 61508. *Program 7th International conference - Dependable Systems, Services and Technologies DESSERT2014*. (May 16-18, 2014). Kiev, Ukraine P.21.

258. Odarushchenko, O. Odarushchenko, E, .Butenko, V., Ruchkov, E. Tool-Based Assessment of Reactor Trip Systems Availability and Safety Using Markov Modeling. *Cyber Security and Safety of Nucler Power Plant Instrumentation and Control Systems*. Hershey, Pennsylvania, United States of America, IGI Global, 2020. P. 175-203.

259. Модели отказов информационно-управляющих систем на основе самодиагностируемых программируемых платформ в системах аварийной защиты реакторов / О.Н. Одарущенко и др. *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ».* 2015. №4, С.19-24.

260. Kharchenko V., Odarushchenko E., Butenko V., Moskalets V., Strjuk O. Application of Markov Modeling for Safety Modeling for Safety Assessment of Self-Diagnostic Programmable Instrumentations and Control Systems. *Central European Researchers Journal*. Vol.2 Issue 2. URL: http://ceres-journal.eu/iss160202 (дата звернення: 25.02.2021).

261. Марковьскі моделі оцінювання функціональної безпеки програмно-технічних комплексів на самодіагностовних програмовних платформах з урахуванням помилок засобів контролю / О. М. Одарущенко та ін. *Радіоелектронні і комп'ютерні системи науково-технічний журнал. Національний аерокосмічний університет «ХАІ».* 2019.№4(92).С.17-29.

262. Odarushchenko O., Ivasyuk O., Bulba E. Fault injection-based technique and tool for FPGA modules safety assessment. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013.* (May 23-26,

2013). Sevastopol, Ukraine, 2013. P.14.

263. Одарущенко О.Н., Одарущенко Е.Б. Оценка надежности восстанавливаемых управляющих и вычислительных систем с учетом характеристик средств контроля в условиях дефектов программных и аппаратных средств. Тези доповідей науково-технічної конференції. Харків: ХВУ, 1999.Вип.3.С.38-39.

264. Отказобезопасные информационно-управляющие системы на программируемой логике :монография / под ред. В. С. Харченко, В. В. Скляра. Х. : Кировоград, 2008. 380 с.

265. Харченко В.С., Скляр В.В., Герасименко А.Д. Модели надежности информационно–управляющих систем с сетевым многоярусным мостиковым мажоритированием. *Радіоелектронні і комп'ютерні системи*. 2007. № 6(25). С.196–201.

266. Харченко В.С., Скляр В.В., Аль–Тарази А.Х. Модели состояний и событий отказоустойчивых информационно–управляющих систем с учетом их влияния на безопасность / *Радіоелектронні і комп'ютерні системи.* 2004. № 2.– С. 67–74.

267. Сиора А.А., Краснобаев В.А., Харченко В.С. Отказоустойчивые системы с версионно–информационной избыточностью. Харьков: Нац. аэрокосмический ун-т "ХАИ", 2009. 321 с.

268. Diversity and Security of Computing Systems: Points of Interconnection. Part 2: Methodology and Case Study / I. Komari Elyasi, V. Kharchenko, A. Romanovsky, E. Babeshko, I. Lysenko. *Masaum Journal of Open Problems in Science and Engineering (MJOPSE)*. Masaum Network, 2009. V. 1, N 1. P.33–41.

269. Одарущенко О.Н. Оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для програмно-технічних комплексів інформаційно-керуючих систем. *Системи управління, навігації та зв'язку. Полтавський національний технічний університет*. 2020. Вип.3(61). С.90-93.

270. Multi–Version Systems and Technologies for Critical Applications / A. Volkovoj, I. Lysenko, V. Kharchenko, O. Shurygin; editor V. Kharchenko. National Aerospace University “KhAI”, 2009. 231 p.

271. Preckshot, G. Method for Performing Diversity and Defense–in–Depth Analyses of Reactor Protection Systems. NUREG/CR–6303. U.S. Nuclear Regulatory Commission, Lawrence Livermore National Laboratory, 1994. 45 p.

272. Kharchenko V.S., Siora A.A., Bakhmach E.S. Diversity–Scalable Decisions for FPGA–based Safety–Critical I&Cs: from Theory to Implementation. *International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human–Machine Interface Technologies: proceedings of the 6th International Topical Meeting*.– Knoxville, Tenessi, USA, 2009. P.143–150.

273. Поморова О. В. Теоретичні основи, методи та засоби інтелектуального діагностування комп’ютерних систем: дис. докт. техн. наук : 05.13.13 / Поморова Оксана Вікторівна ; Хмельницький національний університет. Х.:, 2007. 410 с.

274. ПЛИС-платформа в критических приложениях: Гарантоспособные масштабируемые решения для информационных и управляющих систем АЭС/ Е.С. Бахмач, А.А. Сиора, В.В. Скляр, В.И. Токарев, В.С. Харченко. *Радіоелектронні і комп’ютерні системи*. 2008. № 6 (33). С. 12-19.

275. Модель и инструментальная поддержка анализа сигналов при оценке функциональной безопасности FPGA-модулей / О.Н. Одарущенко и др. *Системи обробки інформації. Науково-технічний журнал. Харківський університет Повітряних Сил імені Івана Кожедуба*. 2013. Вип 4(111).С.20-22.

276. Обеспечение тестового покрытия для электронных проектов FPGA при оценивании функциональной безопасности по критериям SIL3 / О.Н. Одарущенко и др. *Системи обробки інформації. Науково-технічний журнал. Харківський університет Повітряних Сил імені Івана Кожедуба*. 2013. Вип 5(112). С.62-65.

277. Моделі математичних блоків дискретного перетворення інформації

для верифікації програмного забезпечення програмованих логічних контролерів / О.Н. Одарущенко и др. *Системи управління, навігації та зв'язку. Полтавський національний технічний університет*. 2017. Вип.4. С.273-280.

278. Odarushchenko O., Kharchenko V., Sklyar V, Ivasuyk A. Fault-Injection Testing: FIT-Ability. *Proceedings of East-West Design&Test Symposium EWDTS"2013*. (September 27-30, 2013). Ростов на Дону, Росія, 2013. P.188-192.

279. Odarushchenko O., Kharchenko V, Sklyar V, Ivasyuk A. Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues. Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication ICONE22. (July 7-11, 2014, Prague). Prague, Czech Republic, 2014. Volume 6: Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. URL: https: // asmedigitalcollection.asme.org /ICONE/ICONE22/volume/45967. (Дата звереннння: 01.03.2021).

280. Odarushchenko O., Kharchenko V, Gordieiev O., Vilkomir S. t-Wise-Based Multi-Fault Injection Technique for the Verification of Safety Critical I&C Systems. *Procceding of 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT.* (February 22-26, 2015). Charlotte, USA, 2015. P. 1827-1836.

281. Odarushchenko O., Kharchenko, Sklyar, V. Multi-Fault Injection Testing: Cases for FPGA-Based NPP I&C Systems. *Proceedings of 23rd International Conference on Nuclear Engineering ICONE-23*.(May 17-21, 2015). Chiba, Japan, 2015. URL: https: // inis.iaea.org / search/search.aspx?orig_q=RN:48025087 (Дата звереннння: 01.03.2021)..

282. Odarushchenko O., Babeshko E., Kharchenko V., Sklyar V. Toward automated FMEDA for complex electronic products. *Proceedings of the International Conference on Information and Digital Technologies* (July 7-9, 2015, Zilina). Zilina, Slovakia, 2015. P. 17-22.

283. Odarushchenko O., Strjuk O., Bulba Y., Leontiiev K., Ivasyuk A., Kharchenko V. Fault insertion software and hardware testing for safety PLC-based system SIL certification. *Proceeding of the 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018* (May 24-27, 2018, Kyiv). Kyiv, Ukraine, 2018. P. 202-206.

284. Babeshko, E., Kharchenko, V., Odarushchenko, O., Leontiiev, K., Strjuk, O. NPP I&C Safety Assessment by Aggregation of Formal Techniques. *Proceedings of the 2018. 26th International Conference on Nuclear Engineering ICONE26*. (July 22-26, 2018, London). London , England. P. 1-6.

285. Babeshko E., Kharchenko V., Gorbenko A. Applying F(1)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring. *Proceeding of IEEE DepCoS-RELCOMEX Conference.* June 26-28, 2008 Szklarska Poreba. Poland. 2008. P.309-315.

286. Nggada S.H. Software Failure Analysis at Architecture Level Using FMEA. *International Journal of Software*. 2012. № 6 P. 61-74.

287. Odarushchenko O., Sklyar V., Bulba E., Horbenko R., Ivasyuk A., Kotov D. Assessment of Energy Consumption for Safety-Related PLC-based Systems. *Green IT Engineering: Concepts, Models, Complex Systems Architectures, Studies in Systems, Decision and Control series*. Springer. Springer International Publishing Switzerland 2017. V.Kharchenko et al. (eds.), 2017. P. 269 – 281.

288. Odarushchenko O., Odarushchenko E, Strjuk O., Leontiiev K., Software Fault Insertion Testing for SIL Certification of Safety PLC-based System. *Proceeding of The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020* (May 14-18, 2020). Kiev, Ukraine P.80-84.

289. Основи побудови АСУ /Барсов В.І., Одарущенко О.М., Краснобаєв В.А., Тиртишніков О.І., Барсова З.В./ Під загальною редакцією В.І. Барсова: Підручник для студентів ВНЗ.-Полтава:2012.-400с.

290. Бабешко Е.В., Ильяшенко О.А., Харченко В.С. Многоэтапный

анализ надежности и безопасности информационно управляющих систем. *Радиоэлектронные и компьютерные системы*. Харьков: "ХАИ". 2010. № 7(48). С. 283-287.

291. Волковой А.В., Скляр В.В., Харченко В.С. Метод формирования моделей многоверсионного жизненного цикла для программных проектов. *Інформаційно–управляючі системи на залізничному транспорті.* 2004. № 2. С. 40–44.

292. Radiy. Продукция для АЭС. URL: http://radiy.com/ru/produktsiya-dlya-aes/produktsiya/platforma-radics.html

293. Модельний спосіб розроблення алгоритмів цифрових систем на програмованих логічних інтегральних схемах/ О.М. Одарущенко та ін. *Кібернетика і системний аналіз*, 2020, том 56, №5. С.29-37.

294. Університетсько-індустріальна кооперація. Модельно-орієнтований підхід. Практичне керівництво та приклади /Харченко В.С., Скляр В.В.. Одарущенко О.М., Одарущенко О.Б. та інш./ Під ред Харченка В.С. – Міністерство освіти і науки України, Національний

295. Grassman W., Taksar M, Heyman D. Regenerative analysis and steady state distribution for Markov chains. *Operations Research*. 1985. № 33. P. 1107 – 1116.

296. Hairer E., Wanner G. Solving Ordinary Differential Equations II: Stiff and Differential Algebraic Problems. Springer, 2010. 631 p.

297. PERFORM Performability Engineering Research Group. Möbius: Model-based environment for validation of system reliability, availability, security, and performance.– University of Illinois at Urbana-Champaign. URL: http://www.perform.csl.uiuc.edu/mobius/manual/ MobiusManual.pdf, n. – 2005.

298. Sanders W. H., Meyer J. F. Reduced base model construction methods for stochastic activity networks. *IEEE journal on selected areas in communications*. 1991. Vol. 9, № 1. P.25 – 36.

299. Buchholz, P. Efficient computation of equivalent and reduced representations for stochastic automata. *Int. Journal of computer systems science and*

engineering. 2000. Vol. 15, № 2. P. 93 – 103.

300. Bobbio A., Trivedi K. S. An aggregation technique for transient analysis of stiff Markov chains. *IEEE Trans. on comp*. 1986. C(35). P. 803 – 814.

301. Харченко В.С. Гарантоздатність комп'ютерних систем: межа універсальності в контексті інформаційно-технічоного стану. *Радіоелектронні і комп'ютерні системи*. 2007. № 8. С.8-16.

302. Макконнелл С. Совершенный код. Мастер-класс. Пер. с англ. / С. Макконнелл – М.: Издательско-торговый дом «Русская Редакция»; Санкт Петербург.: Питер, 2005. 896 с.

303. Sanders J. Software Quality – A Framework for Success in Software Development and Support / J. Sanders. – USA: Addis. Wesley, 1994. 112 p.

304. William M. Goble, Harry Cheddie ISA-The Instrumentation, Systems, and Automation Society, 2005 - 382 стор. Safety Instrumented Systems Verification: Practical Probabilistic Calculations.

305. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security/ V. Kharchenko [et al.]. – IGI Global, 2014. 470 p

306. Butenko, V. Modeling of a reactor-trip system using Markov chains: case study / V. Butenko // Proc. of the 22nd Int. Conf. on Nuclear Engineering. – Czech Republic, Prague, July 7 – 11, 2014. P. 1 – 10.

