НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Леонтієв Костянтин Петрович

УДК 004.052+004.077

ДИСЕРТАЦІЯ

МЕТОДИ І ЗАСОБИ ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ НА ПРОГРАМОВНИХ ПЛАТФОРМАХ З УРАХУВАННЯМ КРИТИЧНОСТІ ПРИПУЩЕНЬ І ПОМИЛОК АНАЛІЗУ

Спеціальність 123 Комп’ютерна інженерія

Галузь знань 12 Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

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

_____ К. П. Леонтієв

Науковий керівник Харченко Вячеслав Сергійович,
член-кореспондент Національної академії наук України,
доктор технічних наук, професор

Харків – 2026

АНОТАЦІЯ

Леонтієв Костянтин Петрович. Методи і засоби оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з урахуванням критичності припущень і помилок аналізу. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія. – Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Дисертацію присвячено теоретичному обґрунтуванню й новому вирішенню актуального наукового завдання розроблення та удосконалення моделей, методів і засобів оцінювання функційної безпечності одно- і багатоверсійних інформаційно-керуючих систем на програмовних платформах з урахуванням розширеної номенклатури одиничних та множинних дефектів та їх комбінацій та зниження залежності від помилок аналізу експертів. Об'єктом дослідження є процеси оцінювання та забезпечення функційної безпечності при розробленні та валідації інформаційно-керуючих систем.

Аналіз безпечності та надійності – критична процедура в рамках життєвого циклу інформаційно-керуючих систем (ІКС). Вимоги до функційної безпечності (ФБ) ІКС АЕС швидко зростають за кількістю, складністю виконання (десятки національних і міжнародних нормативних документів). Зростає номенклатура та обсяг процедур для підтвердження виконання вимог до ФБ ІКС в умовах модернізації технологій (від реалізації логіки до високорівневих вимог). Додається аспект інформаційної безпеки, яка впливає на ФБ (нові стандарти ISO/IEC/IAEA/ДСТУ). Ліцензування платформ і систем потребує великих коштів і монополізується ключовими гравцями ринку (US NRC, exida та ін. : 15-річний досвід НВП Радій/Радікс).

Більшість сучасних технік оцінювання ФБ ІКС АЕС потребують експертної підтримки, незважаючи на наявність інструментальних засобів.

Існує суперечність між рівнем вимог до технологій і засобів оцінювання функційної безпечності ІКС та обмеженістю існуючих XMECA методів щодо аналізу множинних відмов, врахування помилок експертів і врахування аспекту диверсності

У роботі виконано аналіз нормативних вимог, методів і засобів оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах. Встановлено, що нині існуючі методи аналізу видів і наслідків відмов значною мірою залежать від експертних припущень та не забезпечують належного врахування множинних дефектів і помилок аналізу. При цьому питання оцінювання критичності припущень та узгодження експертних оцінок залишаються недостатньо дослідженими. У роботі показано, що підвищення повноти та достовірності оцінювання може бути досягнуто шляхом удосконалення моделей FMECA/FMEDA та застосування спеціалізованих процедур експертного оцінювання.

З урахуванням проведеного аналізу в роботі поставлене та вирішене наукове завдання розроблення та удосконалення моделей, методів і засобів оцінювання функційної безпечності одно- і багатоверсійних інформаційно-керуючих систем на програмовних платформах з урахуванням розширеної номенклатури одиничних та множинних дефектів та їх комбінацій та зниження залежності помилок аналізу експертів.

Обґрунтована методика проведення досліджень і математичний апарат, що використовується. При вирішенні наукових задач використовувалися методи теорії графів та теорії імовірностей, методи системного аналізу, теоретико-множинного опису, теорія надійності та технічної діагностики, методи ризик-орієнтованого FMECA аналізу та експертних оцінок.

Удосконалено моделі і показники для оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з використанням табличного методу аналізу видів і наслідків відмов (FMECA/FMEDA), шляхом визначення і зменшення кількості критичних припущень і обмежень при формуванні і заповненні таблиць, а також детермінованого представлення і

перебору причин відмов і рівнів небезпеки внаслідок різних дефектів, що дозволяє збільшити повноту оцінки.

Удосконалено метод експертного оцінювання функційної безпечності інформаційно-керуючих систем на програмовній логіці при використанні процедур FMECA/FMEDA шляхом зменшення кількості операцій із залученням експертів та впровадження спеціальних сценаріїв узгодження експертних оцінок у вигляді вербальної, нечіткої і кількісної інформації, що дозволяє підвищити достовірність оцінки.

Вперше розроблено метод оцінювання функційної безпечності двохверсійних інформаційно-керуючих систем на програмовних платформах з використанням комбінованих процедур аналізу дефектів версій, який відрізняється від відомих тим, що при аналізі видів та наслідків відмов формуються профілі відносних і абсолютних дефектів, а також використовуються регресійні процедури ін'єктування множинних дефектів з урахуванням їхнього самомаскування і блокування системи, що дозволяє зменшити час і підвищити достовірність оцінки ризиків відмов за загальною причиною.

Усі теоретичні розроблення, виконані у дисертаційній роботі, доведено до конкретних інженерних методик та алгоритмів.

Результати досліджень впроваджені у НВП «Радій», ТОВ «НВП «Радікс» (ІКС АЕС, верифікація), ХАІ (навчальний процес, НДР).

Ключові слова**:** багатоверсійні ІКС, комп'ютерні системи та мережі, інтернет речей, FPGA платформи, кібербезпека і функційна безпечність, інтелектуальні системи для експертного оцінювання, моделювання, діагностичні моделі, патерни проєктування, формальна верифікація, зміна і оцінка вимог.

Список публікацій здобувача за темою дисертації

1. Babeshko E., Kharchenko V., Kovalenko A., Leontiiev K. Cyber security assurance approaches for FPGA-based safety platform configuration tool //

Proceedings of the International Conference on Information and Digital Technologies (IDT 2017). 2017. P. 160–163.

2. Kharchenko V., Brezhniev I., Kovalenko A., Leontiiev K. Secure Environment Establishment for FPGA-based Safety-Critical Systems: Quality Management System Context // Proceedings of the 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2017). San Francisco, California, USA, June 11–15, 2017. P. 434–441.

3. Andrashov A., Leontiiev K., Kovalenko A., Bakhmach I., Kharchenko V. NPP I&C Modernization Approaches Using FPGA-based RadICS Platform // Fourth International Conference on Nuclear Power Plant Life Management. Lyon, France, October 23–27, 2017. P. 14.

4. Kharchenko V., Babeshko E., Leontiiev K., Ruchkov E., Sklyar V. Reliability assessment of safety critical system considering different communication architectures // Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT 2018). 2018. P. 17–20.

5. Kharchenko V., Kovalenko A., Leontiiev K., Panarin A., Duzhy V. Multi-Diversity for FPGA Platform Based NPP I&C Systems: New Possibilities and Assessment Technique // Proceedings of the International Conference on Nuclear Engineering (ICONE 2018). 2018. Paper ID: ICONE26-82377.

6. Babeshko E., Kharchenko V., Leontiiev K., Odarushchenko O., Strjuk O. NPP I&C Safety Assessment by Aggregation of Formal Techniques // Proceedings of the International Conference on Nuclear Engineering (ICONE 2018). 2018. Paper ID: ICONE26-82270.

7. Gordieiev O., Kharchenko V., Leontiiev K. Usability, Security and Safety Interaction: Profile and Metrics Based Analysis // Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing. Vol. 761. Springer, 2018. P. 238–247.

8. Andrashov A., Bakhmach I., Leontiiev K., Kovalenko A., Kharchenko V., Babeshko E. Diversity in FPGA-Based Platform and Platform Based I&Cs

Applications: Strategy and Implementation // Proceedings of the 11th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019). Orlando, Florida, USA, February 9–14, 2019. P. 174–182.

9. Babeshko I., Kovalenko A., Tokarev V., Leontiiev K. FPGA Technology and Platforms for NPP I&C Systems // Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems. Hershey, PA, USA : IGI Global, 2020. Chapter 16. P. 419–457. DOI: 10.4018/978-1-7998-3277-5.ch016.

10. Odarushchenko O., Striuk O., Leontiiev K., Odarushchenko E. Software Fault Insertion Testing for SIL Certification of Safety PLC-Based System // Proceedings of the 11th IEEE International Conference «DEpendable Systems, SERvices and Technologies» (DESSERT'2020). Kyiv, Ukraine, May 14–18, 2020. P. 80–84.

11. Leontiiev K., Babeshko I., Kharchenko V. Assumption Modes and Effect Analysis of XMECA: Expert Based Safety Assessment // Proceedings of the 11th IEEE International Conference «DEpendable Systems, SERvices and Technologies» (DESSERT'2020). Kyiv, Ukraine, May 14–18, 2020. P. 90–94.

12. Гордєєв О. О., Лєонтієв К. П. Модель сценарію оцінювання якості програмного забезпечення // Технічні науки та технології. 2020. № 3(21). С. 209–219. DOI: 10.25140/2411-5363-2020.

13. Гордєєв О. О., Лєонтієв К. П. Модель життєвого циклу дефекту програмного забезпечення // Математичне та комп'ютерне моделювання. Серія: Технічні науки. 2020. Вип. 21. С. 51–60.

14. Babeshko E., Kharchenko V., Leontiiev K., Ruchkov E. Practical Aspects of Operating and Analytical Reliability Assessment of FPGA-Based I&C Systems // Радіоелектронні і комп'ютерні системи. 2020. № 3(95). С. 75–83.

15. Babeshko I., Leontiiev K., Kharchenko V., Brezhniev E. Application of Assumption Modes and Effects Analysis to XMECA // Theory and Engineering of Dependable Computer Systems and Networks. Proceedings of the Sixteenth International Conference on Dependability of Computer Systems (DepCoS-

RELCOMEX 2021). Advances in Intelligent Systems and Computing. Vol. 1389. Springer Nature Switzerland AG, 2021. P. 1–11. DOI: 10.1007/978-3-030-76773-0.

16. Kliushnikov I., Kharchenko V., Fesenko H., Leontiiev K., Illiashenko O. UAV Fleet with Battery Recharging for NPP Monitoring: Queuing System and Routing Based Reliability Models // New Advances in Dependability of Networks and Systems. DepCoS-RELCOMEX 2022. Lecture Notes in Networks and Systems. Vol. 484. Springer, Cham, 2022. P. 133–143. DOI: 10.1007/978-3-031-06746-4_11.

17. Babeshko I., Illiashenko O., Kharchenko V., Leontiiev K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques // Mathematics. 2022. Vol. 10, No. 13. Article 2297. 25 p. DOI: 10.3390/math10132297.

18. Babeshko I., Kharchenko V., Leontiiev K. Enhancing FMECA(XMECA)-based Safety Assessment Considering Criticality of Assumptions and Analysis Errors. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2024, pp. 1-5, doi: 10.1109/DESSERT65323.2024.11122229.

19. Babeshko I., Kharchenko V., Leontiiev K. Method for enhancing FMECA (XMECA) safety assessment procedures considering the criticality of assumptions and analysis errors. *Computer Systems and Information Technologies*, (4), 96–102. https://doi.org/10.31891/csit-2025-4-10.

ANNOTATION

Leontiiev Kostiantyn. Methods and means of evaluating the functional safety of information-management systems on programming platforms, taking into account the criticality of assumptions and analysis errors. – Manuscript copyright.

Thesis on competition of scientific degree of Doctor of Philosophy by specialty 123 Computer Engineering. – National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, 2026.

The dissertation is devoted to improving the completeness and credibility of safety assessment of information and control systems (ICSs) implemented on programmable logic platforms and used in safety-critical applications.

The research analyzes existing standards, methods, and software-hardware tools for safety assessment of programmable-platform-based ICSs. Particular attention is paid to Failure Modes, Effects and Criticality Analysis (FMECA), Failure Modes, Effects and Diagnostics Analysis (FMEDA), and Fault Injection Testing (FIT), as well as to the influence of expert assumptions and analysis errors on assessment results.

Models and indicators for safety assessment based on FMECA/FMEDA procedures have been improved by identifying, formalizing, and reducing critical assumptions used during the construction and completion of analysis tables. A method for expert-based safety assessment has been improved through the introduction of expert judgment aggregation scenarios and procedures supporting verbal, fuzzy, and quantitative assessments. A novel method for assessing dual-version programmable-platform-based ICSs has been developed using combined defect-analysis procedures and fault-injection techniques.

The proposed methods and information technology make it possible to increase the completeness, consistency, and credibility of safety assessment results while reducing the effort required for expert analysis. The developed models, methods, algorithms, and software tools have been validated through practical application in the assessment of safety-critical information and control systems.

Keywords**:** multi-version ICS, computer systems and networks, Internet of Things, FPGA, cybersecurity and functional safety, intelligent systems for expert assessment, modeling, diagnostic models, design patterns, formal verification, requirements change and assessment.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AMECA	Assumption Modes, Effects and Criticality Analysis
AXI	розширений масштабований інтерфейс – Advanced eXtensible Interface
B-Method	формальний метод B – B-Method
CAD	автоматизоване проєктування – Computer-Aided Design
CCF	відмова за спільною причиною – Common Cause Failure
CCFA	Common Cause Failure Analysis
CDC	перетин тактових доменів – Clock Domain Crossing
CRC	циклічний надлишковий код – Cyclic Redundancy Check
DC	Diagnostic Coverage
DCM	цифровий менеджер тактового сигналу – Digital Clock Manager
DD	небезпечна виявлена відмова – Dangerous Detected
DMVS	множина дефектів багатоверсійної системи – Defects of Multi-Version Systems
DU	небезпечна невиявлена відмова – Dangerous Undetected
EM	електроміграція – Electromigration
EMI	електромагнітні завади – Electromagnetic Interference
ETA	Event Tree Analysis
Event-B	формальний метод моделювання та верифікації – Event-B
FIT	Fault Injection Testing
FIT	кількість відмов на 10^9 годин роботи – Failures In Time
FMEA	Failure Modes and Effects Analysis
FMEA	аналіз видів і наслідків відмов – Failure Mode and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis

FMECA	аналіз видів, наслідків і критичності відмов – Failure Modes, Effects and Criticality Analysis
FMEDA	Failure Modes, Effects and Diagnostics Analysis
FPGA	програмовна вентильна матриця – Field-Programmable Gate Array
FSM	кінцевий автомат – Finite State Machine
FTA	Fault Tree Analysis
HAZOP	Hazardous Operations
HCI	ін’єкція гарячих носіїв – Hot Carrier Injection
HDL	мова апаратного опису – Hardware Description Language
I/O	введення/виведення – Input/Output
IEC	International Electrotechnical Commission
IMECA	Intrusion Modes, Effects And Criticality Analysis
IP	інтелектуальний програмний/апаратний блок – Intellectual Property (IP Core)
JTAG	група спільних дій з тестування – Joint Test Action Group
MATLAB	матрична лабораторія – MATrix LABoratory
MEMS	мікроелектромеханічні системи – Micro-Electro-Mechanical Systems
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
MV	багатоверсійний – Multi-Version
MVS	багатоверсійна система – Multi-Version System(s)
MVSD	дефекти багатоверсійних систем – Multi-Version Systems Defects
MVSD-FMEA	FMEA багатоверсійних систем з урахуванням дефектів – Multi-Version Systems Defects FMEA
NaN	не число – Not a Number
NBTI	нестабільність при негативному зміщенні під дією температури –

	Negative Bias Temperature Instability
PFD	Probability of Failure on Demand
PFDavg	середня ймовірність небезпечної відмови при вимозі – Average Probability of Failure on Demand
PFH	імовірність небезпечної відмови за годину – Probability of dangerous Failure per Hour
PLC	програмований логічний контролер – Programmable Logic Controller
PLL	фазове автопідстроювання частоти – Phase-Locked Loop
PSN	шум джерела живлення – Power Supply Noise
RBD	Reliability Block Diagram
RPN	число пріоритету ризику – Risk Priority Number
RRF	Risk Reduction Factor
SCADA	Supervisory Control And Data Acquisition
SD	безпечна виявлена відмова – Safe Detected
SEE	одноразові радіаційні ефекти – Single Event Effects
SEL	одноразове защіпання – Single Event Latch-up
SET	одноразовий перехідний імпульс – Single Event Transient
SEU	одноразове порушення стану – Single Event Upset
SFF	Safe Failure Fraction
SFF	частка безпечних відмов – Safe Failure Fraction
SIF	функція безпеки приладової системи – Safety Instrumented Function
SIL	Safety Integrity Level
SoC	система на кристалі – System on Chip
SPOF	єдина точка відмови – Single Point of Failure
SPI	послідовний периферійний інтерфейс – Serial Peripheral Interface

SU	безпечна невиявлена відмова – Safe Undetected
SystemVerilog	мова апаратного опису SystemVerilog – SystemVerilog Hardware Description Language
Verilog	мова апаратного опису Verilog – Verilog Hardware Description Language
VHDL	мова апаратного опису VHDL – VHSIC Hardware Description Language
VMVS	множина вразливостей багатоверсійної системи – Vulnerabilities of Multi-Version Systems
Yosys	відкрите середовище синтезу апаратної логіки – Yosys Open Synthesis Framework
Z-notation	формальна математична нотація Z
АЗ	апаратні засоби
БД	база даних
ІБР	імовірність безвідмовної роботи
ІЗ	інструментальні засоби
ІКС	інформаційно-керуючі системи
ІТ	інформаційна технологія
МЕК	міжнародна електротехнічна комісія
НВП	науково-виробниче підприємство
НД	нормативний документ
НДР	науково-дослідна робота
ОС	операційна система
ПАЗ	протиаварійний захист
ПАТ	публічне акціонерне товариство
ПЗ	програмне забезпечення
ПЛ	програмовна логічна платформа

ПЛІС	програмована логічна інтегральна схема
ППЛ	платформи на програмовній логіці
РПД	ризики прихованих дефектів
САПР	система автоматизованого проєктування
ССН	структурна схема надійності
ТЗ	технічне завдання
ТОВ	товариство з обмеженою відповідальністю
ФБ	функційна безпечність

ВСТУП

Обґрунтування вибору теми дослідження. Стрімкий розвиток цифрових технологій та широке впровадження програмовних платформ в інформаційно-керуючі системи критичного призначення зумовлюють необхідність удосконалення методів оцінювання їх функційної безпечності. Особливої актуальності ця проблема набуває для систем атомної енергетики, транспортної інфраструктури та промислової автоматизації, де помилки проєктування, дефекти реалізації або некоректні припущення можуть призвести до значних економічних втрат та створення небезпечних ситуацій.

Теоретичні і прикладні дослідження з аналізу функційної безпечності інформаційно-керуючих систем та інфраструктур виконано українськими та закордонними науковцями Є. В. Брежнєвим, В. А. Заславським, О. В. Іванченком, Б. М. Коноревим, О. М. Одарущенком, В. В. Скляром, В. С. Харченком, М. О. Ястребенецьким; Альгірдасом Авіженісом, Робіном Блумфілдом, Річардом Вудом, Фелічітою Ді-Джандоменіко, Ненсі Левенсон, Бевом Літлвудом, Пітером Поповим та ін. Однак, програмовні платформні рішення ІКС, важливих для безпеки АЕС, інших критичних застосувань стають дедалі складнішими, вимоги стандартів і сертифікаційних компаній – жорсткішими, тому методи оцінювання мають враховувати специфіку електронних компонент і проєктів, а також суттєву замученість експертів, У зв’язку з цим актуальним є розроблення моделей, методів і засобів оцінювання функційної безпечності, які враховують критичність припущень і можливі помилки експертного аналізу.

Об’єкт дослідження – процеси оцінювання та забезпечення функційної безпечності при розробленні та валідації інформаційно-керуючих систем.

Предмет дослідження – методи і засоби оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з урахуванням критичності припущень і помилок аналізу відмов компонентів.

Метою дисертаційної роботи є підвищення повноти та достовірності оцінювання функційної безпечності ІКС на платформах програмовної логіки (програмовних платформах) зі структурно-версійною надмірністю шляхом розроблення і практичного впровадження методів та засобів аналізу виду та наслідків відмов (FMEDA), обумовлених фізичними та проєктними дефектами.

Для досягнення поставленої мети необхідно вирішити такі **задачі**:

– провести аналіз існуючих методів і програмно-апаратних засобів оцінювання функційної безпечності інформаційно-керуючих систем АЕС, інших критичних застосувань, обґрунтувати завдання і методику досліджень;

– удосконалити моделі і показники для оцінки функційної безпечності інформаційно-керуючих систем на програмовних платформах з використанням табличного методу аналізу видів і наслідків відмов (FMECA/FMEDA);

– удосконалити метод оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з використанням аналізу видів і наслідків відмов (FMECA), який виконується із залученням експертів;

– розробити метод оцінювання функційної безпечності двохверсійних інформаційно-керуючих систем на програмовних платформах з урахуванням множини проєктних і фізичних дефектів;

– розробити алгоритми і програмно-апаратні засоби оцінювання та вибору засобів підвищення функційної безпечності інформаційно-керуючих систем на програмовних платформах;

– виконати практичне впровадження розроблених методів і засобів оцінювання функційної безпечності одно- і двохверсійних систем при створенні інформаційно-керуючих систем АЕС.

Методи дослідження. При вирішенні наукових задач використовувалися такі методи: методи системного аналізу, теоретико-множинного опису, теорія надійності та технічної діагностики, методи ризик-орієнтованого FMECA аналізу та експертних оцінок.

Наукова новизна отриманих результатів полягає в тому, що:

1) **удосконалено** моделі і показники для оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з використанням табличного методу аналізу видів і наслідків відмов (FMECA/FMEDA), шляхом визначення і зменшення кількості критичних припущень і обмежень при формуванні і заповненні таблиць, а також детермінованого представлення і перебору причин відмов і рівнів небезпеки внаслідок різних дефектів, що дозволяє збільшити повноту оцінки.

2) **удосконалено** метод експертного оцінювання функційної безпечності інформаційно-керуючих систем на програмовній логіці при використанні процедур FMECA/FMEDA шляхом зменшення кількості операцій із залученням експертів та впровадження спеціальних сценаріїв узгодження експертних оцінок у вигляді вербальної, нечіткої і кількісної інформації, що дозволяє підвищити достовірність оцінки.

3) **вперше розроблено** метод оцінювання функційної безпечності двохверсійних інформаційно-керуючих систем на програмовних платформах з використанням комбінованих процедур аналізу дефектів версій, який відрізняється від відомих тим, що при аналізі видів та наслідків відмов формуються профілі відносних і абсолютних дефектів, а також використовуються регресійні процедури ін’єктування множинних дефектів з урахуванням їхнього самомаскування і блокування системи, що зменшує час і підвищує достовірність оцінки ризиків відмов за загальною причиною.

Особистий внесок здобувача полягає у постановці задач дослідження, розробленні моделей і методів оцінювання функційної безпечності ІКС на програмовних платформах, проведенні теоретичних досліджень, розробленні алгоритмів та програмних засобів, виконанні експериментальних досліджень і аналізі отриманих результатів. У працях, опублікованих у співавторстві, здобувачеві належать результати, пов’язані з розробленням процедур експертного оцінювання, удосконаленням методів FMECA/FMEDA та оцінюванням критичності припущень і помилок аналізу.

Апробація матеріалів дисертації. Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на міжгалузевому науково-технічному семінарі «Критичні комп'ютерні технології та системи» на кафедрі кібербезпеки та інтелектуальних інформаційних технологій у Національному аерокосмічному університеті «ХАІ».

Наукові результати роботи доповідалися також на:

– міжнародній науково-технічній конференції «Dependable Systems, Services and Technologies»;

– міжнародній конференції з надійності та безпеки критичних комп'ютерних систем DepCoS-RELCOMEX;

– міжнародній конференції з ядерної інженерії ICONE;

– міжнародній конференції Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT).

Структура та обсяг дисертації.

Дисертація складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та додатків. Повний обсяг роботи становить 208 сторінок друкованого тексту, з них анотація – на 3 стор., зміст – на 3 стор., перелік умовних скорочень – на 5 стор., основний текст – на 168 стор., список зі 90 використаних джерел – на 12 стор., додатки – на 11 стор. Дисертація містить 21 рисунок та 15 таблиць.

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

Дослідження, результати яких викладені в дисертації, проводилися відповідно до державних планів НДР, програм та договорів, виконаних в Національному аерокосмічному університеті, «ХАІ» та індустріальних підприємствах галузі атомної енергетики відповідно до державних і галузевих програм модернізації інформаційно-керуючих систем АЕС, а саме:

– Науково-виробничому підприємстві «Радій» – при розробленні та впровадженні ІКС на енегроблоках Рівненської, Хмельницької та Південноукраїнської атомних станцій, зокрема, в систем аварійного захисту та суміжних систем, реалізованих на сертифікованих програмовних платформах;

– Науково-виробничому підприємстві «Радікс» – при виконанні сертифікації платформи RadICS на відповідність вимогам стандарту IEC61508 (рівень SIL3 для одного каналу) та вимогам американського ядерного регулятора US NRC.

Роль автора в цих НДР і проєктах, в яких він є безпосереднім виконавцем, полягає у розробленні, експериментальній перевірці та впровадженні нових і удосконалених методів та програмно-апаратних засобів для оцінювання функційної безпеки ЫКС АЕС на базі FMECA-FIT процедур з урахуванням критичності припущень і помилок експертів.

Практичне значення отриманих результатів. Практичне значення отриманих результатів полягає в доведенні теоретичних положень дисертації до конкретних алгоритмів, рекомендацій та їх безпосередньому використанні на підприємствах, що займаються розробленням та впровадженням інформаційно-керуючих систем у галузях, критичних до безпеки. Зокрема, до практичних результатів слід віднести:

– алгоритм AMECA аналізу критичності припущень;

– алгоритм експертного оцінювання результатів FMECA/FMEDA;

– алгоритми формування узгоджених експертних оцінок;

– програмні засоби підтримки процедур оцінювання функційної безпечності та ін..

Результати дисертаційної роботи впроваджено у (додаток Б):

– НВП «Радій» при розробленні та впровадженні ІКС АЕС, зокрема систем аварійного захисту реакторів (акт впровадження від 12.05.2026 р.);

– ТОВ «Радікс» при реалізації процесів сертифікації платформи RadICS на відповідність вимогам стандарту IEC61508 та US NRC (акт впровадження від 12.05.2026р.);

– навчальному процесі Національного аерокосмічного університету «ХАІ» – при викладанні курсів «Надійність та функційна безпечність інформаційно-керуючих систем», «Сучасні технології програмної інженерії» та ін. (акт впровадження від 10.03.2026 р.).

РОЗДІЛ 1.
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ І ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ НА ПРОГРАМОВНИХ ПЛАТФОРМАХ

1.1. Аналіз вимог до безпечності ІКС АЕС та інших критичних систем

1.1.1. Основні поняття. Функційна та інформаційна безпечність

Інформаційно-керуючі системи критичного призначення характеризуються одночасною наявністю апаратних, програмних та комунікаційних компонентів, відмова або некоректна поведінка яких може впливати на виконання функцій, критичних до безпеки. Особливу групу становлять ІКС АЕС, для яких застосування програмовних логічних платформ, зокрема FPGA, дозволяє реалізовувати складні функції керування та захисту, але водночас розширює множину потенційних причин відмов.

З розвитком цифрових технологій значна частина функцій ІКС реалізується на програмовних електронних платформах. До них належать мікропроцесорні системи, FPGA, програмовані контролери та інші програмовні цифрові пристрої. Застосування таких платформ забезпечує високу гнучкість, можливість реалізації складних алгоритмів керування та діагностування, апаратну реконфігурацію, використання різних архітектур резервування і диверсності, а також можливість інтеграції апаратних і програмних засобів. Водночас програмовна реалізація функцій безпеки призводить до розширення множини потенційних джерел небезпечних відмов, які повинні враховуватися під час оцінювання.

У роботах, присвячених ІКС АЕС на базі технологій FPGA, показано, що застосування FPGA як основи критичних до безпеки платформ потребує одночасного врахування властивостей апаратної платформи, програмної конфігурації, інтерфейсів, архітектури системи та засобів забезпечення диверсності. У роботі [1] розглядаються технології та платформи FPGA для ІКС

АЕС, а в роботах [2, 3] досліджуються питання диверсності та архітектурних засобів підвищення стійкості ІКС до відмов, у тому числі відмов загальної причини.

У загальному випадку безпечність системи визначається її здатністю виконувати задані функції таким чином, щоб ризик виникнення небезпечних наслідків підтримувався на прийнятному рівні. Для інформаційно-керуючих систем доцільно розглядати безпечність не як одну ізольовану властивість, а як комплекс характеристик, пов’язаних із коректністю виконання функцій, стійкістю до відмов, здатністю виявляти небезпечні стани та протидіяти зовнішнім впливам.

Одним із центральних понять цього дослідження є функційна безпечність (functional safety). Відповідно до загальної концепції IEC 61508, функційна безпечність є частиною загальної безпечності, яка залежить від правильного функціонування електричних, електронних та програмовних електронних систем, пов’язаних із безпекою. Її досягнення передбачає виконання заданих функцій безпеки з необхідною характеристикою безпеки протягом визначеного життєвого циклу системи. Таким чином, функційна безпечність безпосередньо пов’язана з правильним виконанням safety functions та досягненням необхідного рівня safety integrity.

Для ІКС функційна безпечність означає, що система повинна не лише виконувати свої функції в штатному режимі, а й правильно реагувати на відмови, несправності та інші передбачені небезпечні події. У цьому контексті необхідно розрізняти функціональну працездатність системи та її функційну безпечність. Працездатна система може виконувати заданий алгоритм керування, однак це саме по собі не гарантує безпечності. Наприклад, система може продовжувати функціонувати після виникнення дефекту, але формувати неправильний керуючий сигнал, який створює небезпечний стан об’єкта. Тому під час оцінювання необхідно встановлювати не тільки факт виникнення відмови, але й характер її впливу на функції системи та кінцевий ефект для об’єкта керування.

У критичних ІКС доцільно виділяти такі взаємопов’язані рівні розгляду:

– об’єкт керування та його потенційно небезпечні стани;

– функції безпеки для запобігання або обмеження небезпечних наслідків;

– ІКС, яка реалізує відповідні функції;

– апаратні, програмні та комунікаційні компоненти ІКС;

– дефекти та відмови окремих компонентів;

– види відмов (failure modes);

– наслідки відмов (failure effects);

– критичність відмов для функцій та системи в цілому.

Таке представлення є принциповим для подальшого застосування FMECA/FMEDA, оскільки ці методи встановлюють відповідність між елементом системи, потенційним видом його відмови та наслідками такої відмови. Отже, оцінювання функційної безпечності фактично передбачає встановлення ланцюга «компонент → дефект → вид відмови → наслідок → вплив на функцію безпеки → критичність».

У випадку програмовних платформ зазначений ланцюг повинен охоплювати як апаратні, так і програмні дефекти. Для заснованих на FPGA систем додатково необхідно враховувати конфігураційні дані, логічну структуру, апаратні інтерфейси, тактові та комунікаційні засоби. У роботах [1, 4] показано, що оцінювання надійності та безпечності заснованих на FPGA ІКС може виконуватися із застосуванням декількох взаємодоповнюючих аналітичних та експериментальних методів, зокрема RBD, FTA, FMECA/FMEDA та тестування з засівом дефектів.

Функційна безпечність тісно пов’язана з поняттям надійності, однак надійність характеризує здатність системи виконувати необхідні функції протягом заданого часу та за заданих умов, тоді як функційна безпечність концентрується на здатності системи виконувати функції, критичні для запобігання або зменшення небезпечних наслідків. Відмова компонента не обов’язково означає втрату функції безпеки, якщо система має відповідні діагностичні засоби, засоби резервування або диверсності. Водночас навіть

одинична відмова може бути критичною, якщо вона призводить до втрати необхідної функції безпеки.

У зв’язку з цим важливо враховувати не тільки одиничні відмови, але й комбінації відмов. Особливо це стосується багатоверсійних та резервованих ІКС, у яких декілька компонентів або версій можуть зазнавати одночасних чи взаємопов’язаних дефектів. У роботах [2, 3] досліджувалося застосування диверсності для FPGA платформ та ІКС АЕС як засобу зниження ризику відмов загальної причини. Застосування диверсності змінює характер задачі оцінювання безпеки: необхідно оцінювати не тільки незалежні відмови окремих компонентів, а й можливість того, що одна причина спричиняє відмови декількох каналів або версій системи.

Іншою важливою характеристикою ІКС є діагностованість. Виявлення відмови до того, як вона призведе до небезпечного ефекту, може суттєво змінювати результат оцінювання функційної безпечності. Саме тому для програмовних платформ доцільно розглядати не тільки FMECA, але й FMEDA, у якому для видів відмов додатково оцінюється можливість їх виявлення діагностичними засобами. У подальшому це дозволяє враховувати співвідношення виявлених і невиявлених небезпечних відмов та їхній внесок у показники функційної безпечності.

Окрему групу характеристик становлять інформаційна безпечність та кібербезпека. Для цифрових ІКС порушення конфіденційності, цілісності або доступності інформації може мати не лише інформаційні, але й функційно-безпечні наслідки. Наприклад, несанкціонована модифікація конфігурації програмовної платформи, зміна переданих даних або порушення доступності критичного каналу можуть призвести до некоректного функціонування системи. Тому в критичних ІКС питання функційної безпеченості та інформаційної безпечності не повинні розглядатися як повністю незалежні.

У роботі [5] досліджується взаємодія функційної безпеченості та інформаційної безпечності і показано необхідність комплексного розгляду цих характеристик. Для ІКС АЕС це має особливе значення, оскільки цифрові

системи одночасно повинні забезпечувати правильність виконання функцій безпеки та стійкість до несанкціонованих впливів. Водночас функційна безпечність і кібербезпека мають різні цілі, моделі загроз та методи оцінювання. Тому в межах цього дослідження інформаційна безпечність розглядається насамперед у частині її потенційного впливу на функційні властивості та безпечне функціонування ІКС.

Для подальшого дослідження доцільно розрізняти поняття «небезпечний дефект», «відмова» та «небезпечний ефект». Дефект є причиною або внутрішнім станом, який може спричинити неправильне функціонування компонента. Відмова є подією або переходом системи до стану, у якому вона не виконує задану функцію належним чином. Ефект відмови характеризує результат її прояву на відповідному рівні системи. Один і той самий дефект може мати різні ефекти залежно від архітектури, режиму роботи, наявності діагностики та резервування.

Це розмежування є особливо важливим для тестування з засівом дефектів (fault injection testing, FIT). Під час засіву дефектів необхідно встановлювати не тільки факт створення штучної несправності, а й відповідь системи на неї: виявлення дефекту, локалізацію, перехід до резервного каналу, блокування небезпечного результату або, навпаки, формування небезпечного виходу. У роботах [6] та [7] розглядається застосування тестування з засівом дефектів для підтвердження характеристик критичних до безпеки систем та сертифікації на відповідність рівню повноти безпеки SIL.