307. URL: https://www.liga.net/incidents/articles/pochemu-oni-padayut-vse-26-000-aviakatastrof-za-100-let-v-semi-grafikah (дата звернення: 19.03.2021).

308. Скляр В.В., Харченко В.С., Ястребенецкий М.А. Цифровые информационные и управляющие системы атомных электростанций и ракетно–космических комплексов: Сравнительный анализ, тенденции развития, обеспечение безопасности. *Ядерная и радиационная безопасность.* 2004. Т. 7, № 2. С. 35-41.

309. Бутенко В. О. Информационная технология выбора инструментальных средств для оценивания готовности информационно-управляющих систем с использованием марковских моделей: дис. к-та техн. наук : 05.13.06 / Бутенко Валентина Олеговна ; НАУ «ХАИ». Х., 2015. 218 с.

310. Харченко В.С. Парадигмы и принципы гарантоспособных вычислений: состояние и перспективы развити. *Радіотехнічні й комп'ютерні системи*. 2009. №2 (36). С. 91 – 100.

311. . The Möbius framework and its implementation / D. D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. M. Doyle, W. H. Sanders, P. G. Webster. IEEETransaction on Software Engineering. 2002. Vol. 28, № 10. P. 956 – 969.

312. Розен Ю.В., Ястребенецкий М.А. Новые нормативные документы, регламентирующие требования к информационным и управляющим системам, важным для безопасности АЭС. *Ядерна та радіаційна безпека 2(62)*. 2014. с.50-64.

313. Lakshmanana I., Ramasamya S. Selection of Right Software Reliability Growth Models for Every Software Project. *International Journal of Control Theory and Applications*. Volume 9. Number 40. 2016. P.807-817.

314. Hobbs C.. Embedded Software Development for Safety-Critical Systems. Taylor & Francis Group, LLC CRC Press. 2016. p. 342.

315. Бабешко Є., Ілляшенко О., Харченко В. Функційна безпека індустріальних систем:біла книга. Стандарт IEC 61508. Технічний комітет 185 «Промислова автоматизація», Київ. 2019. с.37. URL: https://tk185.appau.org.ua/functional-safety/ (дата звернення: 11.03.2021).

316. Phillip A. Laplante. Requirements Engineering for Software and Systems. CRC Press. Taylor&Francis Group, LLC. 2018.p. 399.

317. Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties. World Nuclear Association. Registered in England and Wales. Report No. 2020/001. 2020. P. 36. URL: https://www.world-nuclear.org/getmedia/966e6b51-d109-49ab-8c9f-a12f5d8e7b06/CORDEL-Current-Status-2020.pdf.aspx (дата звернення: 11.03.2021).

Додаток А. ПОКАЗНИКИ, ПАРАМЕТРИ, СИСТЕМНІ ПОЗНАЧЕННЯ, ВИЗНАЧЕННЯ

$K_г(t)$ – коефіцієнт (функція) готовності

$P_{ог}(t)$ - коефіцієнт (функція) оперативної готовності

PFD_{avg} – ймовірність неспрацювання функції безпеки після подачі сигналу на її включення

PFH- очикувана частотність настання аварій і, таким чином, інтенсивність запиту на виконання функції безпеки

N_d - кількість залишкових дефектів ПЗ після їх розробки

$P_n(t,\tau_{set})$ - ймовірність безпомилкового виконання програми

λ_d - інтенсивність прояву дефекту ПЗ (інтенсивність прояву дефекта проектування ПЗ)

f_d – відносна частота прояву дефектів

$N_{d(in)}$ - відома кількість штучно внесених дефектів

N_{d1}- кількість виявлених дефектів в ході тестування

$P_a(t_i)$ - ймовірність безвідмовного (безпомилкового) виконання програм на і-му часовому інтервалі

λ_{di} - інтенсивність прояву ДП на і – му інтервалі

T_b - початкове значення середньої наробки на відмову (прояву ДП ПЗ)

K_m - коефіцієнт, який враховує "ущільнення" часу тестування й налагодження відносно реального часу функціонування системи

$\tau_{set(add)}$ - додатковий час налагоджування

τ_{renew} - час відновлення (виявлення, діагностика, усунення) після прояву чергового ДП ПЗ

μ_d - інтенсивність відновлення системи після прояву ДП ПЗ

$\mu_{d(min)}$ – мінімальна інтенсивність відновлення системи після прояву ДП ПЗ

$\mu_{d(max)}$- максимальна інтенсивність відновлення системи після прояву ДП ПЗ

T_d - середній час необхідний для проведення діагностики, усунення та

відновлення роботи системи

T_{in} - початкове значення часу відновлення

τ_{pp} -час налагоджування програми

n^{in}- кількість вторинних дефектів ПЗ

E_{crit} - програмне значення здатності людського мозку, що характеризує його можливості обробляти п'ять "об'єктів"

K_r - відношення обсягу лінійного тексту до вихідного обсягу програми

V_1 - обсяг лінійного тексту програми

$V_р$ - вихідний обсяг програми

N_{def_in} - число виявлених власних дефектів ПЗ

N_{def_add} - число спеціально внесених в програму дефектів

N_{def} -обчислене значення ДП ПЗ

Надійність (dependability) – властивість об’єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування.

Безвідмовність (reliability) – властивість об’єкта безперервно надавати коректні (необхідні) послуги;

Готовність (availability) – властивість доступності ресурсів об’єкта для надання необхідних послуг;

Функційна безпечність (safety) - властивість виключати або мінімізувати шкідливі (катастрофічні) наслідки при відмовах для користувачів, інших систем або навколишнього середовища;

Інформаційно- технічний стан - під ІТС слід розуміти сукупність властивостей і ознак як технічного, так і інформаційного характеру, притаманних системі в певний момент часу.

Додаток Б. РЕЗУЛЬТАТИ ОЦІНЮВАННЯ ГОТОВНОСТІ ПТК ДУБЛЬОВАНИХ АРХІТЕКТУР

1. Результати оцінювання готовності (функційної безпечності) ПТК S_{21} у відповідності до ББМ1 представлено в таблиці В.1. Колонки таблиці мають наступні означення: T,г – час дослідження готовності (час інтегрування СДУ); $P_n(t)$ – ймовірність знаходження системи у відповідному стані базової багатофрагментної марковської моделі; A(t) – функція готовності. Показник функційної безпечності, а саме PFD_{avg} є функцією неготовності U(t), а саме доповненням A(t) до одиниці. Аналіз результатів моделювання архітектури ПТК S_{21} за різними ББМ дає інформацію, що комбінації параметрів моделювання значно впливають на час переходу системи у сталий стан. Тому вірний вибір ББМ із множини має значення з точки зору ризиків переоцінювання або недооцінювання шуканих показників. Аналіз табличної інформації та графічного представлення дає змогу встановити , що найбільший приріст надійності і функційної безпечності дає стан стан S_{10} (ймовірність $P_{10}(t)$). В інтервалі часу від 0 годин до 14000 годин маємо період приробки та усунення дефектів проєктування. Стан S_{10} характеризується тим, дефекти проєкутвання усунено и далі перехід у непрацездатний стан можливий лише за умовою прояву фізичного дефекту в одному з двох каналів ПТК.

Таблиця В.1

Результати оцінювання готовності (функційної безпечності) ПТК S_{21} у відповідності до ББМ1

T,г	$P_1(t)$	$P_2(t)$	$P_3(t)$	$P_4(t)$	$P_5(t)$	$P_6(t)$	$P_7(t)$	$P_8(t)$	$P_9(t)$	$P_{10}(t)$	$P_{11}(t)$	A(t)	U(t)
999	0,227894	0,011518	0,001721	0,417775	0,020451	0,002091	0,252991	0,012005	0,000629	0,050596	0,002329	0,949256	0,050744
1999	0,054655	0,002762	0,000413	0,261695	0,01297	0,001313	0,415607	0,020206	0,001038	0,218898	0,010443	0,950854	0,049146
2999	0,013108	0,000662	9,90E-05	0,125069	0,006222	0,000628	0,396395	0,019417	0,000992	0,417279	0,020129	0,95185	0,04815
3999	0,003144	0,000159	2,37E-05	0,054033	0,002693	0,000271	0,308764	0,015175	0,000773	0,58653	0,028435	0,95247	0,04753
5000	0,000754	3,81E-05	5,70E-06	0,022232	0,001109	0,000112	0,218108	0,010738	0,000546	0,711761	0,034595	0,952856	0,047144
5999	0,000181	9,14E-06	1,37E-06	0,00891	0,000445	4,48E-05	0,146146	0,007202	0,000366	0,797859	0,038836	0,953096	0,046904
6999	4,34E-05	2,19E-06	3,28E-07	0,003517	0,000176	1,77E-05	0,09501	0,004685	0,000238	0,854674	0,041637	0,953244	0,046756
7999	1,04E-05	5,26E-07	7,86E-08	0,001376	6,87E-05	6,91E-06	0,060672	0,002993	0,000152	0,891279	0,043442	0,953337	0,046663
9000	2,49E-06	1,26E-07	1,88E-08	0,000535	2,67E-05	2,69E-06	0,038328	0,001891	9,60E-05	0,914528	0,044589	0,953394	0,046606
10000	5,98E-07	3,02E-08	4,52E-09	0,000208	1,04E-05	1,04E-06	0,024054	0,001187	6,03E-05	0,929168	0,045311	0,95343	0,04657
10999	5,98E-07	7,25E-09	1,08E-09	8,04E-05	4,01E-06	4,04E-07	0,015035	0,000742	3,77E-05	0,938337	0,045764	0,953453	0,04647
11999	5,98E-07	1,74E-09	2,60E-10	3,11E-05	1,55E-06	1,56E-07	0,009374	0,000463	2,35E-05	0,944061	0,046046	0,953466	0,046534
12999	5,98E-07	4,17E-10	6,23E-11	1,20E-05	6,00E-07	6,03E-08	0,005836	0,000288	1,46E-05	0,947627	0,046222	0,953475	0,046525
13999	5,98E-07	1,00E-10	1,49E-11	4,64E-06	2,31E-07	2,33E-08	0,003629	0,000179	9,10E-06	0,949846	0,046332	0,95348	0,04652
14999	5,98E-07	2,40E-11	3,59E-12	1,79E-06	8,93E-08	8,99E-09	0,002256	0,000111	5,65E-06	0,951225	0,0464	0,953484	0,046516
15999	5,98E-07	5,75E-12	8,60E-13	6,90E-07	3,45E-08	3,47E-09	0,001402	6,92E-05	3,51E-06	0,952083	0,046442	0,953486	0,046514
17000	5,98E-07	1,38E-12	2,06E-13	2,66E-07	1,33E-08	1,34E-09	0,000871	4,30E-05	2,18E-06	0,952615	0,046469	0,953487	0,046513
18000	5,98E-07	3,31E-13	4,90E-14	1,03E-07	5,13E-09	5,16E-10	0,000541	2,67E-05	1,36E-06	0,952946	0,046485	0,953488	0,046512
19000	5,98E-07	7,90E-14	1,20E-14	3,97E-08	1,98E-09	1,99E-10	0,000336	1,66E-05	8,42E-07	0,953152	0,046495	0,953488	0,046512
20000	5,98E-07	1,90E-14	3,00E-15	1,53E-08	7,64E-10	7,69E-11	0,000209	1,03E-05	5,23E-07	0,953279	0,046501	0,953488	0,046512