Таким чином, функційну безпечність у межах цього дослідження доцільно розглядати як комплексну властивість програмовної ІКС виконувати визначені функції безпеки із заданою цілісністю та забезпечувати прийнятну реакцію на передбачені дефекти, відмови та їх комбінації протягом життєвого циклу. Таке визначення безпосередньо пов’язує функційну безпечність із процедурами FMECA/FMEDA, тестуванням з засівом дефектів, резервуванням, диверсністю та діагностикою. При цьому результат оцінювання функційної безпечності залежить не тільки від властивостей досліджуваної системи, але й

від побудованої моделі аналізу. Під час формування FMECA/FMEDA необхідно визначити склад компонентів, множину можливих видів відмов, наслідки, ймовірності, тяжкість наслідків, діагностичне покриття та комбінації відмов. Значна частина таких рішень ґрунтується на експертних судженнях. Тому припущення, зроблені експертом під час побудови таблиці аналізу, фактично стають частиною моделі, на якій ґрунтується висновок про безпечність системи. Саме ця обставина є принциповою для подальшого дослідження. У роботах [8-11] показано, що результати XMECA можуть залежати від припущень щодо складу системи, множини відмов, їхньої множинності, рівнів системи, взаємодії між рівнями та інших параметрів аналізу. Зокрема, неврахування окремих компонентів або видів відмов може призводити до завищення оцінки безпечності, тоді як включення надлишкових компонентів чи відмов – до її заниження.

Отже, оцінювання функційної безпечності повинно враховувати не лише невизначеність параметрів, але й самої структури моделі. Це підтверджується результатами аналізу моделей життєвого циклу дефектів та їх впливу [11-14], різних модифікацій процедур оцінювання критичності відмов з використанням табличних методів і методів інєктування дефектів [15-19].

Таким чином, у під час аналізу методів оцінювання функційної безпечності основну увагу доцільно зосередити на FMECA/FMEDA та FIT як на взаємодоповнюючих засобах аналітичного й експериментального оцінювання. Водночас необхідно дослідити вплив експертних припущень та помилок аналізу на повноту й достовірність отриманих результатів. Це створює основу для застосування XMECA та AMECA і для розроблення методів підвищення достовірності оцінювання функційної безпечності програмовних ІКС.

1.1.2. Аналіз вимог стандартів

Оцінювання функційної безпечності інформаційно-керуючих систем, що застосовуються у критичних системах, повинно здійснюватися з урахуванням

нормативних вимог, які визначають принципи побудови, розроблення, верифікації, валідації, експлуатації та оцінювання таких систем. Для ІКС атомних електростанцій нормативна база має багаторівневу структуру і включає загальні стандарти функційної безпечності, галузеві стандарти для ядерної енергетики, документи щодо програмного забезпечення та програмовних цифрових пристроїв, а також документи, що регламентують питання диверсності, незалежності та захисту від відмов загальної причини.

У контексті цього дослідження особливе значення мають IEC 61508 [20], IEC 61513 [21], IEC 60880 [23], IEC 62138 [24], IEC 61226 [25], а також IEEE 7-4.3.2 [26]. Зазначені документи формують нормативну основу для забезпечення необхідної функційної безпечності цифрових ІКС та визначають вимоги, які повинні бути враховані при розробленні методів їх аналізу.

Базовим міжнародним стандартом у сфері функційної безпечності електричних, електронних та програмовних електронних систем, пов’язаних із безпекою, є IEC 61508 [20]. Стандарт встановлює системний підхід до забезпечення функційної безпечності протягом життєвого циклу критичних до безпеки систем. Його концепція передбачає послідовний перехід від аналізу небезпек і визначення необхідного зниження ризику до формування вимог до функцій безпеки, проєктування системи, реалізації, верифікації, валідації, експлуатації та модифікації.

Стандарт IEC 61508 [20] пов’язує функційну безпечність із правильним виконанням визначених функцій безпеки та необхідною повнотою безпеки. Таким чином, недостатньо продемонструвати лише функціональну працездатність системи. Необхідно обґрунтувати, що система з необхідною ймовірністю виконує функцію безпеки в умовах передбачених відмов, несправностей та інших небезпечних подій.

Зазначена вимога має безпосередній зв’язок із FMECA/FMEDA та FIT. FMECA дозволяє систематично визначати види відмов компонентів та оцінювати їхні наслідки і критичність. FMEDA доповнює цей аналіз оцінюванням діагностичних можливостей системи. FIT забезпечує

експериментальну перевірку поведінки системи при ін’єктуванні дефектів. У такий спосіб аналітичне та експериментальне оцінювання можуть використовуватися як взаємодоповнюючі засоби підтвердження виконання вимог функційної безпечності.

У галузі атомної енергетики загальні принципи функційної безпечності доповнюються спеціалізованими вимогами до ІКС АЕС. Основним документом загального рівня для систем керування та контролю, важливих для безпеки, є IEC 61513 [21]. Стандарт встановлює вимоги та рекомендації до загальної архітектури ІКС, яка може містити традиційні апаратні засоби, комп’ютеризовані системи або їх комбінацію.

Особливістю IEC 61513 [21] є розгляд вимог до ІКС у контексті загального життєвого цикла безпеки. Вимоги до окремих ІКС повинні бути пов’язані з вимогами та цілями безпеки АЕС, а архітектура ІКС повинна забезпечувати реалізацію необхідних функцій безпеки. У третій редакції IEC 61513:2026 [22] додатково підкреслено, що повні та точні вимоги, похідні від цілей безпеки атомної електростанції, є необхідною передумовою формування комплексних вимог до ІКС та окремих систем. Неповнота вимог на верхньому рівні може призвести до неповноти вимог до окремих компонентів і, відповідно, до неповноти множини відмов, що розглядаються під час FMECA/FMEDA. Тому повнота аналізу безпечності не може забезпечуватися лише коректністю обчислень усередині FMECA. Необхідно також забезпечити повноту вихідної моделі системи та вимог, на основі яких формується таблиця аналізу.

Окреме місце займає IEC 61226 [25], який встановлює категоризацію функцій ІКС, важливих для безпеки. Категоризація функцій дозволяє визначати рівень значущості відповідної функції та є основою для подальшого встановлення вимог до архітектури, програмного забезпечення та засобів верифікації й валідації.

Для комп’ютеризованих систем, що виконують функції категорії А, застосовується IEC 60880. Стандарт визначає вимоги до програмного

забезпечення комп’ютеризованих ІКС АЕС, включаючи вимоги до специфікації, проєктування, реалізації, верифікації, валідації та документації. Таким чином, програмна частина ІКС розглядається не ізольовано, а як складова критичної до безпеки системи, для якої повинна бути забезпечена необхідна якість та надійність.

Особливе значення для програмовних платформ має IEEE 7-4.3.2 [26]. Цей стандарт встановлює додаткові критерії для програмовних цифрових пристроїв, що використовуються як компоненти систем безпеки атомних електростанцій. Під програмовним цифровим пристроєм розуміється пристрій, який використовує програмні інструкції або програмовану логіку для виконання певної функції. До цієї категорії належать, зокрема, комп’ютери, програмовані апаратні пристрої та пристрої з firmware.

Застосування IEEE 7-4.3.2 [26] є особливо актуальним для ІКС на FPGA-платформах, оскільки FPGA поєднує властивості апаратного та програмовного засобу. Логічна функціональність пристрою визначається програмованою конфігурацією, а тому при оцінюванні необхідно враховувати як фізичні та апаратні відмови, так і дефекти конфігурації та логіки. Саме ця особливість пояснює доцільність використання комбінованих методів аналітичного та експериментального оцінювання.

Важливою вимогою до safety-critical ІКС є забезпечення незалежності та захисту від відмов загальної причини (Common Cause Failures, CCF). Наявність резервованих каналів сама по собі не гарантує необхідного рівня функційної безпечності, якщо декілька каналів можуть бути одночасно уражені однією фізичною, систематичною або проєктною причиною. Тому при оцінюванні необхідно аналізувати не тільки одиничні відмови, а й множинні відмови, включаючи відмови різних каналів та версій системи. Застосування диверсності є одним із засобів зниження ризику CCF. Для оцінювання відповідної архітектури необхідно встановлювати, які дефекти є незалежними, які можуть бути спільними для декількох каналів, а також які комбінації дефектів можуть призвести до втрати функції безпеки.

Ще одним нормативно значущим аспектом є верифікація та валідація. Вимоги до програмного забезпечення передбачають виконання систематичних процедур перевірки на різних етапах життєвого циклу. При цьому аналітичні методи, такі як FMECA, FTA та інші, не повинні розглядатися як заміна випробувань. Навпаки, для підвищення достовірності оцінювання доцільним є поєднання аналітичних та експериментальних методів.

У цьому контексті важливим є тестування з засівом дефектів. Основна ідея полягає у створенні контрольованих дефектів та спостереженні за реакцією системи. Отримані результати дозволяють перевірити здатність системи виявляти та локалізувати дефекти, перемикатися на резервні засоби або блокувати небезпечні виходи.

Таким чином, нормативна база формує декілька груп вимог, безпосередньо пов’язаних із предметом цього дослідження.

Першу групу становлять вимоги до визначення функцій безпеки та їхніх характеристик. Для кожної функції безпеки необхідно визначити призначення, умови активації, необхідний рівень цілісності та допустиму реакцію системи на відмови. Другу групу становлять вимоги до системної архітектури. Вони охоплюють резервування, незалежність, диверсність, сегментацію, комунікаційні структури та заходи протидії CCF.

Третю групу становлять вимоги до апаратних та програмних компонентів, включаючи FPGA. Четверту групу становлять вимоги до верифікації та валідації, які передбачають систематичну перевірку відповідності реалізації встановленим вимогам.

П’яту групу становлять вимоги до оцінювання надійності та функційної безпечності, у межах яких застосовуються аналітичні та експериментальні методи, включаючи FMEA/FMECA, FTA, FMEDA та засів дефектів. Шосту групу становлять вимоги до документації, простежуваності (трасування) та обґрунтування результатів. Для критичних до безпеки систем принциповим є забезпечення можливості відтворити логіку прийнятих інженерних рішень і перевірити відповідність результатів вихідним вимогам.

Навіть за наявності формально визначеної процедури FMECA/FMEDA результат аналізу залежить від того, як саме аналітик сформував модель системи. Необхідно визначити, які компоненти включити до аналізу, які види відмов враховувати, які наслідки приписувати цим відмовам, які комбінації відмов розглядати та які рівні системи включати до моделі.

Отже, нормативні вимоги самі по собі не усувають невизначеність процесу оцінювання безпеки. Вони визначають необхідні властивості та результати, але конкретна модель аналізу формується із застосуванням інженерних методів і, в багатьох випадках, експертних суджень. Саме тому одна з ключових проблем, що випливає з аналізу нормативної бази, полягає у необхідності забезпечення повноти та відтворюваності процедур оцінювання.

У роботі [15] показано, що експертні припущення можуть впливати на результат аналізу XMECA. Подальший розвиток цього підходу у роботі [18] передбачає систематичний розгляд припущень та їхніх наслідків. У роботі [19] запропоновано поєднання експертних та інструментальних процедур для підвищення достовірності результатів.

Проведений аналіз дозволяє сформулювати принципову вимогу до методів оцінювання функційної безпечності програмовних ІКС: процедура повинна забезпечувати не тільки правильне оброблення заданих даних, але й контроль повноти та обґрунтованості вихідної моделі. Зокрема, необхідно контролювати припущення щодо складу системи, множини відмов, множинності дефектів, взаємодії між рівнями, апаратних і програмних дефектів та діагностованості.

Таким чином, нормативні документи задають цілі та загальні вимоги до функційної безпечності, тоді як FMECA/FMEDA, FIT та інші методи забезпечують практичні засоби оцінювання відповідності цим вимогам. Проте традиційне застосування зазначених методів може залишати неявними припущення, зроблені під час побудови моделі. Це створює потенційну причину неповноти або систематичної похибки оцінювання.

Отже, подальше дослідження повинно бути спрямоване на формування такого профілю вимог до ІКС на програмовних платформах, який, крім традиційних характеристик функційної безпечності, враховує повноту аналізу, можливість розгляду одиничних і множинних дефектів, діагностичне покриття, диверсність та CCF, а також контроль критичних експертних припущень. Такий підхід створює нормативне та методологічне підґрунтя для розроблення моделей і методів.

1.1.3. Формування профілю вимог для ІКС ППЛ АЕС

Проведений понять функційної безпечності та нормативних вимог до інформаційно-керуючих систем (ІКС) дозволяє сформувати профіль вимог до ІКС на програмовних платформах, призначених для застосування на атомних електростанціях. Необхідність формування такого профілю зумовлена тим, що вимоги до безпечності розподілені між нормативними документами різного рівня та охоплюють функціональні, апаратні, програмні, архітектурні, експлуатаційні й організаційні аспекти.

Під профілем вимог до ІКС АЕС розуміється систематизована сукупність вимог та характеристик, які повинні бути враховані під час розроблення, аналізу, верифікації, валідації та оцінювання функційної безпечності ІКС, реалізованої на програмовній платформі. Профіль повинен забезпечувати зв’язок між цілями та функціями безпеки АЕС, вимогами до ІКС, архітектурними та технічними рішеннями, можливими дефектами й відмовами та показниками, за якими здійснюється оцінювання функційної безпечності.

Для ІКС на програмовних платформах такий профіль має враховувати особливості цифрової реалізації. На відміну від традиційних апаратних систем, у цифрових ІКС функціональність може визначатися не тільки фізичною структурою компонентів, але й програмним кодом, конфігурацією FPGA, параметрами налаштування та взаємодією між програмними й апаратними

засобами. Тому профіль вимог має охоплювати як фізичні та проєктні відмови апаратних засобів, так і дефекти програмної й конфігураційної частини.

Вихідним рівнем профілю є вимоги до функцій безпеки. Для кожної функції безпеки повинні бути визначені її призначення, умови активації, необхідна реакція системи, допустимий час реакції, наслідки невиконання та необхідний рівень функційної безпечності. Функції безпеки є первинним об’єктом, від якого повинні виводитися вимоги до окремих систем, підсистем і компонентів. Відповідно, профіль вимог доцільно формувати за принципом послідовної декомпозиції: «цілі безпеки → функції безпеки → вимоги до ІКС → архітектура → компоненти → дефекти та відмови → показники функційної безпечності».

Така декомпозиція забезпечує простежуваність між вимогами верхнього та нижнього рівнів. Водночас вона є важливою для проведення FMECA/FMEDA, оскільки дозволяє встановити, які саме відмови компонентів можуть впливати на конкретну функцію безпеки.

1.1.3.1 Вимоги до функціональності та коректності виконання функцій безпеки

Першою групою профілю є функціональні вимоги. ІКС повинна реалізовувати визначений набір функцій відповідно до специфікації та забезпечувати їх коректне виконання як у нормальних умовах, так і при передбачених відмовах.

Для кожної функції повинні бути визначені:

– вхідні дані та допустимі діапазони їх значень;

– алгоритм оброблення інформації;

– вихідні сигнали та керуючі впливи;

– умови спрацювання функції;

– умови блокування або припинення функції;

– допустимий час реакції;

– безпечний стан системи у випадку відмови;

– вимоги до діагностування та контролю результатів.

Для програмовної платформи додатково необхідно забезпечити відповідність реалізованої логіки заданим функціональним вимогам. При цьому функціональна коректність не повинна ототожнюватися з функційною безпечністю. Програмна система може відповідати функціональній специфікації у штатних режимах, але не забезпечувати необхідної реакції при виникненні дефектів.

Тому вимоги до функцій безпеки повинні доповнюватися вимогами до реакції на відмови. Для кожної потенційної відмови необхідно визначити, чи повинна вона бути виявлена, локалізована, маскована, компенсована резервним каналом або призводити до переходу системи у визначений безпечний стан.

1.1.3.2 Вимоги до архітектури та резервування

Наступною групою є архітектурні вимоги. Для ІКС АЕС, що виконують функції, важливі для безпеки, архітектура повинна забезпечувати необхідний рівень незалежності, резервування та стійкості до відмов. У найпростішому випадку підвищення стійкості до одиничної відмови може забезпечуватися резервуванням. Однак просте дублювання компонентів не гарантує необхідного рівня безпечності, якщо існує спільна причина їхньої відмови.

Тому профіль вимог повинен містити вимоги щодо:

– кількості резервованих каналів;

– незалежності каналів;

– відсутності небажаних зв’язків між резервованими каналами;

– механізмів перемикання;

– діагностування каналів;

– оброблення конфліктних результатів;

– поведінки системи при відмові одного або декількох каналів;

– стійкості до відмов загальної причини.

Звідси випливає вимога до профілю: під час оцінювання багатоканальної або багатоверсійної ІКС необхідно враховувати не тільки незалежні відмови окремих компонентів, а й можливі множинні дефекти та відмови, що впливають на декілька каналів.

1.1.3.3 Вимоги до апаратної частини програмовної платформи

Окрему групу становлять вимоги до апаратних компонентів. Незважаючи на програмованість FPGA, їх функціонування залежить від фізичних електронних компонентів, тактових генераторів, пам’яті, джерел живлення, інтерфейсів, комунікаційних засобів та інших апаратних елементів.

Тому профіль повинен враховувати:

– фізичні дефекти компонентів;

– проєктні дефекти апаратури;

– відмови живлення;

– відмови тактування;

– відмови пам’яті;

– відмови комунікаційних інтерфейсів;

– відмови засобів введення та виведення;

– відмови діагностичних засобів;

– відмови резервованих компонентів;

– можливість одночасної відмови декількох апаратних компонентів.

При формуванні FMECA/FMEDA необхідно забезпечити відповідність множини компонентів, включених до аналізу, фактичній структурі системи. Неврахування частини компонентів може призвести до неповного визначення множини можливих відмов та, відповідно, до завищення оцінки функційної безпечності.