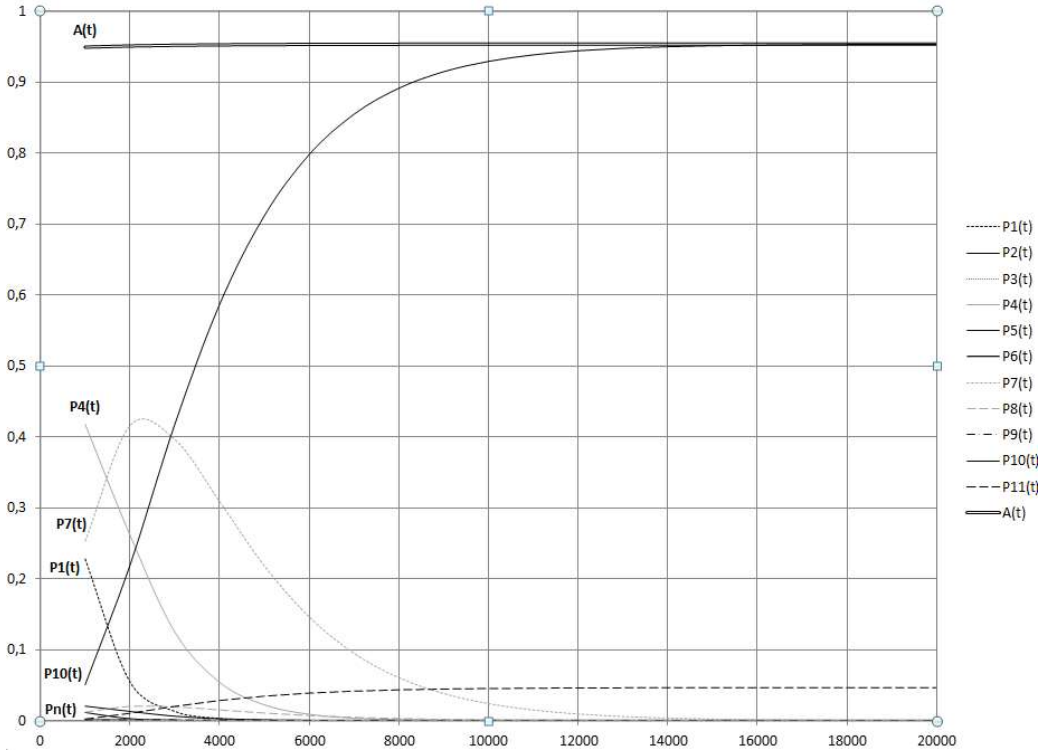


Рис. В.1 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ1

2. Результати оцінювання готовності ПТК S_{21} у відповідності до ББМ2

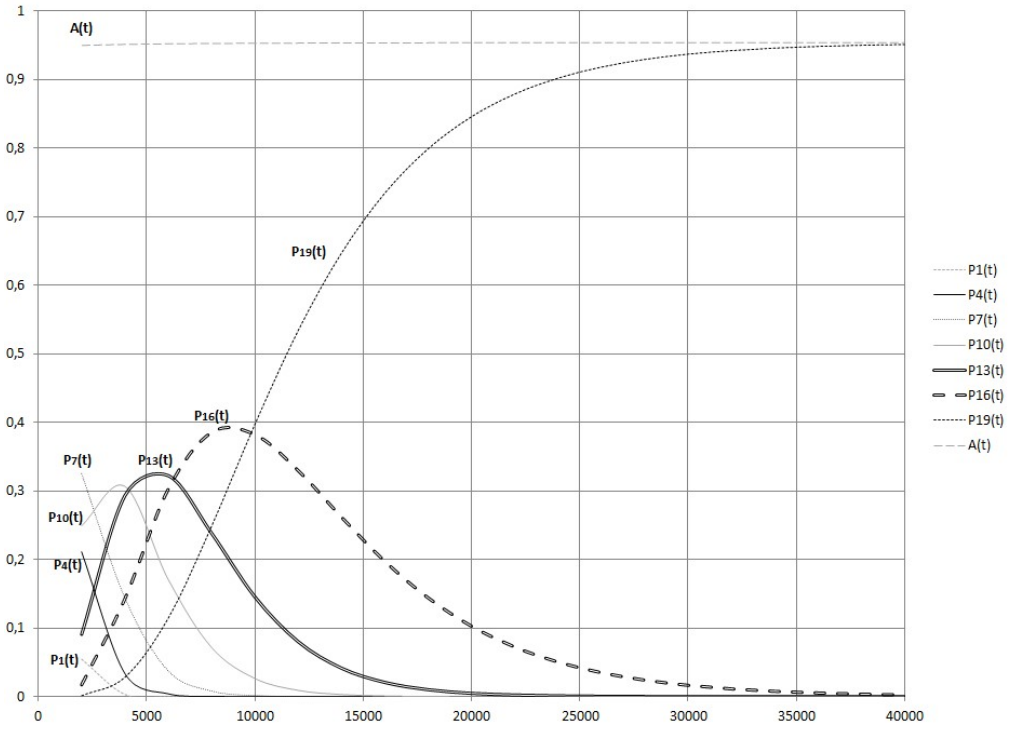


Рис. В.2 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ2

3. Результати оцінювання готовності ПТК S_{21} у відповідності до ББМ4

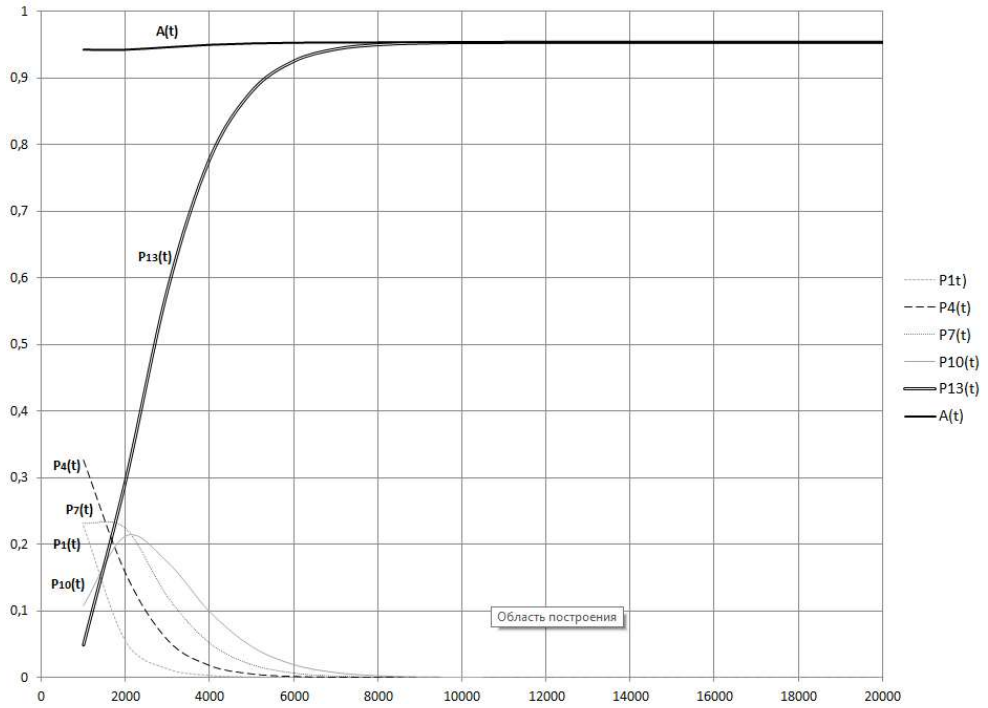


Рис. В.3 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для
ПТК S_{21} у відповідності до ББМ4

4. Результати оцінювання готовності ПТК S_{21} у відповідності до ББМ5

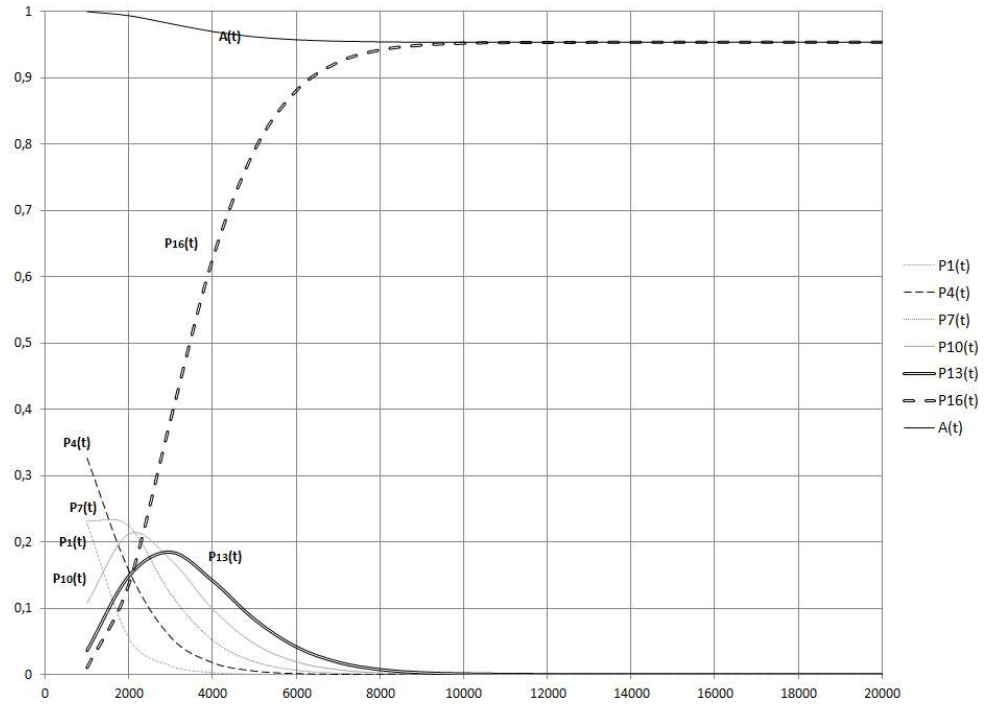


Рис. В.4 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ5

5. Результати оцінювання готовності (функційної безпечності) ПТК S_{21} у відповідності до ББМ6

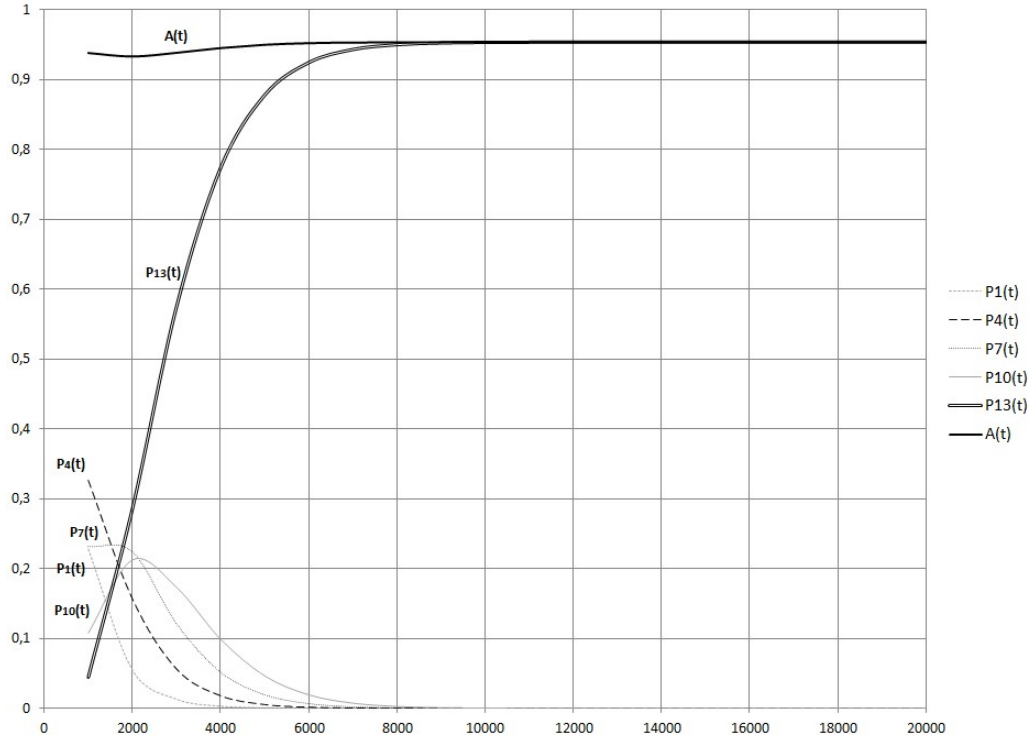


Рис. В.5 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ6

6. Результати оцінювання готовності (функційної безпечності) ПТК S_{21} у відповідності до ББМ8

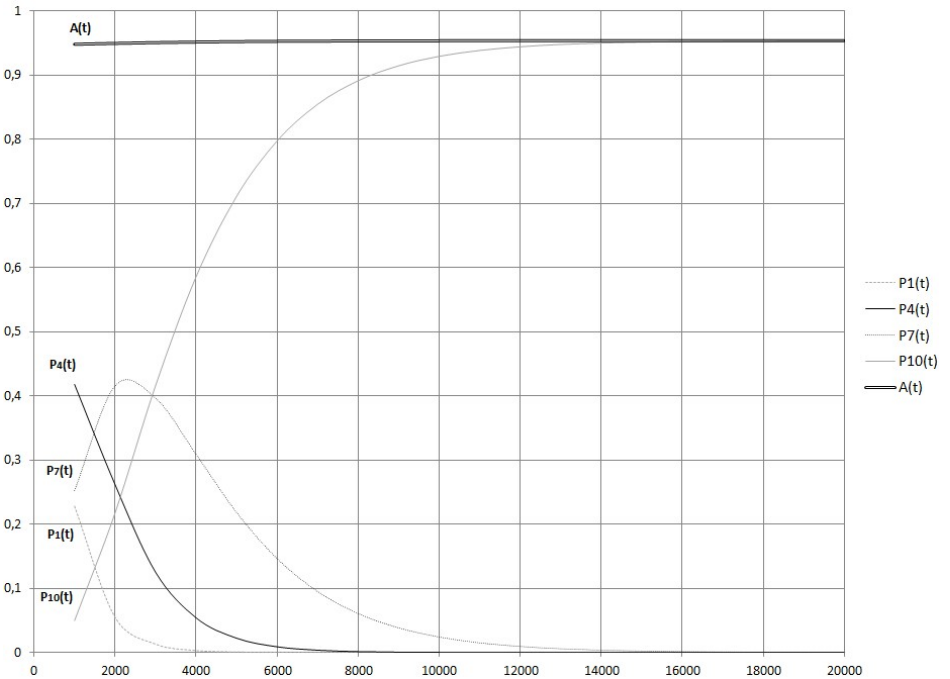


Рис. В.6 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ8

7. Результати оцінювання готовності (функційної безпечності) ПТК S_{21} у відповідності до ББМ9