1.1.3.4 Вимоги до програмної та конфігураційної частини

Для систем на програмовній логіці суттєве значення мають вимоги до програмного забезпечення та конфігураційних даних. До потенційних джерел небезпечних дефектів належать помилки алгоритмів, неправильні параметри, помилки конфігурації, некоректне оброблення граничних значень, помилки синхронізації та взаємодії програмних компонентів.

Для FPGA додатково необхідно враховувати конфігураційну логіку, яка визначає реалізовану апаратну функціональність. У такому випадку межа між апаратним та програмним забезпеченням є менш однозначною, ніж у класичній комп'ютерній системі. Тому профіль вимог повинен передбачати:

– простежуваність між функціональними вимогами та реалізацією;

– контроль конфігурації;

– верифікацію логічної функціональності;

– валідацію виконання функцій безпеки;

– контроль змін;

– перевірку програмних і конфігураційних компонентів;

– аналіз можливих програмних та конфігураційних дефектів.

Відповідно, під час FMECA/FMEDA до множини потенційних дефектів повинні включатися не тільки фізичні відмови компонентів, але й систематичні та програмні дефекти, якщо вони можуть впливати на функцію безпеки.

1.1.3.5 Вимоги до діагностування

Наступною складовою профілю є діагностованість. Для safety-critical ІКС важливим є не тільки запобігання відмовам, але й своєчасне їх виявлення. У випадку FMEDA для кожного виду відмови доцільно визначати можливість його виявлення діагностичними засобами. Формалізація FMEDA-таблиці містить елемент системи, множину видів відмов, множину наслідків, діагностованість та критичність відмови.

Звідси профіль вимог повинен містити:

– перелік контрольованих параметрів;

– засоби виявлення дефектів;

– умови формування діагностичного сигналу;

– допустимий час виявлення;

– вимоги до локалізації дефекту;

– вимоги до реакції системи після виявлення дефекту;

– вимоги до діагностичного покриття.

При цьому неправильне припущення про діагностованість відмови може безпосередньо впливати на результат оцінювання. Якщо небезпечна відмова помилково вважається виявленою, рівень безпечності буде завищено. Навпаки, якщо виявлену відмову помилково вважають невиявленою, оцінка буде заниженою.

1.1.3.6 Вимоги до множинних дефектів

Традиційний аналіз видів і наслідків відмов орієнтується на аналіз одиничних відмов. Однак для резервованих і багатоверсійних цифрових ІКС цього недостатньо. Профіль вимог повинен передбачати можливість аналізу:

– одиничних дефектів;

– множинних дефектів одного компонента;

– дефектів різних компонентів одного рівня;

– дефектів різних рівнів системи;

– одночасних дефектів резервованих каналів;

– дефектів різних версій програмовної платформи;

– комбінацій апаратних та програмних дефектів.

Особливо важливим є аналіз дефектів різних версій. Якщо багатоверсійна ІКС використовується для зниження ризику систематичних відмов, необхідно визначити, які дефекти є спільними для версій, а які – специфічними для окремої версії.

1.1.3.7 Вимоги до міжрівневої взаємодії

ІКС має ієрархічну структуру. Відмова компонента нижчого рівня може проявлятися як відмова компонента вищого рівня, а взаємодія між рівнями може створювати додаткові комбінації дефектів.

Тому профіль вимог повинен враховувати:

– структуру рівнів ІКС;

– зв’язки між рівнями;

– передачу інформації між рівнями;

– залежність функцій вищого рівня від компонентів нижчого рівня;

– можливість поширення наслідків відмови між рівнями;

– можливість множинних дефектів на різних рівнях.

Неповний аналіз ієрархічної структури може призвести до того, що наслідок відмови буде оцінено тільки локально, без врахування його системного ефекту. Саме тому під час формування FMECA-моделі необхідно встановлювати не тільки склад компонентів, а й рівень, на якому розглядається кожний компонент та його відмова.

1.1.3.7 Вимоги до комунікацій

Для сучасних цифрових ІКС важливими є вимоги до комунікаційних засобів. Комунікаційна відмова може проявлятися як втрата інформації, затримка, дублювання, спотворення або неправильна адресація даних. Тому профіль вимог повинен включати:

– достовірність передачі інформації;

– контроль помилок;

– допустимі затримки;

– поведінку при втраті зв’язку;

– діагностування комунікаційних каналів;

– незалежність резервованих комунікацій;

– стійкість до відмов комунікаційної інфраструктури.

Таким чином, комунікаційні компоненти не повинні автоматично виключатися з FMECA як «допоміжні». Якщо їхня відмова може призвести до втрати функції безпеки, вони повинні бути включені до відповідної моделі.

1.1.3.8 Вимоги до безпеки інформації

Цифровізація ІКС призводить до необхідності одночасного врахування функційної та інформаційної безпечності. Порушення цілісності або доступності інформації може призвести до порушення функційної безпечності, якщо змінені або недоступні дані використовуються для формування керуючого рішення.

Отже, профіль вимог повинен передбачати:

– захист конфігураційних даних;

– контроль цілісності програмного забезпечення;

– контроль доступу до критичних функцій;

– захист каналів передавання критичної інформації;

– контроль несанкціонованих змін;

– можливість виявлення порушень цілісності;

– аналіз впливу подій інформаційної безпечності на функції безпеки.

При цьому інформаційна безпечність не замінює функційну безпечність. Вона повинна розглядатися як додаткова характеристика цифрової ІКС, потенційні порушення якої повинні оцінюватися з погляду їхнього впливу на функції безпеки.

1.1.3.9 Вимоги до верифікації, валідації та випробувань

Профіль вимог повинен містити вимоги до перевірки відповідності системи встановленим характеристикам. Для програмовної платформи доцільно виділяти:

– верифікацію вимог;

– верифікацію архітектури;

– перевірку програмного та конфігураційного коду;

– функціональне тестування;

– аналіз відмов;

– fault injection testing;

– валідацію функцій безпеки;

– перевірку діагностичного покриття.

Це дозволяє пов’язати аналітичне FMECA/FMEDA з експериментальним FIT. Результати FMECA можуть визначати множину критичних дефектів, які доцільно перевірити за допомогою засіва дефектів, а результати FIT можуть використовуватися для підтвердження або уточнення аналітичної моделі.

1.1.3.10 Вимоги до оцінювання та повноти аналізу

Однією з ключових груп профілю є вимоги до самого процесу оцінювання функційної безпечності. Традиційна процедура FMECA/FMEDA передбачає послідовне визначення елементів, які враховуються в аналізі, можливих видів їхніх відмов, наслідків, імовірностей, тяжкості та критичності. Експерт під час виконання FMECA/FMEDA фактично визначає підмножину компонентів, підмножину видів відмов, підмножину наслідків, а також оцінки імовірності, тяжкості та критичності.

Це означає, що результат аналізу залежить не тільки від властивостей самої системи, але й від повноти сформованої експертом моделі.

Зокрема, можливими є такі критичні припущення:

– не всі компоненти системи включені до аналізу;

– включено надлишкові компоненти;

– не всі види відмов враховані;

– враховано надлишкові види відмов;

– недооцінено або переоцінено критичність відмов;

– відмова помилково вважається діагностованою;

– відмова помилково вважається недіагностованою;

– недооцінено або переоцінено множинність відмов;

– не враховано відмови на окремих рівнях системи;

– не враховано взаємодію між рівнями;

– не враховано множинні відмови різних версій;

– не враховано окремі програмні дефекти;

– не враховано окремі апаратні дефекти;

– не враховано взаємодію апаратних і програмних дефектів.

Таким чином, до профілю вимог повинна входити не тільки вимога отримати певне числове значення показника безпечності, а й вимога забезпечити повноту та обґрунтованість самої процедури оцінювання.

1.1.3.11 Вимоги до зменшення залежності від експертних припущень

Особливістю FMECA/FMEDA є значна кількість операцій, що можуть виконуватися експертом. Розгляд експертних припущень як окремого об’єкту аналізу формує підґрунтя для переходу від традиційного FMECA до розширеного аналізу, в якому враховуються не тільки види відмов, а й припущення, на яких ґрунтується побудова таблиці.

Це положення має бути включене до профілю вимог у вигляді вимоги до простежуваності припущень. Для кожного суттєвого припущення бажано визначати: його зміст; джерело; обґрунтування; область застосування; можливий вплив на результат; напрямок потенційної похибки; можливість перевірки припущення; необхідність експертного підтвердження.

1.1.3.12 Узагальнений профіль вимог

На основі проведеного аналізу профіль вимог до ІКС ППЛ АЕС може бути представлений сукупністю взаємопов’язаних груп.

Таблиця 1.1 – Узагальнений профіль вимог

Група	**Основні вимоги**
Функційні	Реалізація визначених функцій безпеки, коректність алгоритмів, допустимий час реакції
Архітектурні	Резервування, незалежність, диверсність, стійкість до CCF
Апаратні	Врахування фізичних та проєктних відмов компонентів
Програмні	Контроль програмних, конфігураційних та систематичних дефектів
Діагностичні	Виявлення, локалізація та оброблення небезпечних відмов
Множинні відмови	Аналіз одиничних і множинних дефектів та їх комбінацій
Багатоверсійні	Аналіз абсолютних і відносних дефектів різних версій
Ієрархічні	Врахування рівнів ІКС та взаємодії між ними
Комунікаційні	Врахування відмов та залежностей комунікацій
Security	Захист цілісності, конфігурації та критичної інформації
V&V	Верифікація, валідація та засів дефектів
FMECA/FMEDA	Повнота множини компонентів, відмов, наслідків та діагностичних характеристик
Експертні	Контроль експертних припущень, оцінок та можливих помилок
Простежуваність	Зв’язок «вимога – функція – компонент – відмова – наслідок – показник»
Повнота оцінювання	Контроль пропущених компонентів, відмов, рівнів та комбінацій дефектів

Сформований профіль можна представити також у вигляді багаторівневої моделі вимог. На першому рівні розташовуються цілі безпеки об’єкта. На другому – функції безпеки, які забезпечують досягнення цих цілей. На третьому – вимоги до ІКС, що реалізує функції безпеки. На четвертому – вимоги до архітектури та ППЛ. На п’ятому – вимоги до окремих апаратних,

програмних і конфігураційних компонентів. На шостому – вимоги до аналізу дефектів та відмов. На сьомому – показники, за якими визначається відповідність системи вимогам функційної безпечності.

Така структура дозволяє встановити відповідність між нормативними вимогами та процедурами оцінювання. Наприклад, вимога щодо стійкості до одиничної відмови повинна бути відображена в архітектурі резервування, а потім перевірена шляхом аналізу відповідних видів відмов. Вимога щодо діагностування повинна бути відображена в архітектурі діагностичних засобів та перевірена в рамках FMEDA і FIT. Вимога щодо диверсності повинна бути відображена в архітектурі диверсних версій та перевірена шляхом аналізу спільних і специфічних дефектів.

Важливим результатом формування профілю є визначення вимог до повноти моделі FMECA/FMEDA. Якщо профіль вимагає врахування всіх компонентів, що можуть впливати на функцію безпеки, то множина компонентів FMECA повинна відповідати відповідній множині системних компонентів. Якщо профіль вимагає аналізу множинних відмов, таблиця FMECA повинна забезпечувати можливість представлення таких комбінацій. Якщо профіль вимагає врахування багатоверсійної реалізації, модель повинна розрізняти абсолютні та відносні дефекти версій.

Таким чином, профіль вимог визначає не тільки те, якою повинна бути ІКС, але й те, що саме повинно бути перевірено під час оцінювання її функційної безпечності.

1.1.3.13 Вимоги до показників оцінювання

Останнім елементом профілю є вимоги до показників функційної безпечності. Показники повинні дозволяти встановити, чи відповідає система визначеним вимогам, а також оцінити вплив окремих дефектів і їх комбінацій.

Для FMECA доцільно враховувати щонайменше:

– імовірність відмови;

– тяжкість наслідків;

– критичність відмови;

– кількість врахованих видів відмов;

– кількість неврахованих або невизначених відмов.

Для FMEDA додатково необхідно враховувати:

– діагностованість;

– частку небезпечних виявлених відмов;

– частку небезпечних невиявлених відмов;

– вплив діагностичного покриття на функцію безпеки.

Для розширеного FMECA/XMECA необхідно додатково враховувати:

– кількість критичних припущень;

– критичність припущень;

– кількість потенційних помилок аналізу;

– повноту множини компонентів;

– повноту множини видів відмов;

– повноту множини наслідків;

– повноту врахування множинних дефектів;

– повноту врахування різних рівнів системи;

– повноту врахування взаємодії між рівнями;

– повноту врахування програмних та апаратних дефектів.

У такому вигляді профіль вимог безпосередньо пов’язується із подальшим формуванням показників повноти оцінювання.

1.1.3.14 Вимоги до процесу оцінювання

Узагальнюючи сформований профіль, процес оцінювання функційної безпечності ІКС ППЛ АЕС повинен передбачати такі основні етапи:

- визначення цілей та функцій безпеки;
- декомпозицію функцій до рівня ІКС, підсистем та компонентів;
- формування архітектурної моделі системи;

– визначення апаратних, програмних та конфігураційних компонентів;
– визначення множини потенційних одиничних і множинних дефектів;
– визначення наслідків дефектів на різних рівнях системи;
– оцінювання імовірності, тяжкості та критичності відмов;
– визначення діагностованості відмов;
– аналіз резервування, диверсності та можливих відмов загальної причини;
– проведення FMECA/FMEDA;
– визначення критичних припущень та потенційних помилок аналізу;
– перевірку критичних результатів за допомогою FIT;
– формування підсумкових показників функційної безпечності;
– оцінювання повноти сформованої моделі;
– формування висновку щодо відповідності встановленим вимогам.

Особливістю запропонованого підходу є те, що контроль повноти повинен виконуватися не тільки після завершення FMECA/FMEDA, а й на етапі формування вихідної моделі. Це дозволяє виявити ситуації, коли небезпечний результат отримано не через математичну помилку, а через те, що певний компонент, вид відмови або комбінація дефектів взагалі не потрапили до моделі.

1.1.3.15 Висновок щодо сформованого профілю

Таким чином, на основі аналізу вимог до функційної безпечності та нормативної бази сформовано профіль вимог до ІКС АЕС на програмовній логіці, який охоплює функційні, архітектурні, апаратні, програмні, діагностичні, комунікаційні, безпекові та експлуатаційні характеристики, а також вимоги до верифікації, валідації та оцінювання.

Особливістю сформованого профілю є включення вимог до повноти моделі оцінювання. Поряд із традиційним врахуванням одиничних відмов необхідно забезпечити можливість аналізу множинних дефектів, взаємодії між

рівнями, апаратних і програмних дефектів, а для багатоверсійних систем – абсолютних та відносних дефектів різних версій.

Важливим є також врахування залежності результату оцінювання від експертних припущень. Оскільки експерт під час FMECA/FMEDA визначає склад аналізованих компонентів, множину видів відмов, наслідки, імовірність, тяжкість та критичність, припущення експерта фактично є складовою математичної моделі оцінювання. Тому вони повинні розглядатися як окремий об’єкт контролю та аналізу.

Сформований профіль вимог дозволяє визначити основні характеристики методів оцінювання, які повинні бути проаналізовані в наступному підрозділі. Зокрема, метод повинен забезпечувати можливість систематичного представлення компонентів, видів відмов та їх наслідків; враховувати діагностованість; підтримувати аналіз одиничних і множинних дефектів; забезпечувати врахування апаратних та програмних дефектів; дозволяти аналізувати багаторівневі та багатоверсійні структури; а також забезпечувати контроль критичних припущень і повноти оцінювання.

Отже, сформований профіль вимог є зв’язувальною ланкою між нормативними вимогами до функційної безпечності ІКС АЕС та методами їх практичного оцінювання.

1.2. Аналіз методів і засобів оцінювання функційної безпечності ІКС

Функційна безпечність інформаційно-керуючих систем, що застосовуються у критичних до безпеки галузях, визначається не тільки властивостями архітектури та технічних засобів, а й здатністю обґрунтовано підтвердити виконання встановлених вимог. Тому одним із ключових етапів життєвого циклу ІКС є оцінювання функційної безпечності, метою якого є визначення можливості системи виконувати задані функції у встановлених умовах та забезпечувати прийнятний рівень ризику при виникненні передбачених відмов і дефектів.

Проведений у підрозділі 1.1 аналіз вимог до функційної безпечності показав, що для ІКС на програмовних платформах необхідно враховувати широкий спектр потенційних дефектів: фізичні та проєктні дефекти апаратури, дефекти програмного забезпечення, конфігураційні помилки, дефекти комунікацій, відмови діагностичних засобів, а також множинні дефекти та їх комбінації. Для резервованих і багатоверсійних систем додатково виникає необхідність аналізу спільних та специфічних дефектів різних версій.

У зв’язку з цим метод оцінювання повинен забезпечувати не тільки визначення окремих видів відмов, а й можливість встановлення їхнього впливу на функції системи, визначення наслідків, оцінювання імовірності та тяжкості, аналіз діагностованості, а також встановлення відповідності отриманих показників заданим критеріям безпечності.

У сучасній практиці застосовується сукупність аналітичних, експериментальних, експертних і комбінованих методів оцінювання. Серед них особливе місце посідають аналіз видів і наслідків відмов та їх критичності FMECA (Failure Modes, Effects and Criticality Analysis), аналіз видів, наслідків і діагностування відмов FMEDA (Failure Modes, Effects and Diagnostic Analysis), аналіз дерев відмов FTA (Fault Tree Analysis), марковські моделі, аналіз надійності структурних схем, аналіз подій та методи ін’єктування дефектів FIT (Fault Injection Testing).