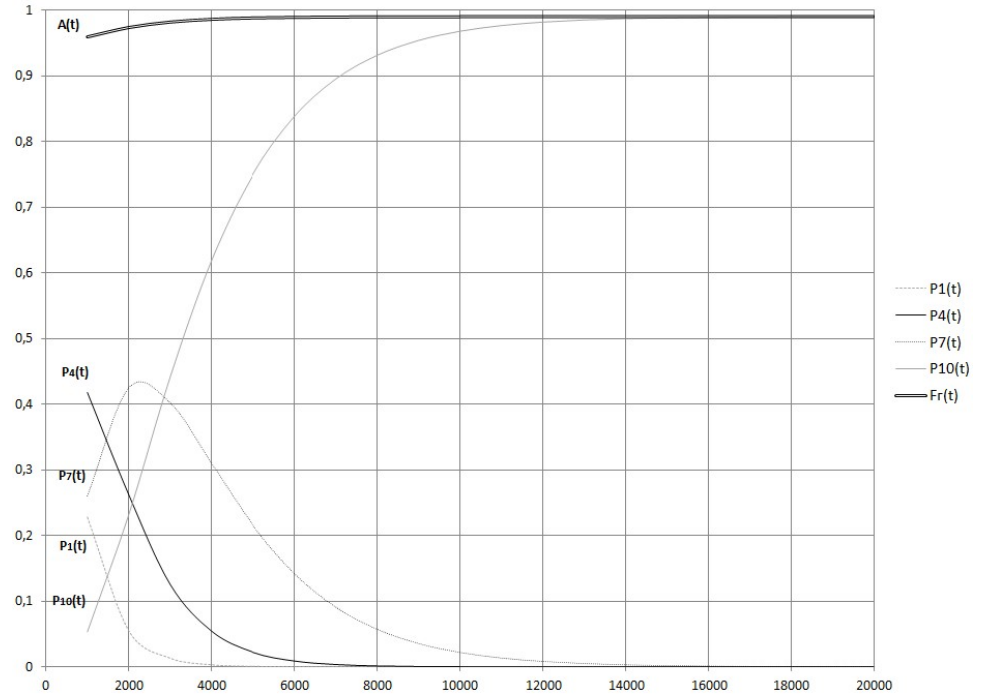


Рис. В.7 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ9

8. Результати оцінювання готовності (функційної безпечності) ПТК S_{21} у відповідності до ББМ12

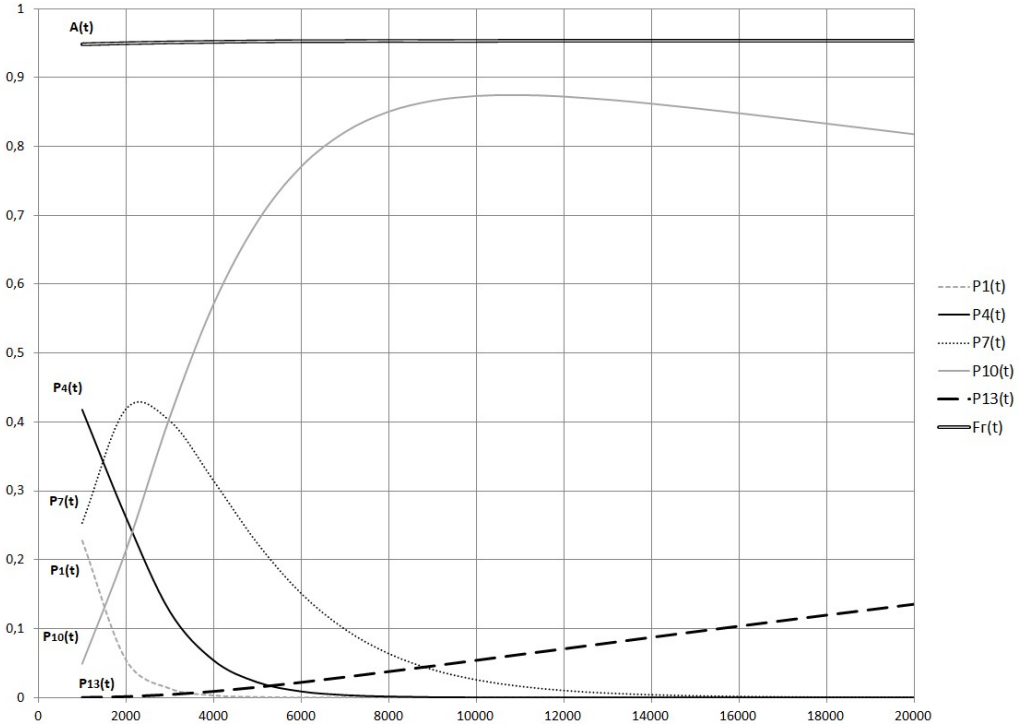


Рис. В.8 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{21} у відповідності до ББМ12

9. Результати оцінювання готовності (функційної безпечності) ПТК S_{22} у відповідності до ББМ1

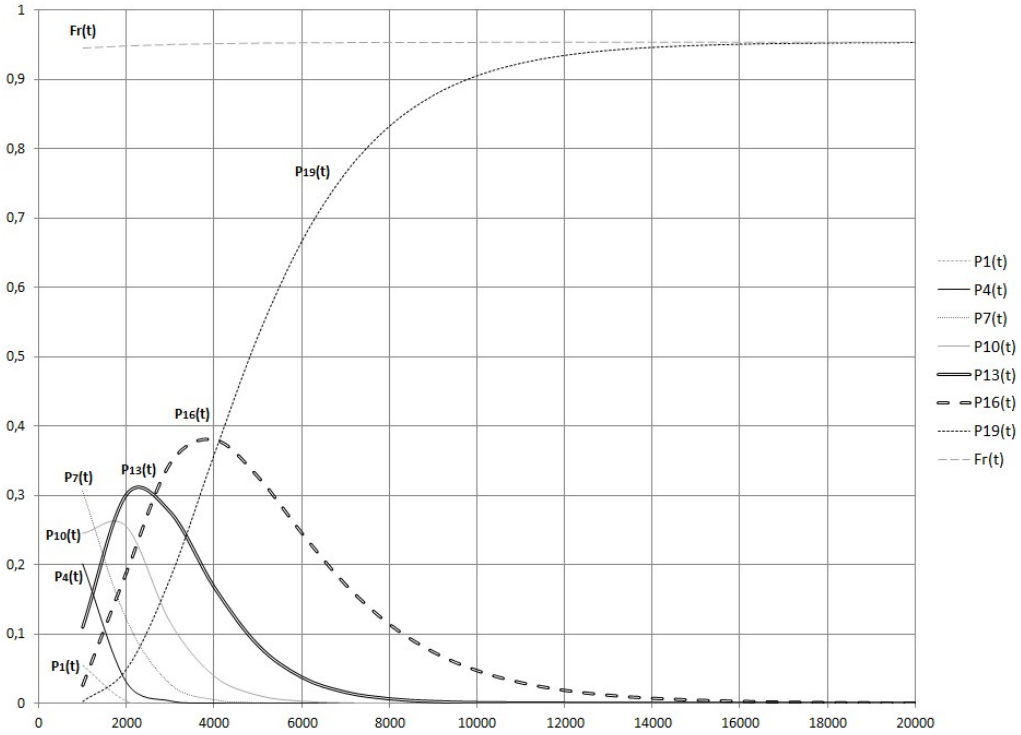


Рис. В.9 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{22} у відповідності до ББМ1

10. Результати оцінювання готовності (функційної безпечності) ПТК S_{22} у відповідності до ББМ2

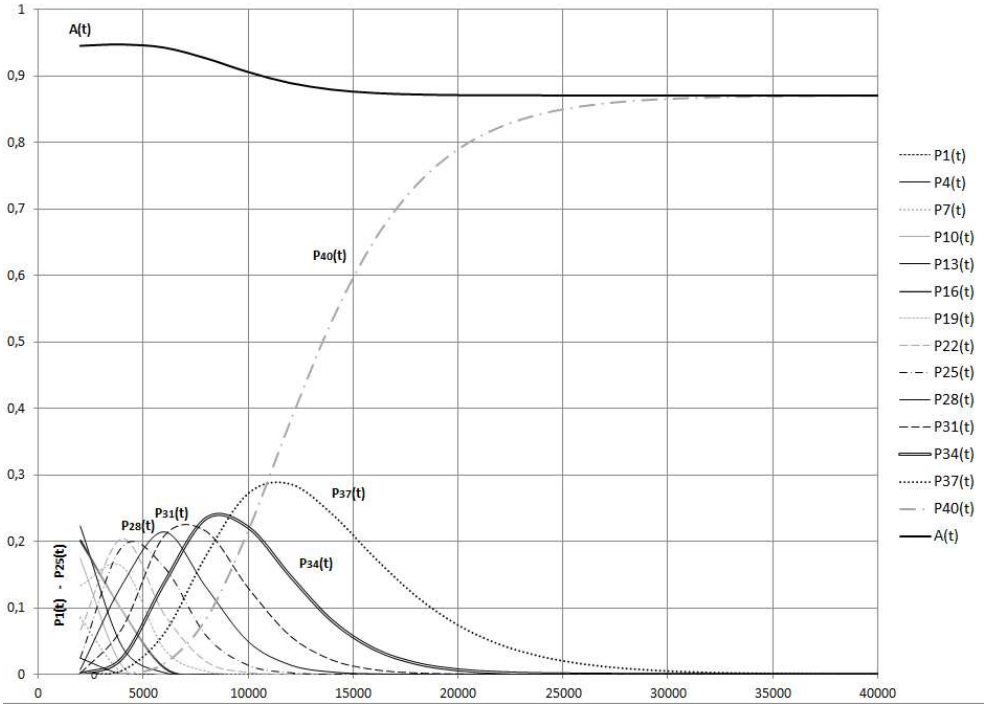


Рис. В.10 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{22} у відповідності до ББМ2

11. Результати оцінювання готовності (функційної безпечності) ПТК S_{22} у відповідності до ББМ7

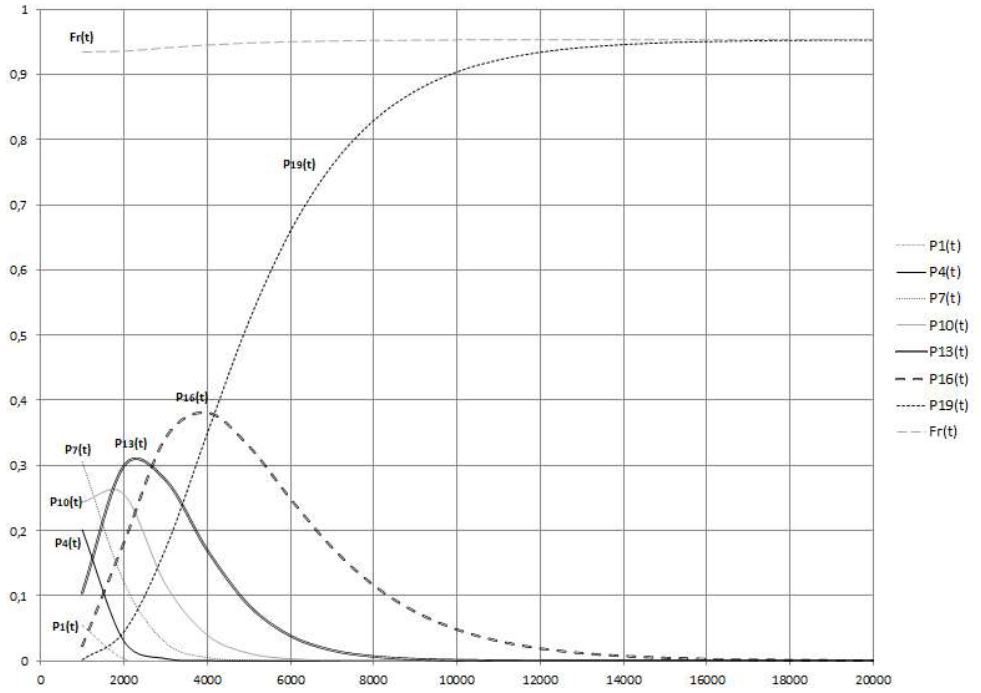


Рис. В.11 Графік залежності ймовірностей знаходження системи у працездатних станах та функції готовності від часу для ПТК S_{22} у відповідності до ББМ7

Додаток В. ЗАГАЛЬНА ПРОЦЕДУРА ВЕРИФІКАЦІЇ І ВАЛІДАЦІЇ

ПТК ІКС КЗ

Verification and Validation (General Procedure)

Revision 4

PREPARED BY _____ DATE: May 10, 2019

O.ODARUSHCHENKO

VERIFICATION
DEPARTMENT MANAGER

PURPOSE

The objectives of V&V are to assure that: the system architectural design is implemented correctly; the integrated system meets the system requirements; all requirement specifications, test plans, and specifications are traceable to the system architectural design; test results are traceable to test plans/specifications; requirements are forward and backward traceable through all the design documents;
the unavoidable constraints that influence requirements are addressed correctly;
the integration of human performance into systems and their operation is correct;
the system satisfies the test acceptance criteria specified in Software Verification and Validation Plan (SVVP); any found anomalies are recorded and addressed; all design anomalies are resolved; all uncovered anomalies are eliminated or reasonably justified.

SCOPE

This procedure applies to V&V activities performed at the A2. Planning, A3. Requirements specification, A7. Software Requirements Specification, A61. Hardware Requirements Specification validation, A8. Software Design, A62. Hardware Design, A9. Software Verification, A4. Validation, A102. FAT stages of RadICS I&C project lifecycle. V&V activities performed at hardware and software design stages are described in QP 03-4 and QP 03-5, so this procedure refers to them at relevant sections. Figure 1 shows RadICS projects V-model. Input and Output

V&V documents for the overall RadICS projects are given in Figure 2.

Source documents

Regulatory Guide 1.28, Revisions 3 & 4

10 CFR Part 50 Appendix B

10 CFR Part 21, Reporting of Defects and Noncompliance

NQA-1-1994, Parts I, Requirement 3 w/ Supplement 3S-1 and Requirement 11 w/ Supplements 11S-1 and 11S-2; Part II Subpart 2.7

NQA-1a-2009, Parts 1 and II, Requirements 3 and 11 w/Subparts 2.7 and 2.14

IEC 61508:2010 Functional safety of electrical/electronic programmable electronic safety related systems

IEC 61513:2009 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems

IEC 62566:2012 Nuclear power plants – Instruments and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions

IEEE Std 1012-2004, IEEE Standard for Software Verification and Validation

IEEE Std 7-4.3.2-2003,

IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations

IEEE Std 1028-2008, IEEE Standard for Software Reviews and Audits

IEEE Std 829-2008, IEEE Standard for Software and System Test Documentation

IEEE Std 1044-2009, IEEE Standard Classification for Software Anomalies

Regulatory Guide 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (IEEE Std 7-4.3.2-2003)

Regulatory Guide 1.153, Revision 1, Criteria for Safety Systems (IEEE Std 603-1991 and the correction sheet of January 30, 1995)

Regulatory Guide 1.168, Revision 1, Verification, validation, reviews, and audits for digital computer software used in safety systems of

nuclear power plants

Regulatory Guide 1.170, Revision 1, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

Regulatory Guide 1.171, Revision 1, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

IEEE 830-1998, IEEE Recommended Practice for Software Requirements Specifications

PROCEDURE

General procedural requirements for verification and validation activities

Each verification and validation task shall be started on a basis of verified input data/documents. Each anomaly and/or error that is uncovered during task execution shall be resolved (eliminated) or reasonably justified.

Verification of the product of a development stage shall be performed before the start of the next stage. Possible preparatory work for a subsequent stage may be done before the preceding stage has been verified.

If input data/documents for a task have been modified, that task and subsequent tasks shall be repeated (regression tested) as necessary to address potential impact. Project Manager shall initiate each repetition of verification tasks.

RadICS projects V-model is given in Figure 1.

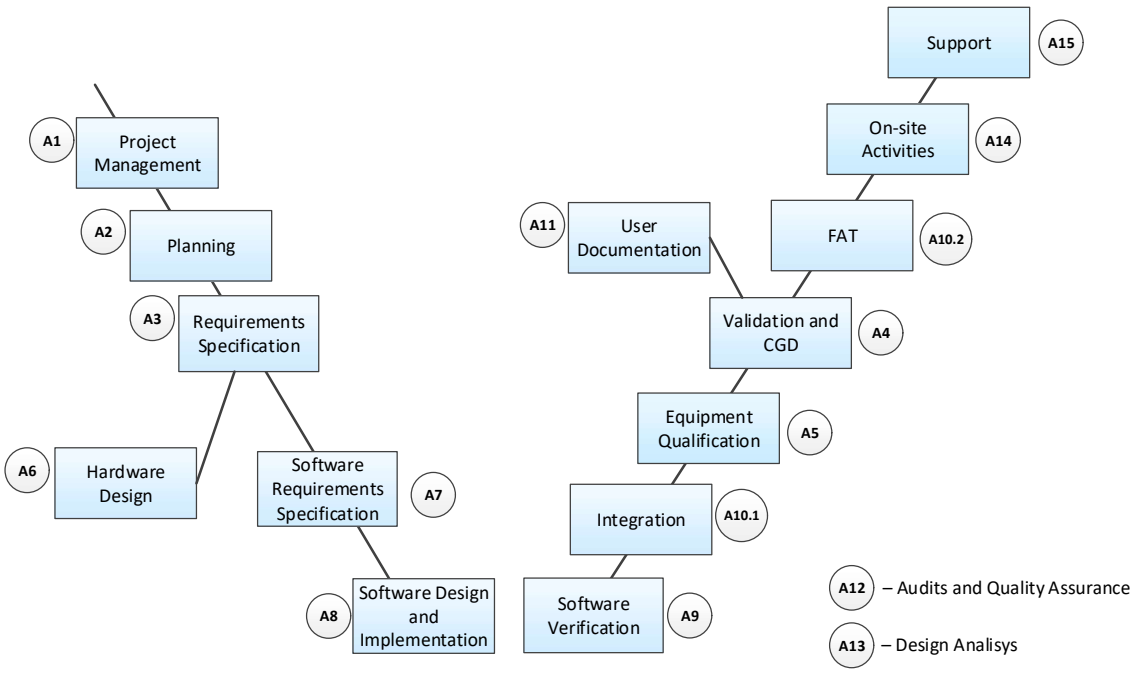


Figure 1.RadICS project V-model includes the following stages:

A1. Project Management;

A2. Planning;

A3. Requirements Specification;

A4. Validation and CGD (***SW&HW Fauly Insertion Testing***);

A5. Equipment Qualification;

A6. Hardware Design (divided into A61 Hardware Requirements Specification and A62 Hardware Design);

A7. Software Requirements Specification;

A8. Software Design and Implementation;

A9. Software Verification;

A101. Integration;

A102 FAT;

A11. User Documentation;

A12. Audits and Quality Assurance;

A13. Design Analysis;

A14. On-site Activities;

A15. Support.

Додаток Г. АКТИ ВПРОВАДЖЕННЯ

ЗАТВЕРДЖУЮ
Генеральний директор
ПАТ «НВП «Радій»»
кандидат технічних наук,
Лауреат Державної премії
України в галузі науки та
техніки
О.А. Сіора
«___» _____ 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Одарущенка Олега Миколайовича, виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови комісії – генерального конструктора ПАТ «НВП “Радій”» кандидата технічних наук Токарєва В.І. та членів комісії начальників відділів конструкторського бюро АСУ ТП кандидатів технічних наук Головира В.О., Бєлого Ю.О., констатує, що нові наукові результати дисертаційних досліджень, отримані Одарущенком О.М., а саме:

1) методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного призначення за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушення внаслідок проектних і фізичних дефектів та дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і забезпечення виконання вимог до відповідних показників;

2) моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання їх показників;

3) 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;

4) моделі оцінювання готовності та функційної безпечності ПТК на самодіагностованих платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функціональної безпеки та можливість висунення вимог до засобів контролю та діагностування;

5) 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 (FMECA/SFMECA) та ін'єктування фізичних і проектних (HWFIT/SWFIT), що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності;

6) метод забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною;

7) 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;

були використані для оцінювання рівня функційної безпечності цифрової інформаційно-керуючої платформи RadICS в процесі її SIL-3 сертифікації. Результати дисертаційних досліджень дозволили вдосконалити систему

менеджменту якості ПАТ «НВП “Радій”» в частині вдосконалення процесів розроблення, верифікації та валідації програмних та апаратних компонент програмно-технічних комплексів та інформаційно-керуючих систем критичного застосування.

Голова комісії Токарєв В.І.

Члени комісії Головир В.О.

Бєлий Ю.О.

ЗАТВЕРДЖУЮ

Директор

ТОВ «НВП «Радікс»

Андрашов А. О.

«16» 09 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Одарущенка Олега Миколайовича, виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови комісії – директора ТОВ «НВП «Радікс» Андрашова Антона Олександровича, членів комісії – старшого наукового співробітника к.т.н. доцента Стрюка Олексія Юрійовича, наукового співробітника Божко Віктора Івановича встановила, що для оцінки показників надійності та функційної безпечності перспективної цифрової інформаційно-управляючої платформи (ЦІУП) RadICS, в процесі її SIL-3 сертифікації використані наступні результати наукових досліджень Одарущенка Олега Миколайовича, а саме:

1) методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного призначення за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушення внаслідок проектних і фізичних дефектів та дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і забезпечення виконання вимог до відповідних показників;

2) моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання їх показників;

3) 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;

4) моделі оцінювання готовності та функційної безпечності ПТК на самодіагностованих платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функціональної безпеки та можливість висунення вимог до засобів контролю та діагностування;

5) 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 (FMECA/SFMECA) та ін'єктування фізичних і проектних (HWFIT/SWFIT), що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності;

6) метод забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною;

7) 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;

Побудова та використання запропонованих моделей та методів дозволило підвищити точність дослідження показників надійності та функційної безпечності ЦІУП RadICS в процесі її SIL-3 сертифікації, розробити рекомендації щодо

варіантів архітектури ПТК, які будуються на базі зазначеної ЦІУП із забезпеченням вимог до надійності та функційної безпечності системи, а також розробити процедури та інструкції з верифікації та валідації ПТК та їх програмних і апаратних компонентів, які стали частиною системи менеджмента якості підприємства.

Голова комісії А. О. Андрашов

Члени комісії О. Ю. Стрюк

В. І. Божко

ЗАТВЕРДЖУЮ

Головний конструктор
ДНВП «Об'єднання «Комунар»
Начальник НТ СКБ «Полісвіт»,
Лауреат Державної премії України у галузі науки і техніки,
заслужений винахідник України,
к.т.н., доцент
М.Ф.Сидоренко
„ 28 " серпня 2020 року

АКТ
реалізації результатів дисертаційної роботи
Одарущенка Олега Миколайовича,
виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови комісії – заступника начальника відділу Чумак О.І., членів комісії – начальника лабораторії Сальникова В.В., начальника лабораторії Кравченка О.М. склала даний акт в тому, що при розробленні бортових інформаційно-керуючих систем для літаків АН-70, АН-148 та інших було використано наступні нові наукові результати досліджень Одарущенка О.М.:

- принципи і моделі оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів (ПТК) з урахуванням їх інформаційно-технічного стану, змінності інтенсивностей відмов і відновлень;
- моделі оцінювання надійності програмних засобів шляхом урахування вторинних дефектів з урахуванням різних сценаріїв їх внесення впродовж тестування і супроводу;
- метод оцінювання і забезпечення надійності та функційної безпечності ПТК, побудованих на самодіагностовних платформах, який враховує різні варіанти використання структурно-версійної надмірності, дефекти програмних, програмовних і апаратних засобів;
- методи верифікації і валідації програмовних платформ шляхом об'єднання процедур аналізу видів, наслідків і критичності відмов та ін'єктування фізичних і проектних дефектів.

Впровадження результатів досліджень Одарущенка О.М. надало змогу підвищити точність оцінювання та значення показників надійності і функційної безпечності з урахуванням різних типів дефектів і відмов програмно-апаратних засобів, ПЛІС і засобів контролю і самодіагностування.