Для ІКС на програмовних платформах особливого значення набуває комплексування аналітичних та експериментальних методів. FMECA/FMEDA дозволяє систематично сформувати модель потенційних відмов і їх наслідків, тоді як FIT забезпечує можливість експериментальної перевірки реакції системи на штучно введені дефекти. Саме тому подальший аналіз зосереджено на FMECA/FMEDA та FIT як основних методах, що можуть бути комплексно використані для оцінювання функційної безпечності ІКС на програмовних платформах. На рис.1.1 структуровано основні обмеження та пов’язані методики XMECA.

1.2.1. Класифікація методів

Класифікуємо методи оцінювання функційної безпечності ІКС за ознаками: способом отримання інформації, характером моделі, що використовується, ступенем формалізації, способом урахування відмов та видом результату, що отримується. З урахуванням особливостей критичних ІКС доцільно виділити аналітичні, експериментальні, експертні та комбіновані методи.

Рисунок 1.1 – Основні обмеження та пов’язані методики XMECA

Аналітичні методи ґрунтуються на побудові математичної або логічної моделі системи та визначенні характеристик її безпечності на основі цієї моделі. До них належать FMEA/FMECA, FMEDA, FTA, ETA, марковський аналіз, аналіз структурних схем надійності та інші методи. Методи FMEA та FMECA належать до методів, орієнтованих на аналіз відмов «знизу вгору». Початковим об’єктом аналізу є окремий компонент, функціональний блок або елемент системи. Для нього визначаються можливі види відмов, причини їх виникнення, локальні та системні наслідки, імовірність та інші характеристики. На відміну від FMEA, FMECA додатково передбачає оцінювання критичності

відмов. Перевагою такого підходу є можливість систематично проаналізувати структуру системи та встановити зв’язок між відмовою конкретного елемента і наслідками для функції, що ним забезпечується. Водночас результат залежить від повноти множини елементів і видів відмов, які включено до аналізу.

Метод FMEDA є розвитком FMEA/FMECA, орієнтованим на safety-critical системи, для яких суттєве значення має можливість виявлення небезпечних відмов. У цьому випадку аналіз доповнюється класифікацією відмов за ознаками їхньої безпечності та діагностованості. Це дозволяє визначити частку небезпечних відмов, які можуть залишитися невиявленими, і відповідно оцінити вплив діагностичного покриття на функційну безпечність.

До аналітичних методів також належить FTA. На відміну від FMECA, яка зазвичай починається з компонентів і рухається до наслідків, FTA є методом аналізу «згори вниз». Вихідною точкою є небажана подія або небезпечний стан системи, після чого визначаються комбінації подій, здатних призвести до її виникнення. FTA є ефективним для дослідження логічних комбінацій відмов, особливо у резервованих системах.

Марковський аналіз дозволяє враховувати переходи системи між станами, зокрема нормальним станом, станами часткової відмови, діагностованої або недіагностованої відмови та відновлення. Такий підхід є особливо корисним для систем, поведінка яких залежить від послідовності подій у часі. Недоліком є необхідність формування відповідної моделі станів та визначення параметрів переходів.

Експериментальні методи передбачають безпосередню перевірку поведінки системи або її компонентів. Одним із найбільш поширених підходів для критичних цифрових систем є fault injection або fault insertion testing. Сутність методу полягає у штучному введенні заданих дефектів або відмов та спостереженні за реакцією системи.

На відміну від аналітичних методів, експериментальний підхід дозволяє перевірити фактичну поведінку реалізованої системи. Це особливо важливо для

програмовних платформ, оскільки поведінка реальної реалізації може відрізнятися від поведінки ідеалізованої математичної моделі.

Окрему групу становлять експертні методи. Їх використання зумовлене тим, що для багатьох критичних систем відсутні повні статистичні дані щодо відмов, а побудова повної формальної моделі є складною. У такій ситуації експерт визначає множину компонентів, видів відмов, наслідків, імовірностей, тяжкостей та інших характеристик.

Експертне оцінювання може використовуватися як самостійний метод або як складова аналітичних методів. Саме такий характер має використання експертів у FMECA/FMEDA, експертні судження розглядаються як складова комплексного процесу оцінювання. Комбіновані методи поєднують переваги різних підходів. Для досліджуваного класу ІКС найбільш перспективним є поєднання FMECA/FMEDA та FIT. Аналітичний метод дозволяє сформувати множину потенційних дефектів і визначити критичні випадки, а FIT – перевірити реакцію системи на вибрані дефекти.

Комплексування FMECA/FMEDA та FIT також дозволяє зменшити ризик того, що висновок про безпечність буде зроблений виключно на основі експертного припущення. Якщо певний вид відмови в аналітичній моделі вважається виявленим, експериментальне ін’єктування відповідного дефекту дозволяє перевірити фактичну реакцію діагностичних засобів.

Таким чином, методи оцінювання функційної безпечності можна представити у вигляді чотирьох основних груп:

1) аналітичні методи – FMEA/FMECA, FMEDA, FTA, ETA, марковський аналіз та інші;

2) експериментальні методи – засів дефектів FIT;

3) експертні методи – формування та оцінювання експертних суджень;

4) комбіновані методи – комплексування аналітичних, експертних та експериментальних процедур.

Для ІКС на програмовних платформах найбільш доцільним є комбінований підхід, у якому FMECA/FMEDA використовується для

систематизації дефектів і їх наслідків, експертні процедури – для отримання інформації, яку неможливо або недоцільно визначити формально, а FIT – для експериментальної перевірки критичних випадків.

Цей висновок визначає подальшу структуру аналізу: спочатку розглядаються особливості FMECA/FMEDA, потім FIT, а після цього – інструментальні засоби, що забезпечують реалізацію відповідних процедур.

Результати аналізу ключових результатів досліджень за темою дисертації представлено рис. 1.2.

Рисунок 1.2 – Результати аналізу ключових результатів досліджень

Дане дослідження продовжує декілька напрямів, які розвивалися у науковій школі ХАІ та в практичних розробках НВП «Радій» і з урахуванням багаторічного індустріального досвіду. До уваги було взято:

– перший напрям – це assurance case та аналітичні методи [1-4, 12, 13]: FMECA, FIT, FTA та їх модифікації для різних типів ІКС. Цей напрям формує методологічну базу для структурованого доведення безпечності;

– другий напрям – комплексування та автоматизація оцінювання [15, 17-19]. Йдеться про зменшення впливу суб’єктивних експертних рішень, нормування вимог і створення процедур, які можна відтворити і перевірити;

– третій напрям – багатоверсійні системи [5, 8, 9, 14]. Для ІКС АЕС це особливо важливо, оскільки диверсність є одним із практичних механізмів зниження ризику відмов за загальною причиною;

– четвертий напрям – оцінювання готовності та безпечності з використанням байєсівських методів, марковських моделей, імітаційного моделювання та інших підходів [5, 16].

Ці та інші напрями досліджуються для різних предметних галузей, пов’язаних з оцінюванням та забезпеченням функційної безпечності та кібербезпеки ІКС на базі програмовних і процесорних технологій [29-90], зокрема:

– методи отримання та агрегування експертних оцінок, практичне застосування експертного аналізу в атомній енергетиці та інженерії безпеки [29-35];

– методи оцінювання ризику та надійності за умов невизначеності [36, 37];

– підвищенні надійності та безпеки критичних систем шляхом використання принципу диверсності [39-42];

– підходи до аналізу видів і наслідків відмов (FMEA/FMEDA) [43-44];

– методи аналізу та оцінювання функціональної безпечності ІКС, ризик-орієнтовані підходи до розроблення ІКС [45, 47,48,53-55, 66-68, 70];

– інтеграція функційної безпечності (safety) та кібербезпеки (security) з побудовою інтегрованих моделей ризику, що враховують як випадкові відмови, так і навмисні кібератаки [46, 51, 52, 61, 62, 64, 65, 69, 71];

– формальні методи верифікації та моделювання безпеки, моделювання впливу кібератак на ІКС [72-75].

– забезпечення безпеки та надійності ІКС для атомної енергетики [57-60, 88];

– використання FPGA-технологій у системах з підвищеними вимогами до безпеки та надійності [63, 76-86];

– методи аналізу та забезпечення функціональної безпеки сучасних транспортних засобів, робототехнічних систем та автономного транспорту [48-50, 52, 55, 80, 81, 86];

– моделювання надійності складних технічних систем [87, 89, 90];

– забезпеченні безпеки цифровізованих виробничих середовищ та критичної інфраструктури [47, 56, 65, 73, 75].

Далі ці методи аналзіюються більш детально в контексті задач досліджень.

1.2.2. Аналіз методу аналізу видів і наслідків відмов FMECA (FMEDA)

Методи FMEA та FMECA призначені для систематичного аналізу можливих відмов системи, визначення їх причин і наслідків та оцінювання їхньої критичності. Для ІКС, що виконують функції, важливі для безпеки, цей підхід є одним із базових способів обґрунтування того, що потенційні відмови були ідентифіковані та їхній вплив на функції системи оцінено.

У загальному випадку FMECA виконується для множини елементів системи. Для кожного елемента визначається множина можливих видів відмов, а для кожного виду відмови – відповідні наслідки. Далі оцінюються імовірність виникнення відмови та тяжкість її наслідків, після чого визначається критичність. Основною перевагою FMECA є систематичність. На відміну від довільного опису можливих проблем системи, таблиця забезпечує структурований опис причинно-наслідкових зв’язків. Це створює можливість простежити шлях від конкретного елемента до наслідку його відмови та далі до оцінки критичності. Разом з тим FMECA має принципове обмеження: таблиця сама по собі не визначає, які саме елементи, види відмов та наслідки необхідно включити. Ці множини формуються під час аналізу.

Для традиційної апаратної системи експерт визначає елементи, відмови яких повинні враховуватися, види відмов кожного елемента, відповідні

наслідки, імовірність, тяжкість та критичність. Для ІКС на програмовній платформі множина елементів є суттєво складнішою, оскільки крім фізичних компонентів можуть аналізуватися функціональні блоки, логічні елементи, оператори програми, операції процесів та інші об’єкти.

Експерт послідовно визначає підмножину компонентів, види відмов, наслідки, а також значення імовірності, тяжкості та критичності. Це дозволяє зробити важливий висновок: результат FMECA залежить не тільки від властивостей ІКС, але й від того, яку модель цієї системи сформував експерт.

Для програмовних платформ ця проблема посилюється через необхідність одночасного врахування апаратних і програмних дефектів. Апаратний компонент може мати фізичну або проєктну відмову, тоді як програмний компонент може мати логічний дефект, помилку алгоритму або помилку конфігурації. Крім того, відмова апаратного компонента може змінювати поведінку програмного компонента, а програмний дефект може маскувати або посилювати наслідки апаратної відмови.

Тому для ІКС ППЛ традиційна модель FMECA повинна бути розширена з урахуванням специфіки цифрової реалізації. Особливого значення набуває аналіз множинних відмов. Для одиничної відмови можна встановити локальний та системний наслідок, однак у резервованій системі одночасне виникнення декількох дефектів може призвести до принципово іншого результату. Наприклад, одинична відмова одного каналу резервованої системи може бути безпечною, оскільки другий канал продовжує виконувати функцію. Якщо ж одночасно виникають дефекти двох каналів, система може втратити здатність виконувати функцію безпеки. Для багатоверсійних систем необхідно додатково визначати, чи є дефекти незалежними, чи мають спільну причину.

Застосування диверсності змінює характер FMECA. Для двох диверсних каналів необхідно визначати не тільки індивідуальні дефекти, а й можливість їх спільного прояву. Якщо два канали мають різну реалізацію, частина дефектів може бути абсолютною, тобто властивою конкретній версії, а частина – відносною, тобто такою, що може проявлятися у декількох версіях.

Ще однією важливою характеристикою є діагностованість. У звичайній FMECA відмова може бути оцінена переважно за імовірністю та тяжкістю. Для критичних до безпеки систем цього недостатньо, оскільки одна й та сама відмова може мати різний вплив залежно від можливості її своєчасного виявлення.

FMEDA доповнює FMECA аналізом діагностування. Для кожного виду відмови необхідно визначити, чи може вона бути виявлена засобами діагностики, а також яким є вплив невиявленої відмови на функцію безпеки. У спрощеному вигляді відмови можуть бути розподілені на: безпечні та небезпечні; виявлені та невиявлені.

Найбільш критичними є небезпечні невиявлені відмови, оскільки система не тільки втрачає необхідну властивість, але й не отримує своєчасної інформації про її втрату. Звідси випливає важлива вимога до FMEDA: оцінювання має враховувати не тільки множину потенційних відмов, а й засоби та можливості їх діагностування. Проте включення діагностованості також створює додаткове джерело експертних припущень. Експерт може помилково вважати певну відмову діагностованою, хоча відповідні засоби не забезпечують гарантованого виявлення. Тоді отримана оцінка безпечності буде завищеною. У даній роботі це виділено як окремий клас припущень: відмова може бути помилково вважатися виявленою або, навпаки, невиявленою, що відповідно призводить до завищення або заниження оцінки безпечності.

Таким чином, FMECA/FMEDA для ІКС ППЛ має враховувати щонайменше такі групи об’єктів:

– апаратні компоненти;

– програмні та конфігураційні компоненти;

– види фізичних і проєктних відмов;

– програмні дефекти;

– діагностичні засоби;

– одиничні та множинні дефекти;

– дефекти різних рівнів системи;

– дефекти різних версій;

– взаємодію апаратних і програмних дефектів.

Окрему проблему становить визначення повноти FMECA. Якщо певний компонент не включений до аналізу, потенційна відмова цього компонента не буде представлена в таблиці. Якщо не враховано певний вид відмови, його наслідок також не буде відображений. У результаті математично правильне оброблення неповної таблиці може призвести до неправильного висновку про безпечність.

Зазначені результати дають підстави розглядати традиційний FMECA як процес, у якому поряд із власне відмовами присутня друга група об’єктів – припущення та обмеження аналізу. До найбільш суттєвих припущень належать:

– врахування не всіх компонентів;

– включення надлишкових компонентів;

– неповний перелік видів відмов;

– надлишковий перелік видів відмов;

– недооцінювання або переоцінювання критичності;

– припущення щодо діагностованості;

– припущення щодо кількості одночасних відмов;

– неврахування множинних відмов різних компонентів;

– неврахування множинних відмов різних рівнів;

– неврахування відмов різних версій;

– неврахування окремих рівнів системи;

– неврахування взаємодії між рівнями;

– неповне врахування програмних дефектів;

– неповне врахування апаратних дефектів;

– неврахування взаємодії апаратних та програмних дефектів.

Отже, головним недоліком класичного FMECA/FMEDA у застосуванні до ІКС ППЛ є не відсутність математичного апарату для обчислення критичності, а залежність результату від повноти та коректності сформованої моделі.

Це визначає напрям подальшого дослідження: необхідно формалізувати множини компонентів, відмов і наслідків, визначити критичні припущення, оцінити їхній вплив та, за можливості, зменшити залежність результату від експертного формування таблиці.

Водночас FMECA/FMEDA є переважно аналітичним методом. Навіть повна та формально узгоджена таблиця не завжди може гарантувати, що реальна система поводитиметься відповідно до припущень моделі. Для перевірки цієї відповідності доцільно використовувати експериментальний метод ін’єктування дефектів.

1.2.3. Аналіз методу ін’єктування дефектів FIT

Ін’єктування дефектів FIT є експериментальним методом оцінювання поведінки системи при штучному введенні заданих дефектів або відмов. Основною метою FIT є перевірка реакції системи на дефект, який у реальній експлуатації може виникнути природним шляхом, але виникнення якого неможливо або недоцільно чекати для проведення випробування.

На відміну від FMECA/FMEDA, що ґрунтуються на аналітичному представленні системи, FIT безпосередньо перевіряє поведінку реалізованої системи. У результаті можна встановити, чи виявляється введений дефект, чи правильно функціонують діагностичні механізми, чи відбувається перехід у передбачений безпечний стан та чи зберігається необхідна функція при відмові окремого компонента. Загалом процедура FIT складається з етапів:

1) визначення об’єкта випробування;
2) формування множини дефектів;
3) вибір способу ін’єктування;
4) визначення очікуваної реакції;
5) введення дефекту;
6) спостереження за поведінкою системи;
7) фіксація результату;

8) порівняння фактичної та очікуваної реакцій;

9) формування висновку.

Об’єктом ін’єктування може бути апаратний компонент, логічний сигнал, програмна змінна, функціональний блок, канал комунікації, елемент пам’яті або інший компонент системи. Для програмовних платформ особливого значення набуває можливість програмної реалізації ін’єктування дефектів. Це дозволяє моделювати відмови без фізичного пошкодження обладнання та виконувати повторювані експерименти з контрольованими умовами.

Для ІКС основаних на FPGA FIT може застосовуватися на різних рівнях. На апаратному рівні можуть ін’єктуватися дефекти компонентів або сигналів, на рівні FPGA – дефекти логічних ресурсів, конфігурації або внутрішніх сигналів, а на програмному рівні – помилки обчислень, змінних або алгоритмічних операцій.

Однією з головних переваг FIT є можливість перевірки діагностичного покриття. Якщо FMECA/FMEDA передбачає, що певна відмова буде виявлена, FIT дозволяє перевірити це припущення експериментально. Наприклад, якщо в аналітичній моделі передбачається, що відмова каналу буде виявлена засобами порівняння резервованих каналів, під час FIT може бути введено відповідний дефект. За результатами спостерігається, чи формується діагностична ознака, чи система переходить у визначений стан та чи зберігається функція безпеки.