Голова комісії: _____ О.І. Чумак

Члени комісії: _____ В.В. Сальников

_____ О.М. Кравченко

ЗАТВЕРДЖУЮ

Директор Харківської філії
Державного підприємства
«Державний науково-технічний центр з
ядерної та радіаційної безпеки»
С.О. Трубчанінов
«____» вересня 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Одарущенка Олега Миколайовича, виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі Голови комісії – заслуженого діяча науки та техніки України д.т.н., професора Ястребенецького М.О. та Членів комісії – к.т.н. Гольдріна В.М. та к.т.н. Клевцова О.Л., встановила, що результати на наукових досліджень Одарущенка О.М., а саме:

- моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання їх показників;

- 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;

- моделі оцінювання готовності та функційної безпечності програмно-технічних комплексів на самодіагностованих платформах, які враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функційної безпечності та можливість висунення вимог до засобів контролю та діагностування;

- методи верифікації і валідації програмовних платформ і програмно-технічних комплексів на їх основі, які базуються на комплексуванні процедур аналізу видів, наслідків і критичності відмов та ін'єктування фізичних і проектних дефектів;

- метод оцінювання та забезпечення функційної безпечності при розробленні та ліцензуванні модулів і платформ для інформаційних та керуючих систем на програмовних логічних інтегральних схемах, який ураховує фізичні та проектні дефекти, а також змінність параметрів відмов і відновлень, і підвищує повноту виконання вимог міжнародних стандартів до рівня функційної безпечності SIL3,

використані в процесі розроблення проєктів нормативних документів і методик оцінювання відповідності інформаційних та керуючих систем АЕС вимогам національних і міжнародних стандартів. Це надало змогу покращити повноту оцінювання і якість відповідних документів.

Голова комісії Ястребенецький М.О.

Члени комісії Гольдрін В.М.

Клевцов О.Л.

ЗАТВЕРДЖУЮ
Директор ПП ЛітСофт
В. Песчаненко

23 вересня 2020 р.

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Одарущенка Олега Миколайовича, виконаної на здобуття наукового ступеня доктора технічних наук

Комісія у складі голови комісії – директора ПП ЛітСофт В. Песчаненко, членів комісії О. Летичевського, М. Полторацького встановила, що в ході розроблення технології модельної розробки апаратного забезпечення (програмованих плат, чіпів, систем електроніки) з використанням комбінації методів машинного навчання та алгебраїчного підходу у їх верифікації та тестуванні використані наступні результати наукових досліджень Одарущенка Олега Миколайовича, а саме:

1) моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання їх показників;

2) моделі оцінювання готовності та функційної безпечності ПТК на самодіагностованих платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функціональної безпеки та можливість висунення вимог до засобів контролю та діагностування;

3) 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 (FMECA/SFMECA) та ін'єктування фізичних і проектних (HWFIT/SWFIT), що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності.

Побудова та використання запропонованих моделей та методів дозволило вдосконалити технологію модельної розробки, основною перевагою якої є можливість перекласти розробку тестових наборів з тестувальника на розроблений інструмент, що дозволить звільнитись від суб'єктивності розробки тестових наборі що, підвищить ефективність тестування (число виявлених дефектів) і відповідно підвищить рівень надійності і функційної безпечності системи, що розробляється.

Голова комісії В. Песчаненко

Члени комісії:

О. Летичевський

М. Полторацький

23 вересня 2020 р.

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного аерокосмічного університету
ім. М.Є. Жуковського
«Харківський авіаційний інститут»
д.т.н., старший науковий співробітник
_____ В.В. Павліков
« » _____ 2020 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи
Одарущенка Олега Миколайовича, виконаної на здобуття наукового ступеня доктора технічних наук, при виконанні міжнародних проектів, які виконувалися у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківській авіаційний інститут»

Комісія у складі Голови комісії – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій Одокієнка Олексія Володимировича та Членів комісії – директора Центру розвитку інновацій міжнародного науково-технічного та освітнього співробітництва Данька Костянтина Анатолійовича, к.т.н., доцента Боярчука Артема Володимировича, к.т.н., доцента Ілляшенка Олега Олександровича встановила, що наукові результати, а саме:

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

– 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;

– метод забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною;

– 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;

Реалізовані у навчальному процесі у вигляді:

– лекцій та практичних занять з методів проектування, оцінювання та забезпечення надійності та функційної безпечності апаратних та програмних засобів інформаційно-керуючих систем у навчальних дисциплінах: «Технології забезпечення якості програмно-технічних комплексів»; «Технології проектування програмних систем»; «Теорія ризиків та технології управління безпекою ІКС»; «Технології розроблення та забезпечення функціональної безпеки ІУС»;

– матеріалів навчальних проектів за програмою Європейського Союзу: JEP 26008-2005: Розробка і впровадження навчальних курсів по підготовці магістрів і докторів філософії (кандидатів наук) за напрямком аерокосмічного критичного комп'ютінга «MASTAC» (Msc and PhD Studies in Aerospace Critical Computing «MASTAC»), 2006-2009 pp., зокрема навчально-методичного забезпечення курсу «Моделирование гарантоспособных систем и сетей»;

– 158886-TEMPUS-1-2009-1-UK-TEMPUS-JPCR: Національна мережа центрів інноваційної університетсько-індустріальної кооперації з інженерії безпеки «SAFEGUARD» (National Safeware Engineering Network of Centres of Innovative Academia-Industry Handshaking «SAFEGUARD»), 2010-2013 pp.,

зокрема навчально-методичного забезпечення курсу «Системы и технологии высокой готовности»;

– 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR: Модернізація післядипломної освіти у галузі безпеки та стійких інформаційних систем для індустрії «SEREIN» (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains «SEREIN»), 2013-2016 рр., зокрема навчально-методичного забезпечення курсу «Энергоэффективность алгоритмов и программ».

Це дозволило підвищити фундаментальність, наочність та практичну спрямованість навчального процесу, покращити міжнародні зв'язки університету у галузі підготовки фахівців і наукового співробітництва.

Голова комісії: О.В. Одокієнко

Члени комісії: К.А. Данько

А.В. Боярчук

О.О. Ілляшенко

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного аерокосмічного університету
ім. М.Є. Жуковського
«Харківський авіаційний інститут»
д.т.н., старший науковий співробітник
_____ В.В. Павліков
« » _____ 2020 року

АКТ ВПРОВАДЖЕННЯ
наукових результатів дисертаційної роботи
Одарущенка Олега Миколайовича, виконаної на здобуття наукового ступеня доктора технічних наук, у навчальному процесі та науково-дослідних роботах, які виконувалися кафедрою комп'ютерних систем, мереж і кібербезпеки

Комісія у складі Голови комісії – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій к.т.н. Одокієнка Олексія Володимировича та Членів комісії – д.т.н., с.н.с. Брежнєва Євгена Віталійовича, к.т.н., професора Фурманова Клайда Костянтиновича, к.т.н., доцента Колісник Марини Олександрівни, встановила, що наукові результати, а саме:

– методологія оцінювання і забезпечення надійності та функційної безпечності програмно-технічних комплексів для інформаційно-керуючих систем критичного призначення за рахунок опису їх інформаційно-технічного стану, удосконалення принципів зменшення та оцінювання ризиків його порушення внаслідок проектних і фізичних дефектів та дефектів взаємодії з урахуванням змінності параметрів потоків відмов і відновлень, що забезпечує підвищення точності оцінювання і забезпечення виконання вимог до відповідних показників;

– моделі оцінювання надійності (безвідмовності) програмних засобів шляхом урахування вторинних дефектів, які вносяться за результатами тестування і супроводу, та різних сценаріїв їх внесення, що забезпечує підвищення точності оцінювання їх показників;

– 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 ПТК на самодіагностованих платформах, які на відміну від відомих враховують помилки контролю та змінність параметрів системи, що забезпечує підвищення точності оцінки готовності і функціональної безпеки та можливість висунення вимог до засобів контролю та діагностування;

– 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 (FMECA/SFMECA) та ін'єктування фізичних і проектних (HWFIT/SWFIT), що забезпечує перевірку виконання вимог стандартів і підвищення функційної безпечності;

– метод забезпечення функційної безпечності програмно-технічних комплексів на програмовних платформах шляхом використання різних варіантів версійної надмірності (диверсності), що зменшує ризики відмов за загальною причиною;

– 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;

Реалізовані у вигляді теоретичних положень при виконанні науково-дослідницьких робот:

1) Розробка науково-методичних основ й інформаційних технологій оцінки і забезпечення відмовостійкості та безпеки комп'ютеризованих систем

аерокосмічних комплексів, інших комплексів критичного застосування (Національний аерокосмічний університет ім. М.Є Жуковського «ХАІ», №Г503-42/2003, №104U003502, 2003-2004);

2) Теоретичні основи, методи та інструментальні засоби аналізу, розробки та верифікації гарантоздатних інформаційно-управляючих систем для аерокосмічних об'єктів і комплексів критичного застосування (Національний аерокосмічний університет ім. М.Є Жуковського «ХАІ», ДР № №0106U001071, 2006-2008);

3) Теоретичні основи, методи та технології забезпечення гарантоздатності еволюціонуючих комп'ютеризованих інфраструктур для аерокосмічних і критичних об'єктів (Національний аерокосмічний університет ім. М.Є Жуковського «ХАІ», ДР№0108U010994, 2009-2011рр.);

4) Теоретичні основи, методи та інформаційні технології розробки програмно-технічних комплексів критичного застосування в умовах ресурсних обмежень (Національний аерокосмічний університет ім. М.Є Жуковського «ХАІ», ДР№ 0112U001058, 2014);

5) Наукові основи, методи і засоби зеленого комп'ютингу і комунікацій (Національний аерокосмічний університет ім. М.Є Жуковського «ХАІ», ДР№0115U000996, 2015-2017 рр.).

Це дозволило підвищити якість виконання держбюджетних НДР.

Голова комісії: О.В. Одокієнко

Члени комісії: Є.В. Брежнєв

К.К. Фурманов

М.О. Колісник

Додаток Д СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні результати дисертації

69.Харченко В.С., Одарущенко О.Н., Поночовный Ю.Л., Одарущенко Е.Б., Скляр В.В. Технологии высокой готовности для программно-технических комплексов космических систем : монография. Харьков, 2010. 372 с. *(Особистий внесок здобувача: моделювання і оцінка готовності ПТК з урахуванням зміни параметрів процессів відмов та відновлень).*

70.Боярчук А.В., Брежнев Е.В., Горбенко А.В., Дубницкий В.Ю., Епифанов А.С., Зайцева Е.В., Засуха С.А., Иванченко О.В., Кочкарь Д.А., Левашенко В.Н., Одарущенко О.Н., Орехов А.А., Резчиков А.Ф., Сиора А.А., Скатков А.В., Скляр В.В., Тарасюк О.М. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения : монография. Харьков, 2011. 641с. *(Особистий внесок здобувача: методи визначення параметрів потоків відмов та відновлення ПЗ та величин їх зміни, послідовність розробки і аналіз моделей готовності ІТ-інфраструктур з змінними параметрами).*

71.Одарущенко О.Н., Харченко В.С., Маевский Д.А., Поночовный Ю.Л., Руденко А.А, Одарущенко Е.Б., Засуха С.А., Жадан В.О., Живило С.В. CASE-оценка критических программных систем. Надежность: монография. Т.2. Харьков, 2012. 292с. *(Особистий внесок здобувача: методи контроля випадкових відмов обладнання, методи виключення систематичних відмов обладнання).*

72.Odarushchenko O., Sklyar V., Bulba E., Horbenko R., Ivasyuk A., Kotov D. Assessment of Energy Consumption for Safety-Related PLC-based Systems. *Green IT Engineering: Concepts, Models, Complex Systems Architectures, Studies in Systems, Decision and Control series*. Springer. Springer International Publishing Switzerland, 2017. P. 269 – 281. *(Особистий внесок здобувача: методика оцінювання енергоспоживання ПЛК).* (Видання входить до міжнародної наукометричної бази Scopus).

73.Odarushchenko, O. Odarushchenko, E, .Butenko, V., Ruchkov, E. Tool-Based Assessment of Reactor Trip Systems Availability and Safety Using Markov Modeling. *Cyber Security and Safety of Nucler Power Plant Instrumentation and Control Systems*. Hershey, Pennsylvania, United States of America, IGI Global, 2020. P. 175-203. *(Особистий внесок здобувача: аналіз недоліків IEC 61508, багатофрагментні марковські моделі та розв'язання систем диференційних рівнянь).*

74.Одарущенко О.Н., Одарущенко Е.Б., Стороженко А.В., Гроза П.Н. Оценка надежности программно-технических комплексов на основе многофрагментных марковских моделей. *Системи обробки інформації*. 2001. Вип. 3(13). С. 110-116. *(Особистий внесок здобувача: багатофрагментна марковська модель).*

75.Одарущенко О.Н., Одарущенко Е.Б., Поночовный Ю.Л. Применение численных методов для решения жестких систем линейных дифференциальных уравнений в задачах оценки надежности обслуживаемых систем. *Авіаційно-космічна техніка і технологія*. 2002. Вип. 35. С. 187-191. *(Особистий внесок здобувача: алгоритм модифікованого експоненційного методу розв'язання систем лінійних алгебраїчних рівнянь).*

76.Одарущенко О.Н., Поночовный Ю.Л. Одарущенко Е.Б. Терминологические аспекты теории надежности программных средств. *Радіоелектронні і комп'ютерні системи*. 2004. Вип. 2(6), С. 88-94. *(Особистий внесок здобувача: визначення термінів дефект ПЗ, відмова ПЗ).*

77.Харченко В.С., Одарущенко О.Н., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов. *Радіоелектронні і комп'ютерні системи*. 2006. Вип. 5(17). С.62-70. *(Особистий внесок здобувача: визначення термінів дефект ПЗ, відмова ПЗ).*

78. Руденко А.А., Одарущенко О.Н., Харченко В.С. Модели оценки надежности программных средств с учетом недетерминированного числа вторичных дефектов. *Радіоелектронні і комп'ютерні системи.* 2010.

Вип.6(47). С.197-203. *(Особистий внесок здобувача: МНПЗ з урахуванням недетермінованого числа вторинних дефектів).*

79. Харченко В.С., Одарущенко О.Н., Модель информационно-технического состояния компьютерной системы. *Системи обробки інформації.* 2008. Вип. 7(74). С.128-130. *(Особистий внесок здобувача: модель інформаційно-технічного стану з урахуванням рівней працездатності, показники гарантоздатності).*

80. Харченко В.С., Одарущенко О.Н., Руденко А.А., Одарущенко Е.Б., Поночовный Ю.Л. Моделирование обслуживаемых компьютерных систем с учетом вторичных дефектов программных средств. *Радіоелектронні і комп'ютерні системи*. 2009. № 7. С.245-249. *(Особистий внесок здобувача*: *марковські моделі з урахуванням прояву вторинних дефектів ПЗ).*

81. Одарущенко О.Н., Харченко В.С. Информационно-технические состояния компьютеризированных систем: модель событий и показатели гарантоспособности. *Системи управління, навігації та зв'язк*. 2009. Вип. 3(11). С.156-159. *(Особистий внесок здобувача: модель подій, показники гарантоздатності).*

82. Летичевский О.О., Песчаненко В.С., Харченко В.С., Волков В.А.. Одарущенко О.М. Модельний спосіб розроблення алгоритмів цифрових систем на програмованих логічних інтегральних схемах. *Кібернетика і системний аналіз*. 2020. Т. 56. №5. С.29-37. *(Особистий внесок здобувач: елементи технології модельної розробки апаратного забезпечення з використанням комбінації методів машинного навчання та алгебраїчного підходу).* (Видання входить до міжнародної наукометричної бази Scopus).

83. Одарущенко О.Н.. Руденко А.А., Харченко В.С. Учет вторичных дефектов в моделях надежности программных средств. *Математичні машини і системи.* 2010. Вип.1. С.205-217. *(Особистий внесок здобувача*: *визначення параметрів функцій ризику моделей надійності програмних засобів для урахування вторинних дефектів).*

84. Харченко В.С., Одарущенко О.Н., Руденко А.А., Одарущенко Е.Б.

Анализ сценариев и определение параметров для оценки надежности программных средств с учетом вторичных дефектов. *Системи управління, навігації та зв'язку.* 2011. Вип.3(11). С.273-280. *(Особистий внесок здобувача*: *список параметрів, які застосовуються в моделях надійності програмних засобів для урахування вторинних дефектів).*

85. Odarushchenko O., Kharchenko V., Popov P., Zhadan V. Empirical evaluation accuracy of mathematical software used for availability assessment of fault-tolerant computer systems. *Electronic Jornal Reliability & risk Analysis: Theory & Applications*. 2012. 3(26), Vol.7. P.85-97. *(Особистий внесок здобувача*: *етапи розроблення багатофрагментних марковських моделей).*

86. Одарущенко О.Н., Руденко А.А., Харченко В.С. Метод оценивания надежности программных средств с учетом вторичных дефетков. *Радіоелектронні і комп'ютерні системи*. 2012. Вип.7(59). С.313-318. *(Особистий внесок здобувача*: *метод оцінювання надійності ПЗ з урахуванням прояву вторинних дефектів).*

87. Ивасюк А.О., Одарущенко О.Н., Фадеева Е.К., Барвинко А.П. Модель и инструментальная поддержка анализа сигналов при оценке функциональной безопасности FPGA-модулей. *Системи обробки інформації.* 2013. Вип. 4(111). С.20-23. *(Особистий внесок здобувача*: *інструментальні засоби функціонального покриття для електронних проектів ПЛІС в ході виконання їх функціонального тестування).*

88. Скляр В.В.. Резуненко А.А., Одарущенко О.Н., Гудзь А.С., Щербаченко С.С., Сенаторо А.А, Вовк Е.Д. Обеспечение тестового покрытия для электронных проектов FPGA при оценивании функциональной безопасности по критериям SIL3. *Системи обробки інформації.* 2013. Вип. 5(112). С. 62-65. *(Особистий внесок здобувача*: *модель функціонального покриття для електронних проєктів ПЛІС).*

89. Odarushchenko O., Kharchenko V., Butenko V. Metric-based analysis of Markov models for computer systems availability assessment. *Радіоелектронні і комп'ютерні системи*. 2013. Вип. 5(64). С.214-220. *(Особистий внесок*

здобувача: *марковські моделі оцінювання готовності комп'ютерних систем).*

90. Одарущенко О.Н., Харченко В.С., Руденко А.А., Одарущенко Е.Б. Учет фактора вторичных дефектов при оценке надежности программных средств. *Научные ведомости Белгородского государственного университета. "История. Политология. Экономика. Информатика".* 2013. №22(165). Вып. 28/1. С.153-160. *(Особистий внесок здобувача: сценарії внесення та усунення дефектів програмних засобів, аналіз моделей надійності програмних засобів з метою визначення переліку моделей для модифікації їх функцій ризику).*

91. Харченко В.С., Бутенко В.О., Одарущенко О.Н. Метрико-интервальные модели и инструментальные средства для оценивания готовности информационно-управляющих систем с использованием марковских процессов. *Системи обробки інформації.* 2014. Вип. 9(125). С.59-64. *(Особистий внесок здобувача: алгоритм обрання інструментальних засобів).*

92. Kharchenko V, Butenko V, Odarushchenko O., Sklyar V. Multi-fragmentation Markov Modeling of a Reactor Trip System. *Journal of Nuclear Engineering and Radiation Science*. 2015. Vol. 1, Iss. 3. 031005 (10 pages). URL: https: // asmedigitalcollection.asme.org/ nuclearengineering/ articleabstract/1/3/031005/472772/ Multifragmentation-Markov-Modeling-of-a-Reactor?redirectedFrom=fulltext (дата звернення: 18.01.2021). *(Особистий внесок здобувача: однофрагментні та багатофрагментні моделі оцінювання надійності комп'ютерних систем).* (Видання входить до міжнародної наукометричної бази Scopus).

93. Скляр В.В., Одарущенко О.Н., Поночовный Ю.Л., Бульба Е.Н., Ивасюк А.О. Модели отказов информационно-управляющих систем на основе самодиагностируемых программируемых платформ в системах аварийной защиты реакторов. *Радіоелектронні і комп'ютерні системи науково-технічний журнал.* 2015. №4. С.19-24. (*Особистий внесок здобувача: базова марковська модель відмов ІКС, структурна модель системи контроля та діагностики на основі самодіагностовних програмовних платформ).*

94. Kharchenko V., Odarushchenko O., Butenko V., Moskalets V., Odarushchenko E., Strjuk O. Application of Markov Modeling for Safety Modeling for Safety Assessment of Self-Diagnostic Programmable Instrumentations and Control Systems. *Central European Researchers Journal*. 2016. Vol.2, Iss. 2. P. 61-69. URL: http://ceres-journal.eu/iss160202 (дата звернення: 18.01.2021). *(Особистий внесок здобувача: однофрагмента та багатофрагментна марковські моделі оцінювання надійності двохканальної комп'ютеризованої системи).*

95. Одарущенко О.Б., Одарущенко О.М., Бутенко В.О., Москалець В.В., Стрюк О.Ю. Моделі математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів. *Системи управління, навігації та зв'язку.* 2017. Вип. 4(44). С.40-45. *(Особистий внесок здобувача: постановка завдання розроблення моделей математичних блоків дискретного перетворення інформації для верифікації програмного забезпечення програмованих логічних контролерів).*

96. Одарущенко О.М., Одарущенко О.Б., Харченко В.С. Марковьскі моделі оцінювання функціональної безпеки програмно-технічних комплексів на самодіагностовних програмовних платформах з урахуванням помилок засобів контролю. *Радіоелектронні і комп'ютерні системи.* 2019. №4(92). С.17-29. *(Особистий внесок здобувача: структурні схеми систем нормальної експлуатаціїта аварійного захисту, дерева відмов, багатофрагментні моделі з урахуванням помилок засобів контролю).*

97. Руденко О.А., Одарущенко О.М., Руденко З.М., Одарущенко О.Б. Оцінювання кількості вторинних дефектів програмних засобів шляхом комплексування модифікованих моделей росту надійності Джелінські-Моранди і Шика-Волвертона. *Системи управління, навігації та зв'язку.* 2020. Вип.1(59). С.97-100. *(Особистий внесок здобувача: модифікована МНПЗ Джелінські-Моранди).*

98. Одарущенко О.Н. Оцінювання та забезпечення функційної безпеки при розробленні та ліцензуванні модулів і платформ для програмно-технічних

комплексів інформаційно-керуючих систем. *Системи управління, навігації та зв'язку.* 2020.Вип.3(61). С.90-93.

Праці апробаційного характеру:

99.Odarushchenko, O., Kharchenko, V. Availability models of critical infrastructures with variable system dependability parameters. *Proceedings of the first International Workshop Critical Infrastructure Safety and Security. CrISS-DESSERT,* May 11-13, 2011, Kirovograd, Ukraine, 2011. P. 319-330. (*Особистий внесок здобувача: математичні моделі готовності критичних інфраструктур з змінними параметрами).*

100. Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Selecting mathematical software for dependability assessment of computer systems described by stiff Markov chains. *ICT in Education, Research and Industrial Applications: Integration, Harmonization and Knowledge Transfer. ICTERI 2013: Procceding of the 9th International Conference,* June 19-22, 2013, Kherson, Ukraine, 2013. P. 146 – 162. (*Особистий внесок здобувача: структурна схема надійності, багатофрагмента марковська модель).* (Видання входить до міжнародної наукометричної бази Scopus).

101.Odarushchenko O., Ivasyuk O., Bulba E. Fault injection-based technique and tool for FPGA modules safety assessment. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013,* May 23-26, 2013, Sevastopol, Ukraine, 2013. P.14. (*Особистий внесок здобувача: процедура тестування з внесенням дефектів).*

102. Butenko V., Odarushchenko O., Kharchenko V. Analysis of markov chains for high availability systems: metric-based approach. *Programm of the 3rd International Workshop Critical Infrastructure Safety and Security CrISS 2013,* May 23-26, 2013, Sevastopol, Ukraine, 2013. P.16. (*Особистий внесок здобувача: етапи оцінювання готовності ПТК).*

103. Odarushchenko O., Kharchenko V., Sklyar V, Ivasuyk A. Fault-Injection Testing: FIT-Ability. *Proceedings of East-West Design&Test Symposium EWDTS"2013*, September 27-30, 2013, Ростов-на-Дону, Росссия, 2013. P.188-192.

(*Особистий внесок здобувача: – оптимальна FIT – процедура, алгоритм та приклад виконання процедури).*

104. Odarushchenko, O., Kharchenko, V, Butenko, D, Butenko V. Assessment of the Reactor Trip System Dependability Two Markov Chains - based Cases. *Proceedings of the 10th International Conference on Digital Technologiesю,* July 9-11, 2014, Zilina, Slovakia, 2014. P. 103-109. (*Особистий внесок здобувача: багатофрагментна марковська модель, індустріальний приклад).* (Видання входить до міжнародної наукометричної бази Scopus).

105. Butenko V., Kharchenko V., Odarushchenko O., Popov P., Sklyar V., Odarushchenko E. Markov's Model and Tool-Based Assessment of Safety-Critical I&C Systems: Gaps of the IEC 61508. *12-th International Conference on Probabilistic Safety Assessment and Modeling*: *Proceeding of 12-th International conference on probabilistic safety assessment and modeling,* June 22-27, 2014, Honolulu, Hawaii, USA, 2014. P. 455-458. URL: http: // iapsam.org/ psam12/ proceedings/paper/ paper_455_1.pdf (дата звернення 18.01.2021). (*Особистий внесок здобувача: результати аналізу недоліків стандарту IEC 61508, структурна схема надійності та марковська модель системи аварійного захисту).* (Видання входить до міжнародної наукометричної бази Scopus).