Тому FIT може розглядатися як засіб верифікації окремих припущень FMECA/FMEDA. Водночас FIT має суттєві обмеження. По-перше, фізично неможливо перевірити всі можливі комбінації дефектів для складної ІКС. Кількість можливих комбінацій швидко зростає зі збільшенням кількості компонентів та видів відмов. По-друге, результати FIT залежать від способу ін’єктування. Якщо механізм ін’єктування не відтворює реальну поведінку дефекту, результат випробування може не відповідати поведінці системи при реальній відмові. По-третє, експериментальне введення дефекту може бути обмежене вимогами безпеки та неможливістю порушення функціонування реальної системи. Тому частина випробувань повинна виконуватися на стендах,

прототипах, моделях або цифрових копіях системи. По-четверте, FIT не замінює аналітичний аналіз. Випробування дозволяє перевірити конкретний набір дефектів, але не доводить автоматично відсутність усіх інших небезпечних комбінацій.

Отже, FMECA/FMEDA та FIT мають взаємодоповнюючий характер. FMECA/FMEDA відповідає на питання «Які дефекти та відмови можуть виникнути і які наслідки вони мають?» FIT відповідає на питання «Як фактично поводиться система при введенні конкретного дефекту?» Їх комплексування дозволяє перейти від суто аналітичного до комбінованого оцінювання. Для цього результати FMECA/FMEDA використовуються для формування множини тестів FIT. Зокрема, першочергово до FIT доцільно включати:

– небезпечні відмови;

– небезпечні невиявлені відмови;

– відмови, критичність яких має найбільше значення;

– відмови, щодо яких існують суттєві експертні припущення;

– відмови, для яких необхідно перевірити діагностованість;

– множинні відмови резервованих каналів;

– відмови, пов’язані з взаємодією апаратних і програмних компонентів.

Особливо перспективним є використання FIT для перевірки критичних припущень FMECA/FMEDA. Наприклад, якщо в процесі аналізу експерт вважає, що певний вид відмови є безпечним або гарантовано діагностується, відповідний тест може підтвердити або спростувати це припущення.

Таким чином, FIT може використовуватися не тільки як окремий метод випробування, а й як механізм зменшення невизначеності аналітичної моделі.

Для багатоверсійних ІКС додатково виникає задача ін’єктування множинних дефектів у декілька версій. Якщо метою диверсності є зниження ризику відмови за загальною причиною, FIT повинен дозволяти перевіряти не тільки кожну версію окремо, а й можливі комбінації дефектів різних версій.

Важливою є також проблема відтворюваності. Результат FIT повинен містити не тільки факт «тест пройдено/не пройдено», а інформацію про:

– тип ін’єктованого дефекту;

– місце його ін’єктування;

– умови випробування;

– очікувану реакцію;

– фактичну реакцію;

– час виявлення;

– стан системи після виявлення;

– можливість відновлення;

– вплив на функцію безпеки.

Це дозволяє використовувати результати FIT для подальшого аналізу та порівняння з FMECA/FMEDA.

Отже, FIT є ефективним засобом експериментальної перевірки функційної безпечності, але його самостійне використання не забезпечує повноти оцінювання. Найбільш доцільним є його застосування в комплексі з FMECA/FMEDA, коли аналітична модель визначає область потенційно критичних дефектів, а FIT забезпечує експериментальну перевірку найбільш суттєвих випадків.

1.2.4. Аналіз інструментальних засобів для FMECA і FIT

Практичне застосування FMECA/FMEDA та FIT для складних цифрових ІКС потребує використання програмних і програмно-апаратних засобів. Обсяг інформації, що опрацьовується під час аналізу, швидко зростає зі збільшенням кількості компонентів, видів відмов, наслідків та комбінацій дефектів.

Для традиційного FMECA результат може бути представлений у вигляді таблиці, однак для складних ІКС цього недостатньо. Необхідно забезпечити взаємозв’язок між елементами системи, видами відмов, наслідками, оцінками, діагностичними механізмами та результатами випробувань. До основних функцій інструментального засобу FMECA/FMEDA доцільно віднести:

– формування структури системи;

– визначення множини компонентів;

– формування множини видів відмов;

– визначення наслідків;

– введення імовірностей;

– введення тяжкостей;

– визначення критичності;

– визначення діагностованості;

– класифікацію відмов;

– формування FMECA/FMEDA-таблиці;

– пошук пропущених елементів;

– аналіз множинних дефектів;

– формування звітів;

– збереження історії змін.

Для програмовних платформ додатково необхідно забезпечити можливість розділення апаратних і програмних компонентів та представлення взаємозв’язків між ними.

Однією з проблем автоматизації FMECA є те, що програмний засіб може автоматично обробляти лише ту інформацію, яка була включена до моделі. Якщо експерт не визначив певний компонент або вид відмови, програмна система не зможе автоматично виправити таке пропущення без наявності додаткової моделі повноти. Тому перспективним напрямом є не просто автоматизація заповнення таблиці, а автоматизація контролю припущень та повноти аналізу. Інструментальний засіб повинен не тільки фіксувати експертну оцінку, а й забезпечувати можливість її аналізу.

Зокрема, доцільно автоматично визначати:

– компоненти, які не були оцінені;

– компоненти з недостатньою кількістю видів відмов;

– відмови без визначених наслідків;

– відмови без оцінки імовірності;

– відмови без оцінки тяжкості;

– небезпечні невиявлені відмови;

– відмови з високою критичністю;

– невизначені або суперечливі експертні оцінки;

– комбінації потенційно критичних дефектів.

Для FIT інструментальні засоби повинні забезпечувати іншу групу функцій. Насамперед це формування сценаріїв випробування, керування введенням дефектів, реєстрація реакції ІКС та порівняння фактичного результату з очікуваним. Залежно від рівня ін’єктування використовуються:

– програмні засоби симуляції;

– засоби ін’єктування дефектів у програмному середовищі;

– апаратні засоби введення сигналів;

– засоби моніторингу та реєстрації;

– засоби автоматичного формування звітів.

Особливе значення для основаних на FPGA ІКС мають засоби, які дозволяють працювати з апаратною логікою та програмною частиною одночасно. Це пов’язано з тим, що FPGA-платформа поєднує конфігуровану апаратну логіку, пам’ять, інтерфейси та програмні компоненти.

Для комплексного оцінювання необхідна інтеграція інструментальних засобів FMECA та FIT. Така інтеграція може бути організована через спільну базу дефектів, у якій кожний вид відмови має відповідний ідентифікатор, опис, очікувані наслідки та, за необхідності, сценарій FIT.

Ще однією важливою вимогою є підтримка експертного оцінювання. З огляду на те, що FMECA/FMEDA містить операції, які не завжди можуть бути автоматизовані, інструментальний засіб повинен забезпечувати введення експертних суджень, їх зберігання, порівняння та узгодження. Отже, інструментальний засіб повинен підтримувати не тільки одиничну експертну оцінку, а й роботу групи експертів. Для цього необхідні засоби:

– формування опитувальників;

– незалежного введення оцінок;

– порівняння суджень;

– виявлення розходжень;

– формування узгодженої оцінки;

– зберігання вихідних суджень;

– контролю сценарію узгодження;

– формування підсумкового висновку.

Автоматизація особливо важлива при аналізі множинних дефектів. Повний перебір усіх комбінацій може бути обчислювально складним, тому необхідно застосовувати критерії відбору критичних комбінацій.

Для багатоверсійних систем інструментальний засіб повинен додатково підтримувати ідентифікацію версії та типу дефекту. Це дозволяє розділяти абсолютні дефекти конкретної версії та дефекти, які можуть бути спільними для декількох версій. Водночас автоматизація не повинна розглядатися як повна заміна експерта. Навпаки, доцільно автоматизувати формалізовані операції, перевірку повноти, пошук розходжень, формування звітів, залишаючи експерту операції, де необхідні спеціалізовані знання про ІКС. Такий підхід дозволяє зменшити кількість експертних операцій і водночас зробити результати більш відтворюваними.

Проведений аналіз показує, що існуючі підходи до оцінювання функційної безпечності мають різні області застосування. FMECA/FMEDA забезпечує систематичний аналіз потенційних відмов, FIT – експериментальну перевірку поведінку системи, а програмні засоби забезпечують автоматизацію оброблення значних обсягів інформації. Однак для ІКС на програмовних платформах залишається низка невирішених питань. зокрема:

– формалізація особливостей апаратних та програмних дефектів;

– повне врахування множини компонентів;

– повне врахування множини видів відмов;

– врахування множинних дефектів;

– аналіз дефектів різних рівнів;

– аналіз дефектів різних версій;

– урахування діагностованості;

– урахування критичних припущень;

– зменшення залежності результатів від суб’єктивних експертних оцінок;

– комплексування FMECA/FMEDA та FIT;

– автоматизований контроль повноти та узгодженості аналізу.

Таким чином, аналіз методів та інструментальних засобів дозволяє сформулювати такі основні висновки.

По-перше, FMECA/FMEDA є доцільним базовим аналітичним методом для оцінювання функційної безпечності ІКС на програмовних платформах, оскільки дозволяє пов’язати компоненти, види відмов, наслідки, імовірність, тяжкість та діагностованість.

По-друге, для програмовних платформ традиційна FMECA повинна бути розширена з урахуванням специфічних програмних, апаратних, конфігураційних та множинних дефектів.

По-третє, достовірність результату FMECA/FMEDA суттєво залежить від повноти сформованої експертом моделі. Тому необхідно аналізувати не тільки види відмов, а й припущення, що використовуються під час побудови таблиці.

По-четверте, FIT є доцільним експериментальним доповненням FMECA/FMEDA, оскільки дозволяє перевіряти фактичну реакцію системи на задані дефекти та контролювати обґрунтованість припущень щодо діагностованості й безпечності.

По-п’яте, комплексне застосування FMECA/FMEDA та FIT потребує відповідних інструментальних засобів, які забезпечують простежуваність між аналітичними та експериментальними результатами.

По-шосте, автоматизація повинна бути спрямована не тільки на механічне формування FMECA-таблиць, а й на контроль повноти, узгодженості та критичності припущень, підтримку експертних процедур і формування FIT-сценаріїв.

Таким чином, проведений аналіз підтверджує доцільність подальшого розвитку FMECA/FMEDA та FIT для їх комплексування при оцінюванні функційної безпечності ІКС на програмовних платформах. Основними

напрямами такого розвитку є формалізація структури аналізу, зменшення кількості критичних припущень, підвищення повноти врахування дефектів, підтримка множинних і багатоверсійних дефектів, а також інтеграція аналітичного та експериментального оцінювання.

1.3. Аналіз впливу експертів при виконанні FMECA і FIT

1.3.1. Операції оцінювання з підтримкою експертів

Оцінювання функційної безпечності ІКС на програмовних платформах передбачає виконання значної кількості операцій, результати яких не завжди можуть бути отримані безпосередньо шляхом формальних розрахунків або автоматизованого оброблення даних. Це обумовлено складністю досліджуваних ІКС, недостатньою кількістю статистичної інформації про відмови, необхідністю врахування особливостей конкретної архітектури та оцінювання властивостей, для яких відсутня однозначна формальна модель.

У таких випадках основним джерелом інформації можуть бути експертні знання. Експертне оцінювання ґрунтується на використанні досвіду та знань фахівця щодо структури системи, принципів її функціонування, можливих відмов, механізмів їх виявлення, способів резервування та наслідків порушення функцій. Оцінювання безпечності експертами суттєво залежить від їхнього досвіду та знань про особливості систем у цілому, можливі ризики для систем відповідного типу та типові відмови. При цьому експерт, як правило, здійснює якісне оцінювання параметрів безпечності без явної та однозначної формалізації власних міркувань на всіх етапах оцінювання.

У FMECA/FMEDA експертна підтримка необхідна вже на етапі формування об’єкта аналізу. Перед виконанням оцінювання необхідно визначити множину компонентів або функціональних елементів ІКС, які повинні бути включені до аналізу. Для кожного компонента необхідно визначити можливі види відмов, їх причини, локальні та системні наслідки,

можливість діагностування, а також інші характеристики, необхідні для визначення критичності.

Таким чином, FMECA/FMEDA не можна розглядати лише як процедуру математичного оброблення наперед заданої таблиці. Формування самої таблиці є частиною процесу оцінювання і містить низку операцій, у яких використовується експертне судження. До основних операцій FMECA/FMEDA, що потребують експертної підтримки, належать:

– визначення компонентів або функціональних елементів системи, які включаються до аналізу;

– визначення ієрархічного рівня, на якому виконується аналіз;

– визначення видів відмов кожного компонента;

– визначення причин виникнення відмов;

– визначення локальних наслідків відмов;

– визначення наслідків відмов на функціональному рівні;

– визначення впливу відмови на функцію безпеки;

– визначення можливості виявлення відмови;

– оцінювання діагностичного покриття;

– визначення категорії відмови;

– оцінювання імовірності або частоти виникнення;

– оцінювання тяжкості наслідків;

– визначення критичності;

– визначення необхідності додаткового аналізу або експериментальної перевірки.

Для ІКС на програмовних платформах перелік таких операцій розширюється через необхідність одночасного аналізу апаратних, FPGA та програмних компонентів. У цьому випадку експерт повинен не тільки визначити фізичні компоненти, але й встановити, які програмні або логічні об’єкти є самостійними об’єктами аналізу.

Особливістю є також необхідність визначення взаємозв’язків між апаратними та програмними компонентами. Один апаратний дефект може

призвести до зміни поведінки програмного компонента, а програмний дефект може змінити реакцію системи на апаратну відмову. Тому експертне оцінювання повинно враховувати не тільки властивості окремих компонентів, а й характер їх взаємодії.

Для FMEDA додатково необхідно оцінити можливість діагностування відмов. Наприклад, експерт повинен визначити, чи буде конкретна відмова виявлена вбудованим механізмом діагностики, чи буде виявлена із заданою імовірністю, або залишиться невиявленою. Помилка на цьому етапі безпосередньо впливає на подальший розподіл відмов на безпечні, небезпечні, виявлені та невиявлені.

У випадку FIT експертна підтримка має інший характер. Основними операціями є визначення множини дефектів, які доцільно ін’єктувати, визначення способу їх ін’єктування, формування очікуваної реакції системи та оцінювання відповідності фактичної реакції очікуваній.

Таким чином, для FIT експерт може визначати:

– які дефекти мають бути ін’єктовані;

– на якому рівні необхідно виконати ін’єктування;

– який механізм відмови необхідно моделювати;

– яку реакцію системи слід вважати правильною;

– які ознаки свідчать про виявлення дефекту;

– який стан системи після виявлення є безпечним;

– які результати тесту повинні бути включені до подальшого аналізу.

Це дозволяє розглядати FMECA/FMEDA та FIT як взаємопов’язані процедури. Результати експертного FMECA/FMEDA можуть використовуватися для формування множини критичних дефектів, які необхідно перевірити за допомогою FIT. У свою чергу, результати FIT можуть використовуватися для уточнення експертних припущень щодо діагностованості та наслідків відмов.

Особливого значення експертні операції набувають при аналізі множинних дефектів. Якщо одиничний дефект може бути оцінений

безпосередньо за його локальним та системним наслідком, то для множини дефектів необхідно визначити можливість їх одночасного виникнення, взаємний вплив, маскування одного дефекту іншим та вплив комбінації на резервовану структуру.

Для багатоверсійних ІКС додатково необхідно визначити, чи є дефекти різних версій незалежними, чи можуть мати спільну причину, а також чи може дефект однієї версії бути компенсований іншою версією. Такі питання не завжди можуть бути вирішені автоматично і потребують спеціальних знань експерта. Експертні операції можна розділити на три основні групи.

До першої групи належать операції формування моделі. Вони визначають, що саме аналізується. До них належать вибір компонентів, визначення видів відмов, визначення наслідків та встановлення зв’язків між об’єктами. До другої групи належать операції параметричного оцінювання. Вони визначають числові або категоріальні характеристики вже сформованої моделі: імовірність, тяжкість, критичність, діагностованість тощо. До третьої групи належать операції інтерпретації результатів. Експерт визначає, чи є отриманий результат прийнятним, які відмови є критичними, які припущення потребують перевірки та які результати повинні бути підтверджені додатковими процедурами.

Для кожної з цих груп характерний свій тип невизначеності. На етапі формування моделі основною проблемою є неповнота. На етапі параметричного оцінювання – суб’єктивність числових значень. На етапі інтерпретації – неоднозначність висновку та залежність від досвіду експерта. При цьому один експерт не обов’язково повинен виконувати всі операції оцінювання. Для складних ІКС доцільним є залучення групи експертів із різними компетенціями. Наприклад, один експерт може спеціалізуватися на апаратній архітектурі, другий – на FPGA, третій – на програмному забезпеченні, четвертий – на функційній безпечності та стандартах.

Такий розподіл дозволяє підвищити якість окремих оцінок, однак одночасно створює проблему узгодження результатів. Різні експерти можуть

сформувати різні множини компонентів, видів відмов та наслідків або по-різному оцінити їхню імовірність, тяжкість та критичність. Тому процес експертного оцінювання повинен передбачати не тільки отримання індивідуальних оцінок, але й процедури їх оброблення та формування узгодженої оцінки.

На рис.1.3 надано підсумовуючі результати аналізу впливу експертів на розглянуті методи оцінки.