106. Odarushchenko O., Kharchenko V, Sklyar V, Ivasyuk A. Fault insertion testing of FPGA-based NPP I&C systems: SIL certification issues*. Proceedings of 22nd International Conference on Nuclear Engineering. Technical Publication ICONE22*, July 7-11, 2014, Prague, Czech Republic, 2014. Vol. 6: Nuclear Education, Public Acceptance and Related Issues; Instrumentation and Controls (I&C); Fusion Engineering; Beyond Design Basis Events. URL: https: // asmedigitalcollection.asme.org /ICONE/ICONE22/volume/45967. ICONE22-31163, V006T13A022; 5 pages. (Дата звереннння: 18.01.2021). (*Особистий внесок здобувача: етапи виконання HW FIT процедури).* (Видання входить до міжнародної наукометричної бази Scopus).

107. Odarushchenko O., Kharchenko V, Gordieiev O., Vilkomir S. t-Wise-Based Multi-Fault Injection Technique for the Verification of Safety Critical I&C

Systems. *Procceding of 9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT,* February 22-26, 2015, Charlotte, USA, 2015. P. 1827-1836. (*Особистий внесок здобувача: основні етапи реалізації процедури тестування АК з внесенням мультидефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

108. Odarushchenko O., Kharchenko, Sklyar, V. Multi-Fault Injection Testing: Cases for FPGA-Based NPP I&C Systems. *Proceedings of 23rd International Conference on Nuclear Engineering ICONE-23*, May 17-21, 2015, Chiba, Japan, 2015. URL: https://inis.iaea.org/search/search.aspx?orig_q=RN:48025087 (Дата звереннння: 18.01.2021). (*Особистий внесок здобувача: індустріальний приклад виконання процедури тестування з внесення мультидефекту).* (Видання входить до міжнародної наукометричної бази Scopus).

109. Odarushchenko O., Babeshko E., Kharchenko V., Sklyar V. Toward automated FMEDA for complex electronic products. *Proceedings of the International Conference on Information and Digital Technologies,* July 7-9, 2015, Zilina, Slovakia, 2015. P. 17-22. (*Особистий внесок здобувача: етапи автоматизації техніки FMEDA).* (Видання входить до міжнародної наукометричної бази Scopus).

110. Odarushchenko O., Kharchenko, V. Butenko V., Odarushchenko, E. Markov's Modeling of NPP I&C Reliability and Safety Optimization of tool-and-technique selection. *Proceeding of Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management,* February 15-18, 2016, Beer Sheva, Israel, 2016. P. 328 – 336. (*Особистий внесок здобувача: процедура обрання інструментальних засобів для оцінювання надійності ПТК).* (Видання входить до міжнародної наукометричної бази Scopus).

111. Odarushchenko O., Strjuk O., Bulba Y., Leontiiev K., Ivasyuk A., Kharchenko V. Fault insertion software and hardware testing for safety PLC-based system SIL certification. *Proceeding of the 9th IEEE International Conference on*

Dependable Systems, Services and Technologies, DESSERT'2018, May 24-27, 2018, Kyiv, Ukraine, 2018. P. 202-206. (*Особистий внесок здобувача: визначення FIT – здатності, SW та HW процедури з внесенням дефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

112. Babeshko, E., Kharchenko, V., Odarushchenko, O., Leontiiev, K., Strjuk, O. NPP I&C Safety Assessment by Aggregation of Formal Techniques. *Proceedings of the 2018. 26th International Conference on Nuclear Engineering ICONE26,* July 22-26, 2018, London, England, 2018. P. 1-6. (*Особистий внесок здобувача:процедура SW FMEA).* (Видання входить до міжнародної наукометричної бази Scopus).

113. Одарущенко О.Н., Одарущенко Е.Б. Оценка надежности восстанавливаемых управляющих и вычислительных систем с учетом характеристик средств контроля в условиях дефектов программных и аппаратных средств // Науково-технічна конференція, 10-11 лист. 1999р.:тези доп. Харків, 1999. С.38-39. (*Особистий внесок здобувача: модель оцінювання надійності відновлюваних управлючих систем з урахуванням засобів контролю).*

114.Одарущенко О.Н., Одарущенко Е.Б., Яковлев В.И. Оценка надежности вычислительных систем с учетом изменения параметров отказов и восстановлений их программных средств // 8-я Международная конференция «Теория и техника передачи, приема и обработки информации» (Интегрированные информационные системы, сети и технологии), 17-19 сентября 2002р.: тез. докл. Харьков, 2002. С. 269-271. (*Особистий внесок здобувача*: *методика оцінка надійності обчислювальних систем).*

115. Одарущенко О.Н., Поночовный Ю.Л. Надежность, как критерий качества программного обеспечения// Матеріали Міжнародної науково-технічної конференції «Інтегровані комп'ютерні технології в машинобудуванні – ІКТМ-2003», тези доп. Харків, 2003. С.221. (*Особистий внесок здобувача*: *визначення надійності як критерія якості програмного забезпечення).*

116. Одарущенко О.Н., Харченко В.С., Одарущенко Е.Б. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем// Матеріали 1-ої Міжнар. науково-техн. конф. „Гарантоспроможні (надійні та безпечні) системи, сервіси та технології - DESSERT-2006”, 25-28 квітня 2006р.: тези доп. Полтава, 2006. С. 12. (*Особистий внесок здобувача*: *багатофрагмента модель для дубльованої архітектури ПТК).*

117. Одарущенко О.Н., Руденко А.А. Модель Джелинского-Моранды с учетом недетерминированного числа вторичных дефектов. Матеріали Третьої міжнародної науково-технічної конференції „Комп’ютерна математика в інженерії, науці та освіті“ (CMSEE-2009), 1-31 жовтня 2009р: тези доп. Київ, 2009. С. 49-50. (*Особистий внесок здобувача*: *модифікація МНПЗ Джелинського-Моранди).*

118. Одарущенко О.Н., Руденко А.А. Использование корреляционных зависимостей при прогнозировании числа вторичных дефектов программных средств// Матеріали Четвертої міжнародної науково-технічної конференції „Комп’ютерна математика в інженерії, науці та освіті“ (CMSEE-2010), 1-31 жовтня 2010р.: тези доп. Полтава, 2010. С. 53-54. (*Особистий внесок здобувача*: *приклад формування кореляційної залежності).*

119. Одарущенко О.Н., Живило С.В. Методология оценки гарантоспособности на основе фактического информационно-технического состояния// Материалы междунар одной научно-практической конференции «Информационные технологии и информационная безопасность в науке, технике и образовании (ИНФОТЕХ -2011), 05-10 вер. 2011р.: тези доп. Севастополь, 2011. С.38-39. (*Особистий внесок здобувача*: *визначенння інформаційно-технічного стану, елементи методології).*

120. Одарущенко О.Н., Руденко А.А. Определение параметров оценки надежности программных средств с учетом вторичных дефектов// Шоста науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання систем. МОДС ’2011’’, 27-30 черв. 2011р.: тези доп.

Чернігів, 2010. С. 391-392. (*Особистий внесок здобувача*: *перелік параметрів оцінювання надійності ПЗ з урахуванням вторинних дефектів).*

121. Одарущенко О.Н., Руденко А.А., Руденко З.Н., Мельник М.А. Метод оценивания надежности программных средств с учетом вторичных дефектов// Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013», 24-27 червня 2013р.: тези доп. Чернігів-Жукин, 2013. С. 336-339. (*Особистий внесок здобувача*: *визначення етапів метода оцінювання надійності програмних засобів).*

122. Одарущенко О.Н., Харченко В.С. Моделирование и оценивание функциональной безопасности программно-технических комплексов в контексте стандарта IEC 61508. Восьма міжнародна науково-практична конференція «Математичне та імітаційне моделювання систем. МОДС 2013», 24-27 червня 2013р.: тези доп. Чернігів-Жукин, 2013. С. 339-339. (*Особистий внесок здобувача*: *аналіз IEC 61508, перелік недоліків стандарта, підходи до їх усунення).*

123.Odarushchenko O., Kharchenko V., Butenko V., Odarushchenko E. Assessing of programmable system availability in context of the IEC 61508. *Program 7th International conference - Dependable Systems, Services and Technologies DESSERT2014*, May 16-18, 2014. Kiev, Ukraine. 2014. P.21. (*Особистий внесок здобувача*: *етапи оцінювання надійности ПТК в контексті 61508).*

124. Odarushchenko O., Odarushchenko E, Strjuk O., Leontiiev K., Software Fault Insertion Testing for SIL Certification of Safety PLC-based System. *Proceeding of The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020,* May 14-18, 2020. Kiev, Ukraine. 2020. P.80-84. (*Особистий внесок здобувача*: *деталізована процедура тестування ПЗ з внесенням дефектів).* (Видання входить до міжнародної наукометричної бази Scopus).

125. Одарущенко О.М., Одарущенко О.Б. Концепція і принципи оцінювання і забезпечення надійності та функціональної безпеки програмно-

технічних комплексів. //Сьома міжнародна науково-технічна конференція «Проблеми інформатизації», 13-15 листопада 2019р.: тези доп. Черкаси-Харків-Баку-Більско-Бяла, 2019. С.5. *(Особистий внесок здобувача: Концепція і принципи оцінювання і забезпечення надійності та функціональної безпечності ПТК).*

126.Одарущенко О.М., Одарущенко О.Б. Метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах// Десята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління», 9-19 квітня 2020р.: тези доп. Баку-Харків-Жиліна, 2020. С.20. (*Особистий внесок здобувача*: *метод оцінювання та забезпечення функційної безпеки при розроблені та ліцензуванні модулів і платформ для інформаційно-керуючих систем на програмовних логічних інтегральних схемах).*

127.Odarushchenko O., Kharchenko V., Odarushchenko V. Multi-fragmental availability models of critical infrastructures with variable parameters of system dependability, information & security. *Information and Security. An International Journal*. 2012, Vol. 28, № 2. P. 248 – 265. *(Особистий внесок здобувача*: *багатофрагментні марковські моделі критичних інфраструктур).*

128.Kharchenko V., Odarushchenko O., Odarushchenko V., Popov P. Availability assessment of computer systems described by stiff Markov chains: case study. *Springer.CCIS (412)*. 2013. P. 112 – 135. *(Особистий внесок здобувача: структурна схема надійності відмовостійкості системи, система диференційних рівнянь).* (Видання входить до міжнародної наукометричної бази Scopus).

Праці, які додатково відображають наукові результати дисертації:

129. Одарущенко О.Н., Харченко В.С., Поночовный Ю.Л., Одарущенко Е.Б., Бутенко В.О., Харыбин А.В. Системы и технологии высокой готовности. Харьков, 2013. 273с. (*Особистий внесок здобувача*: *моделювання та оцінка*

комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ).

130. Одарущенко О.Н., Поночовный Ю.Л., Одарущенко Е.Б., Бутенко В.О., Харыбин А.В. Системы и технологии высокой готовности. Харьков, 2013. 96 с. *(Особистий внесок здобувача*: *практичні заняття змоделювання та оцінки комп'ютерних систем високої готовності з урахуванням зміни параметрів потоків відмов і відновлень ПЗ).*

131. Комп'ютерна програма «MSMC-Method selector for Markov chains»: Свідоцтво про реєстрацію авторського права на твір №57120. - Дата реєстрації 05.10.2014. *(Особистий внесок здобувача*: *алгоритм рішення марковських ланцюгів).*

132. Гарантоздатність програмно-технічних комплексів критичного призначення /Ю. Алексеєв, Б. Конорев, В. Скляр, О. Одарущенко, В. Харченко, Г. Чертков// СОУ-Н НКАУ 0060:2010. Настанова національного космічного агенства України. *(Особистий внесок здобувача*: *поняття про інформаційно-технічний стан,, дефекти та уразливості, що призводять до порушення працездатності).*

133.Харченко В.С., Андрейченко Д.К., Антощук С.Г., Дрозд М.А., Одарущенко О.Н., Бульба Е.Н., Стрюк А.Ю., Ивасюк А.О. Зеленая ИТ-инженерия. В 2-х томах. Том 1. Принципы, компоненты, модели. Харьков, 2014. 594с. *(Особистий внесок здобувача*: *опис методів контроля відмов обладнання, опис функційного тестування, аналіз процесів валідації FPGA систем).*

134. Харченко В.С., Скляр В.В.. Одарущенко О.М., Одарущенко О.Б. Університетсько-індустріальна кооперація. Модельно-орієнтований підхід. Практичне керівництво та приклади. Харків, 2017. 363 с. *(Особистий внесок здобувача*: *опис створення spin-off компанії із задачами забезпечення та оцінювання безпеки ІКС).*

135. Барсов В.І., Одарущенко О.М., Краснобаєв В.А., Тиртишніков О.І., Барсова З.В. Основи побудови АСУ. Полтава, 2012. 400с. *(Особистий внесок*

здобувача: загальна характеристика процесу побудови автоматизованих систем управління).

136. Харченко В.С., Одарущенко О.Н., Иванченко О.В. Принципы анализа и управления безопасностью критических инфраструктур. *Вісник Хмельницького національного університету*. 2010. Вип.5. С. 218-221. *(Особистий внесок здобувача*: *принципи забезпечення безпеки).*