Метод оцінювання ФБ	Експертна підтримка (обмеження)	Відсоток операцій
(S)FME(C,D) A / (Software) Failures Modes Effects (Criticality, Diagnostics) Analysis	Вибір критичних елементів, видів відмов, оцінка критичності (розмірність задач)	Понад 50%
(S)FIT / (Software) Fault Injection Testing	Вибір мовних конструкцій, видів помилок, оцінка критичності (розмірність задач і технологічна складність)	Понад 30%
MM / Markov's Models	Визначення станів, інтенсивностей відмов і відновлень (розмірність задач)	Понад 70%
CCF / Common Cause Failure (оцінка диверсності для багатоверсійних систем)	Визначення видів і метрик диверсності (відсутність репрезентативної статистики, складність тестування)	Понад 50%

Рисунок 1.3 – Результати аналізу впливу експертів на розглянуті методи оцінки

Отже за результатами аналізу констатуємо, що: зростання розмірності задач ускладнює перевірку відповідності ФБ ІКС вимогам; спрощення процедур шляхом формування більш грубих припущень збільшує ризики ФБ; вплив експертних знань на повноту і достовірність оцінки ФБ. Таким чином, з одного боку, експертна підтримка є невід'ємною складовою оцінювання функційної безпечності ІКС на програмовних платформах. Водночас використання експерта створює додаткове джерело невизначеності, пов'язане з

неповнотою знань, суб’єктивністю суджень, різним рівнем компетентності та можливими помилками під час виконання окремих операцій. Тому наступним етапом аналізу є дослідження факторів невизначеності та експертних помилок.

1.3.2. Фактор невизначеності і експертні помилки

Застосування експертного оцінювання дозволяє отримувати інформацію в умовах неповних даних, однак одночасно призводить до виникнення невизначеності результатів. Для функційної безпечності ІКС ця проблема має принципове значення, оскільки експертна оцінка використовується для визначення параметрів, безпосередньо пов’язаних із висновком про безпечність системи. Більшість нормативних документів з функційної безпечності передбачає необхідність оцінювання імовірності або ризику відмов. Проте для складних ІКС на практиці часто відсутні повна всеохоплююча модель системи та достатній обсяг репрезентативних статистичних даних, які можна було б безпосередньо використати для аналізу надійності та безпечності. У такій ситуації експерт змушений виконувати суб’єктивне оцінювання.

Безпосереднє введення експертом числових значень може призводити до упереджених результатів. Причиною цього можуть бути відмінності у досвіді, неповнота інформації, різне трактування запитання, використання евристик, надмірна впевненість у власній оцінці або прагнення спростити складну задачу. Евристичні судження є неформальними міркуваннями, які дозволяють експерту швидко отримати оцінку або розрахунок. Перевагою евристики є швидкість прийняття рішення, однак отриманий результат не обов’язково є найбільш точним або оптимальним.

Для FMECA/FMEDA невизначеність може виникати на різних етапах. На етапі визначення структури системи експерт може не включити до аналізу певний компонент. У такому випадку відмови цього компонента автоматично не потраплять до FMECA-таблиці.

На етапі формування множини видів відмов експерт може пропустити окремий вид відмови або, навпаки, включити відмову, яка не відповідає реальній поведінці системи. На етапі визначення наслідків експерт може неправильно встановити зв’язок між локальною відмовою та системною функцією. На етапі оцінювання імовірності може бути використано неточне або недостатньо обґрунтоване значення. На етапі оцінювання тяжкості може бути завищено або занижено вплив відмови. На етапі оцінювання діагностованості експерт може припустити, що відмова гарантовано виявляється діагностичною системою, хоча фактичне діагностичне покриття є нижчим. На етапі оцінювання множинних відмов може бути зроблене припущення про незалежність дефектів, хоча між ними існує спільна причина або залежність.

Отже, експертна помилка може змінювати не тільки окреме числове значення, а й саму структуру FMECA-моделі. Це дозволяє розділити експертні помилки на дві основні групи: помилки формування моделі; помилки оцінювання параметрів моделі. Помилки першої групи призводять до зміни множини об’єктів аналізу. Наприклад, може бути пропущено компонент, вид відмови або наслідок. Помилки другої групи не змінюють структуру таблиці, але змінюють значення її параметрів – імовірності, тяжкості, критичності або діагностованості.

Для оцінювання функційної безпечності помилки формування моделі можуть бути навіть більш небезпечними, ніж помилки числового оцінювання. Якщо числове значення має невелику похибку, результат може залишатися в межах допустимого діапазону. Якщо ж критична відмова взагалі не включена до аналізу, подальше математичне оброблення не дозволить виявити її. Тому проблема повноти FMECA є безпосередньо пов’язаною з проблемою експертної невизначеності. Окремим джерелом невизначеності є різниця між припущенням і встановленим фактом. Якщо експерт вважає, що певний компонент не може відмовити певним чином, це твердження має розглядатися як припущення, якщо воно не підтверджене відповідними доказами.

Аналогічно, припущення про гарантоване діагностування відмови не повинно автоматично трактуватися як встановлений факт. Воно може бути підтверджене результатами FIT, формальним доказом або іншою незалежною процедурою. Критичність припущення визначається не тільки ймовірністю його помилковості, а й впливом можливої помилки на підсумкову оцінку функційної безпечності.

Наприклад, припущення про відсутність відмови компонента, який не впливає на функцію безпеки, має невисоку критичність. Навпаки, припущення про гарантоване виявлення небезпечної відмови резервованого каналу може мати високу критичність, оскільки помилка цього припущення здатна змінити категорію відмови з безпечної на небезпечну невиявлену.

Таким чином, усі припущення не повинні розглядатися як однаково важливі. Необхідно визначати ті з них, які мають найбільший вплив на результати аналізу, та спрямовувати на їх перевірку першочергові ресурси. Для FIT експертна невизначеність має дещо іншу природу. Тут помилка може полягати у неправильному виборі дефекту для ін’єктування, некоректному способі ін’єктування або неправильному визначенні очікуваної реакції системи.

Наприклад, якщо експерт вважає, що введення певного дефекту повинно призвести до переходу системи в безпечний стан, але фактично цей дефект маскується іншими компонентами, результат тесту може бути неправильно інтерпретований.

Тому експертне FIT також повинно містити явне визначення:

– що саме вважається дефектом;

– де дефект ін’єктується;

– який стан системи перед ін’єктуванням;

– яка реакція очікується;

– які ознаки вважаються ознаками виявлення;

– який результат вважається позитивним;

– які результати свідчать про недостатнє діагностичне покриття.

З огляду на це експертна невизначеність у FMECA/FMEDA та FIT має спільне джерело – залежність результату від суб’єктивного рішення, але проявляється на різних етапах.

Ще одним фактором є різна компетентність експертів. Для складної ІКС один фахівець може мати значний досвід в апаратурі, але недостатню компетентність у програмному забезпеченні або FPGA. Інший експерт може мати протилежний профіль. Тому просте усереднення оцінок не завжди є коректним. Для зменшення впливу суб’єктивності доцільно використовувати кілька незалежних експертів та процедури агрегації їхніх оцінок. При цьому необхідно зберігати не тільки підсумкову оцінку, але й вихідні судження окремих експертів. Це забезпечує можливість простежування процесу формування кінцевого результату.

Окремо необхідно враховувати можливість узгоджених помилок. Якщо всі експерти використовують одне й те саме неправильне припущення, просте збільшення кількості експертів не гарантує підвищення достовірності результату. Наприклад, усі експерти можуть виходити з припущення, що певний механізм діагностики гарантовано виявляє конкретний дефект, хоча це припущення є неправильним.

Тому найбільш критичні припущення доцільно перевіряти незалежними методами, зокрема шляхом FIT, формального аналізу або використання документованих даних. Важливо також розрізняти невизначеність і помилку. Невизначеність характеризує відсутність достатньої інформації або неможливість однозначно встановити значення певного параметра. Помилка означає невідповідність отриманого експертного рішення обґрунтованому або фактичному значенню. Наприклад, якщо для певного компонента відсутні статистичні дані про частоту відмов, оцінка експерта містить невизначеність. Якщо після отримання достатньої кількості даних встановлено, що експертна оцінка систематично відрізняється від фактичного значення, це вже характеризує помилку оцінювання.

Таке розмежування має практичне значення. Невизначеність може бути зменшена шляхом отримання додаткової інформації, проведення випробувань або залучення додаткових експертів. Помилка потребує виявлення її причини та коригування процедури оцінювання.

Для оцінювання впливу експертних припущень доцільно використовувати ризик-орієнтований підхід. У матеріалах, пов’язаних із розробленим підходом, вплив припущень та помилок аналізу розглядається через рівні критичності, зокрема High, Medium та Low. Така класифікація дозволяє визначити припущення, які потребують першочергової перевірки.

Таким чином, експертні операції є невід’ємною складовою FMECA/FMEDA та FIT, але одночасно створюють додатковий фактор невизначеності. Найбільш суттєвими джерелами невизначеності є неповнота інформації, відсутність статистичних даних, суб’єктивність, евристичні судження, різна компетентність експертів, неоднозначність постановки задачі та помилки під час формування моделі. Для ІКС на програмовних платформах ця проблема посилюється необхідністю одночасного аналізу HW, FPGA та SW, а також множинних і багатоверсійних дефектів.

Проведений аналіз дозволяє сформулювати основну вимогу до подальшого розвитку методів оцінювання: необхідно не тільки отримувати експертні оцінки, а й формалізувати операції, у яких вони використовуються, визначати критичні припущення, оцінювати їхній вплив та зменшувати залежність підсумкового результату від потенційних експертних помилок.

1.4. Обґрунтування задач і методики досліджень

1.4.1. Загальна і часткові задачі

Проведений аналіз показав, що оцінювання функційної безпечності ІКС на програмовних платформах характеризується поєднанням кількох взаємопов’язаних суперечливих обставин. З одного боку, такі системи повинні

відповідати високим вимогам до функційної безпечності, установленим нормативними документами для критичних систем, зокрема для ІКС атомних електростанцій. З іншого боку, традиційні методи FMECA/FMEDA та FIT мають обмеження, пов’язані з аналізом складних програмно-апаратних структур, множинних відмов, багатоверсійних систем, диверсності, а також із використанням експертних припущень та суджень.

Отже, загальна задача дослідження полягає в розробленні моделей, показників та методів оцінювання функційної безпечності ІКС на програмовних платформах на основі розвитку табличного методу FMECA/FMEDA та його комплексування з процедурами FIT, що забезпечують підвищення повноти й достовірності оцінювання шляхом урахування критичності припущень, експертних помилок, множинних відмов та особливостей багатоверсійних систем.

Відповідно до загальної задачі сформовано такі часткові задачі дослідження.

1. *Розроблення базової таблично-множинної моделі FMECA/FMEDA для ІКС на програмовних платформах*. Необхідно формалізувати процес формування FMECA-таблиці з урахуванням особливостей програмовних платформ, у тому числі можливості виникнення фізичних, проєктних та програмних дефектів. Модель повинна забезпечувати представлення компонентів системи, видів відмов, наслідків та показників критичності у формі, придатній для подальшого автоматизованого оброблення.

Ця задача безпосередньо відповідає структурі розділу 2, у якому передбачено формування базової моделі FMECA для одноверсійних ІКС та її таблично-множинне представлення з урахуванням особливостей дефектів програмовних платформ.

2. *Формування та аналіз множини припущень, що використовуються при FMECA/FMEDA*. Необхідно визначити множину припущень, на яких базується побудова та використання FMECA-моделі, встановити їхній вплив на результати оцінювання та виділити критичні припущення.

3. *Розроблення удосконаленої моделі FMECA/FMEDA з урахуванням критичності припущень*. Необхідно розробити процедуру модифікації базової FMECA-моделі шляхом видалення або заміни припущень, критичних для оцінювання функційної безпечності, а також визначити правила формування удосконаленої моделі.

4. *Визначення показників функційної безпечності, повноти та достовірності оцінювання*. Необхідно визначити показники, які дозволяють оцінювати не тільки отримане значення критичності, але й якість самого процесу оцінювання. Особливу увагу необхідно приділити показникам повноти охоплення компонентів та режимів відмов, а також достовірності результатів з урахуванням припущень і можливих помилок аналізу.

5. *Розроблення методу експертного оцінювання FMECA/FMEDA-FIT*. Необхідно формалізувати експертні операції, визначити множину експертів, множину експертних задач та множину можливих рішень, а також розробити процедури отримання й узгодження експертних оцінок.

6. *Зменшення впливу суб'єктивності експертного оцінювання.* Необхідно зменшити кількість операцій, що безпосередньо виконуються експертами, та забезпечити формальне узгодження вербальних, нечітких і кількісних суджень.

7. *Розроблення методу комплексування FMECA/FMEDA та FIT.* Необхідно забезпечити використання результатів FMECA/FMEDA для формування множини дефектів, що підлягають перевірці методом FIT, а результатів FIT – для підтвердження або спростування припущень щодо відмов, їх виявлення та наслідків.

8. *Урахування множинних відмов і багатоверсійності ІКС*. Необхідно розширити процедури оцінювання для випадків одночасного виникнення декількох дефектів та функціонування декількох версій ІКС. Для багатоверсійних систем необхідно врахувати як індивідуальні дефекти версій, так і загальні дефекти, що можуть впливати на декілька версій одночасно.

9. *Розроблення процедур практичного застосування запропонованих моделей та методів*. Необхідно забезпечити можливість практичного

використання розроблених моделей і методів у вигляді технології оцінювання та відповідних програмно-інструментальних засобів.

1.4.2. Обґрунтування вибору математичного апарату

Специфіка поставленої задачі визначає необхідність використання не одного математичного методу, а комплексу взаємопов’язаних математичних засобів. Це обумовлено тим, що дослідження охоплює як формалізовані характеристики структури ІКС та відмов, так і експертні судження, які можуть мати вербальну, нечітку або кількісну форму.

Першим рівнем математичного представлення доцільно використати теорію множин та кортежів. Вона дозволяє формалізувати структуру FMECA-таблиці та встановити взаємозв’язки між компонентами, видами відмов, наслідками та оцінками критичності.

Другим необхідним математичним засобом є алгебра логіки та логіко-множинні операції. Вони необхідні для представлення умов виникнення відмов, взаємозалежності дефектів та визначення комбінацій відмов. Особливого значення це набуває для множинних дефектів, коли необхідно встановити умови одночасного або послідовного виникнення декількох відмов.

Для багатоверсійних систем логічний апарат дозволяє розділити індивідуальні та загальні дефекти. Відповідно до сформульованої концепції досліджень, багатоверсійна ІКС може містити індивідуальні дефекти окремих версій та абсолютні, або загальні, дефекти, що впливають на декілька версій.

Третім складником є апарат теорії надійності та ймовірнісного оцінювання. Він використовується для кількісного визначення ймовірностей виникнення відмов та оцінювання їхнього впливу на функції безпеки.

Четвертим складником є теорія нечітких множин та нечітке оцінювання. Її використання обумовлено тим, що експерт не завжди може надати точне числове значення. На практиці оцінка може формулюватися як «низька», «середня», «висока», «дуже висока» тощо. Перетворення таких вербальних

оцінок безпосередньо у точкові значення може призвести до втрати інформації про невизначеність судження.

Тому доцільно зберігати вербальну оцінку та представляти її нечіткою множиною з відповідною функцією належності. Це дозволяє виконувати подальшу агрегацію суджень без передчасного переходу до точкових значень.

П’ятим складником є методи експертного оцінювання та агрегації суджень. Необхідність їх використання визначається тим, що частина параметрів FMECA/FMEDA не може бути достовірно визначена виключно на основі статистичних даних.

Шостим складником є нечітке ризик-орієнтоване оцінювання критичності припущень та помилок. Необхідність такого апарату обумовлена тим, що критичність припущення не визначається тільки фактом його існування. Важливим є потенційний вплив відмови від припущення або помилки аналізу на кінцеву оцінку функційної безпечності.

Сьомим складником є апарат аналізу причинно-наслідкових зв’язків. Він необхідний для встановлення залежності між припущенням, помилкою аналізу, видом відмови та кінцевою оцінкою функційної безпечності.

Восьмим складником є математичний апарат аналізу експериментальних результатів FIT. FIT використовується для практичної перевірки припущень та оцінок, сформованих на етапі FMECA/FMEDA. У цьому випадку математичні процедури повинні забезпечувати порівняння очікуваної та фактичної реакції системи на ін’єктований дефект.

1.4.3. Етапи та методика досліджень

З урахуванням сформульованої загальної та часткових задач дослідження доцільно виконувати послідовно, переходячи від аналізу предметної області та базових моделей до розроблення удосконалених моделей і методів їх практичного використання.

Загальна схема дослідження передбачає такі основні етапи:

Етап 1. Аналіз вимог до функційної безпечності ІКС.

Етап 2. Аналіз існуючих методів та засобів оцінювання.

Етап 3. Аналіз експертних операцій та джерел невизначеності.

Етап 4. Формування базової FMECA-моделі.

Етап 5. Формування множини припущень та помилок.

Етап 6. Проведення AMECA-аналізу.

Етап 7. Побудова удосконаленої EFMECA-моделі.

Етап 8. Розроблення показників повноти та достовірності.

Етап 9. Формалізація задачі експертного оцінювання.

Етап 10. Розроблення процедур узгодження експертних оцінок.

Етап 11. Комплексування EFMECA та FIT.

Етап 12. Розширення методу на множинні відмови.

Етап 13. Розширення методу на багатоверсійні ІКС.

Етап 14. Розроблення програмно-інструментальних засобів.

Етап 15. Експериментальна та практична перевірка.

Така методика досліджень забезпечує цілісність дисертаційного дослідження: нормативні вимоги визначають критерії оцінювання, аналіз існуючих методів визначає їх обмеження, математичний апарат забезпечує формалізацію моделей та експертних суджень, а комплексування EFMECA та FIT забезпечує можливість перевірки критичних припущень і підвищення достовірності кінцевої оцінки функційної безпечності.

1.4.4. Принципи і задачі досліджень

У світі також активно розвиваються методи assurance case, FMECA, FIT, FTA, оцінювання готовності, надійності, функційної безпечності і кібербезпеки критичних систем. У цьому контексті важливими є роботи з різних (напівформальних, формальних, евристичних та експериментальних) методів. Для даної роботи це важливо з двох причин.

По-перше, це підтверджує актуальність теми. Проблеми, які виникають при оцінюванні ІКС АЕС на програмовних платформах, не є локальними. Вони характерні для всієї галузі критичних систем. По-друге, аналіз світових досліджень показує, що існуючі підходи часто розв’язують окремі задачі: або FMECA, або FIT, або security, або diversity, або expert judgment. Але для практичного ліцензування ІКС АЕС потрібна інтегрована процедура, яка одночасно враховує фізичні дефекти, проєктні дефекти, вразливості, множинні відмови, багатоверсійність і помилки аналізу. Саме тому у роботі зроблено акцент на практично застосовній технології оцінювання.

Проведений аналіз показує декілька основних обмежень існуючих підходів. Перше – обмеженість аналізу одиничними дефектами. Для FPGA-систем це критично, тому що реальна поведінка може визначатися не тільки одиничною відмовою, а й комбінацією дефектів на різних рівнях: кристал, модуль, канал, система, VHDL-логіка, конфігурація, взаємодія версій. Друге – окремий розгляд рівнів системи. У складних ІКС АЕС рівні не можна повністю відокремити один від одного, оскільки дефект нижчого рівня може проявитися як функційна відмова на системному рівні. Третє – недостатнє врахування security. Кібербезпека часто розглядається окремо від функційної безпечності, хоча для сучасних цифрових і FPGA-based ІКС порушення інформаційної безпеки може прямо впливати на виконання функцій безпеки. Четверте – недостатність методів для диверсності і CCF. Для багатоверсійних систем важливо оцінювати не тільки індивідуальні дефекти кожної версії, а й спільні дефекти, які можуть одночасно вплинути на декілька каналів. П’яте – людський фактор. Результат залежить від кваліфікації експертів, а узгодження вербальних, нечітких і кількісних оцінок залишається складною задачею.

Отже, основна суперечність полягає в тому, що вимоги до технологій і засобів оцінювання функційної безпечності зростають, а існуючі XMECA-підходи мають обмеження щодо множинних відмов, експертних помилок і диверсності. Саме ця суперечність і визначає мету та задачі дисертаційного дослідження.

Принципи, на яких далі будуються моделі, методи і програмно-технічні засоби оцінювання, є наступними.

Перший принцип – це перехід від аналізу лише одиничних дефектів до аналізу одиничних і множинних дефектів. Для сучасних ІКС на програмовних платформах цього вже недостатньо – розглядати один компонент, один дефект і один наслідок. Реальна система може мати комбінації дефектів, які окремо не є критичними, але разом можуть призвести до небезпечного стану або до помилкового висновку щодо безпечності.

Другий принцип – це охоплення всіх рівнів системи. Для FPGA-based I&C дефект може виникати або проявлятися на різних рівнях: на рівні кристала, модуля, каналу, системи в цілому, а також на рівні проєктного опису – наприклад, VHDL-логіки. Тому аналіз має бути ієрархічним: від фізичних дефектів до системних наслідків.

Третій принцип – це поєднання аспектів надійності, функційної безпечності та інформаційної безпеки. У традиційному підході ці напрями часто розглядаються окремо: reliability окремо, safety окремо, security окремо. Але для сучасних ІКС АЕС таке розділення є умовним. Наприклад, проєктний дефект, вразливість взаємодії або помилка конфігурації можуть впливати не тільки на працездатність системи, а й на виконання функції безпеки.

Четвертий принцип – це врахування багатоверсійності. Для диверсних систем важливо відрізняти дефекти, які є індивідуальними для певної версії, від дефектів, які можуть бути спільними для різних версій.

Відповідно до виявлених обмежень і загальної ідеї дослідження сформульовано мету роботи. Мета полягає у підвищенні повноти та достовірності оцінювання функційної безпечності інформаційно-керуючих систем на платформах програмовної логіки, тобто на програмовних платформах, які мають структурно-версійну надмірність.

Тут важливо підкреслити два ключові слова – повнота і достовірність. Під повнотою мається на увазі те, наскільки оцінювання охоплює всі суттєві дефекти, режими відмов, рівні системи, канали, версії, діагностичні механізми і

небезпечні наслідки. Під достовірністю мається на увазі те, наскільки результат оцінювання є обґрунтованим, відтворюваним і не залежить надмірно від суб'єктивних припущень або помилок окремих експертів.

Досягнення цієї мети пропонується через розроблення і практичне впровадження методів та засобів аналізу видів і наслідків відмов – насамперед FMECA/FMEDA – з урахуванням фізичних і проєктних дефектів.

Науково-прикладна задача, відповідно, полягає у розробленні та удосконаленні моделей, методів і засобів оцінювання функційної безпечності одно- і багатоверсійних ІКС на програмовних платформах. Для досягнення поставленої мети сформульовано шість задач дослідження.

Перша задача – провести аналіз існуючих методів і програмно-апаратних засобів оцінювання функційної безпечності ІКС АЕС та інших критичних застосувань. Необхідно зрозуміти, які методи вже застосовуються, які мають переваги, які мають обмеження, і які з них можуть бути використані або модифіковані для програмовних платформ.

Друга задача – удосконалити моделі і показники для оцінки функційної безпечності ІКС на програмовних платформах з використанням FMECA/FMEDA шляхом введення множин компонентів, режимів відмов, наслідків, критичності, а також додаткових множин припущень і помилок аналізу. Мета – зробити сам процес оцінювання більш повним і контрольованим.

Третя задача – удосконалити метод оцінювання функційної безпечності з використанням FMECA, який виконується із залученням експертів. Оскільки експертний фактор неможливо повністю усунути, потрібно розробити процедури, які дозволяють класифікувати експертні питання, враховувати профіль експертів, узгоджувати вербальні, нечіткі та кількісні оцінки і зменшувати ризик суб'єктивних помилок.

Четверта задача – розробити метод оцінювання функційної безпечності двоверсійних ІКС на програмовних платформах з урахуванням множини проєктних і фізичних дефектів.

Це один із ключових елементів роботи, тому що для ІКС АЕС багатоверсійність і диверсність використовуються як засоби зниження ризику відмов за загальною причиною. Але для цього потрібно мати метод, який відрізняє індивідуальні дефекти версій від спільних дефектів і дозволяє оцінити їх вплив.

П’ята задача – розробити алгоритми і програмно-апаратні засоби оцінювання та вибору засобів підвищення функційної безпечності ІКС на програмовних платформах.
Це вже перехід від моделей і методів до інструментальної підтримки. Для практичного застосування важливо, щоб запропоновані підходи могли бути реалізовані у вигляді процедур, алгоритмів, програмних засобів або технології оцінювання.

Шоста задача – виконати практичне впровадження розроблених методів і засобів при створенні ІКС АЕС.
Це принципово важливо для прикладного характеру дисертації. Результат має бути не лише теоретичним, а придатним для використання у реальних процесах розроблення, верифікації, валідації, сертифікації та ліцензування ІКС.

1.5. Висновки до розділу

1. Не заважаючи на розвиток методів і засобів оцінювання надійності функційної та кібербезпеки, суперечності, які виникають при оцінюванні ІКС АЕС на програмовних платформах, не є локальними. Вони характерні для всієї галузі критичних систем. Існуючі підходи розв’язують окремі задачі (FMECA, FIT, тощо). Для практичного ліцензування ІКС АЕС потрібна інтегрована процедура, яка одночасно враховує фізичні дефекти, проєктні дефекти, вразливості, множинні відмови, багатоверсійність і помилки аналізу.

2. Проведений аналіз надав можливість визначити основні обмежень існуючих підходів, пов’язаних з наступним:

– обмеженість аналізу одиничними дефектами, не завжаючи на те, що для FPGA-систем небезпечна поведінка може визначатися комбінацією дефектів на рівнях кристалу модуля, каналу, VHDL-логіки тощо;

– відокремлений розгляд рівнів системи, хоча дефекти нижчого рівня можуть обумовлювати функційні відмови на системному рівні;

– недостатнє врахування кібербезпеки, яка розглядається окремо від функційної безпечності, хоча для сучасних цифрових і FPGA-based ІКС порушення кібербезпеки може прямо впливати на виконання функцій безпеки;

– недоліки методів для багатоверсійних систем, де важливо оцінювати не тільки індивідуальні дефекти, але й спільні дефекти;

– людський фактор, оскільки результати залежать від кваліфікації експертів, узгодження вербальних, нечітких і кількісних оцінок.

3. Основна суперечність полягає в тому, що вимоги до технологій і засобів оцінювання функційної безпечності зростають, а існуючі XMECA-підходи мають обмеження щодо множинних відмов, експертних помилок і диверсності. Саме ця суперечність і визначає мету та задачі дисертаційного дослідження.

4. Мета полягає у підвищенні повноти та достовірності оцінювання функційної безпечності інформаційно-керуючих систем на платформах програмовної логіки, тобто на програмовних платформах, які мають структурно-версійну надмірність.

5. Досягнення цієї мети пропонується через розроблення і практичне впровадження методів та засобів аналізу видів і наслідків відмов – насамперед FMECA/FMEDA – з урахуванням фізичних і проєктних дефектів. Науково-прикладна задача, відповідно, полягає у розробленні та удосконаленні моделей, методів і засобів оцінювання функційної безпечності одно- і багатоверсійних ІКС на програмовних платформах з урахуванням існуючих припущень та помилок експертів.

6. Сформульовано задачі дослідження:

– удосконалення моделей і показників для оцінки функційної безпечності ІКС на програмовних платформах з використанням FMECA/FMEDA і з урахуванням критичності припущень та помилок експертів;

– розроблення методу оцінювання функційної безпечності з використанням FMECA, який виконується із залученням експертів;

– розроблення методу оцінювання функційної безпечності двоверсійних ІКС на програмовних платформах з урахуванням множини проєктних і фізичних дефектів;

– розроблення алгоритмів і програмно-апаратних засобів оцінювання та вибору засобів підвищення функційної безпечності ІКС на програмовних платформах;

– практичне впровадження розроблених методів і засобів для ІКС АЕС.

РОЗДІЛ 2.
МОДЕЛІ І ПОКАЗНИКИ ДЛЯ ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ НА ПРОГРАМОВНИХ ПЛАТФОРМАХ З ВИКОРИСТАННЯМ ТАБЛИЧНОГО МЕТОДУ АНАЛІЗУ ВИДІВ І НАСЛІДКІВ ВІДМОВ (FMECA/FMEDA)

2.1. Базова модель аналізу видів і наслідків відмов одноверсійних ІКС ППЛ

Табличний метод аналізу видів і наслідків відмов FMECA/FMEDA є одним із базових засобів оцінювання функційної безпечності критичних інформаційно-керуючих систем. Його застосування дозволяє систематизувати інформацію про компоненти системи, можливі види їх відмов, наслідки відмов, імовірність виникнення, тяжкість наслідків та можливість виявлення відмов.

Для інформаційно-керуючих систем, реалізованих на ППЛ, традиційна FMECA-модель потребує розширення. Причиною є те, що об’єктом аналізу є не тільки фізичні компоненти апаратури, але й програмні компоненти, FPGA-логіка, конфігураційні дані, оператори програм, функціональні блоки та інші елементи, для яких поняття фізичної відмови повинно бути доповнене поняттям дефекту.

Особливістю ППЛ є також наявність різних рівнів представлення системи. На апаратному рівні аналізуються фізичні компоненти, на рівні FPGA – логічні та конфігураційні елементи, а на програмному рівні – оператори, функції, програмні модулі та результати їх виконання. Тому базова модель повинна бути незалежною від конкретного способу реалізації компонента та забезпечувати єдине представлення різних типів дефектів.

У подальшому під компонентом будемо розуміти елемент системи, для якого визначається можливість виникнення дефекту та його наслідків. Для одноверсійної ІКС множина таких компонентів задається:

$M\_F = \{f_i\}$, $i = 1,\ldots,F$,

де F – загальна кількість компонентів, включених до аналізу.

Для кожного компонента f_i визначається множина можливих видів відмов:

$M\_M_i = \{m_{ij}\}, j = 1,\ldots,k_i,$

де k_i – кількість видів відмов компонента f_i.

Кожному виду відмови m_{ij} відповідає множина можливих наслідків:

$M\_E_{ij} = \{e_{ijl}\},$

які характеризують прояв відмови на відповідному рівні системи.

Для кількісного або якісного оцінювання кожного виду відмови вводяться імовірність p_{ij}, тяжкість наслідків s_{ij} та критичність c_{ij}. У загальному випадку критичність визначається функцією:

$c_{ij} = \varphi(p_{ij}, s_{ij}).$

Для FMEDA додатково вводиться характеристика діагностованості:

$d_{ij},$

яка характеризує можливість виявлення відповідної відмови засобами діагностики.

2.1.1. Таблично-множинне представлення процесів аналізу видів і наслідків відмов з урахуванням особливостей дефектів програмовних платформ

Табличне представлення є зручним для практичного виконання FMECA/FMEDA, оскільки кожний рядок таблиці відповідає певному виду відмови конкретного елемента системи, а стовпці містять його характеристики.

Для формалізації такої таблиці введемо множину:

$FT_1 = \langle f_i, m_i = \{m_{ij}\}, e_i = \{e_{ij}\}, p_i = \{p_{ij}\}, s_i = \{s_{ij}\}, j = 1,\ldots,k_i\rangle.$

Тут:

f_i – елемент системи, що відмовив;

m_i – множина видів відмов елемента;

e_i – множина наслідків відмов;

p_i – множина значень імовірності відмов;

s_i – множина значень тяжкості наслідків;

k_i – кількість видів відмов елемента f_i.

Загальна кількість видів відмов визначається як:

$K = \Sigma_{i=1}^{G} k_i$.

У цьому випадку кількість рядків FMECA-таблиці визначається загальною кількістю розглянутих видів відмов.

Для FMEDA модель доповнюється характеристикою діагностованості:

$FT_2 = \langle f_i, m_i = \{m_{ij}\}, e_i = \{e_{ij}\}, d_i = \{d_{ij}\}, j = 1,\ldots,k_i \rangle$.

Таким чином, кожний запис таблиці характеризується не тільки видом і наслідком відмови, а й можливістю її виявлення.

З урахуванням особливостей ППЛ поняття «вид відмови» доцільно трактувати узагальнено як дефект або режим прояву дефекту, який може виникнути на певному рівні реалізації системи.

Для апаратного компонента це може бути обрив, коротке замикання, деградація параметра, втрата живлення або інший фізичний механізм.

Для FPGA-компонента дефект може бути пов’язаний із конфігураційною пам’яттю, логічним елементом, маршрутизацією сигналів, тактовим сигналом або порушенням конфігурації.

Для програмного компонента дефект може проявлятися як неправильний результат обчислення, зависання, пропуск операції, виконання некоректної гілки програми або порушення часових характеристик.

Отже, для ППЛ доцільно використовувати узагальнену множину дефектів:

$M\_D = M\_D^{HW} \cup M\_D^{fPGA} \cup M\_D^{sW}$,

де M_D^{HW}, M_D^{fPGA} та M_D^{sW} – множини дефектів апаратної, FPGA- та програмної частин відповідно.

Для кожного елемента f_i доцільно визначити рівень реалізації:

$l_i \in \{HW, FPGA, SW\}$.

Тоді компонент може бути представлений як:

$f_i = \langle id_i, l_i \rangle$,

де id_i – ідентифікатор компонента, а l_i – рівень його реалізації.

Це дозволяє формувати FMECA-таблицю з урахуванням специфіки ППЛ без зміни загального алгоритму аналізу.

Водночас необхідно враховувати рівень, на якому дефект виникає, оскільки один і той самий системний наслідок може бути спричинений дефектами різної природи.

Під час виконання FMECA/FMEDA експерт послідовно визначає елементи, види відмов, наслідки, імовірність, тяжкість та критичність. Фактичний процес побудови таблиці можна представити як:

$M\_F \rightarrow \Delta F \rightarrow \Delta M_i \rightarrow \Delta E_i \rightarrow P, S \rightarrow C.$

Для FMEDA додатково:

$M\_F \rightarrow \Delta F \rightarrow \Delta M_i \rightarrow \Delta E_i \rightarrow D \rightarrow P, S, C.$

Основним недоліком такого підходу є те, що множини ΔF, ΔM_i та ΔE_i формуються на основі експертного рішення. Отже, навіть при формально визначеній структурі таблиці її повнота залежить від того, наскільки повно експерт визначив компоненти, дефекти та наслідки.

Ця проблема є особливо важливою для ППЛ, оскільки дефект може бути представлений на одному рівні, але його наслідок проявлятися на іншому.

Наприклад, дефект програмного оператора може призвести до неправильного керування FPGA-виходом, а в результаті – до порушення функції безпеки на системному рівні. Тому FMECA-модель повинна забезпечувати трасування:

$f_i \rightarrow m_{ij} \rightarrow e_{ij} \rightarrow SF_r,$

де SF_r – відповідна функція безпеки.

Для множинних дефектів необхідно перейти від одиничного виду m_{ij} до множини:

$M_{ij}^{comb} = \{m_{i1j1}, m_{i2j2}, \ldots, m_{irjr}\}.$

Таке розширення є необхідним, оскільки аналіз множинних дефектів є важливою складовою оцінювання функційної безпечності ППЛ.

Таким чином, базова таблично-множинна модель забезпечує формальне представлення FMECA/FMEDA, але ще не усуває залежність результату від

експертних припущень. Для цього необхідно окремо виділити множину припущень та дослідити їхній вплив.

2.1.2. Визначення множини припущень та їх аналіз

Побудова FMECA/FMEDA-таблиці неможлива без використання певної множини припущень. Частина з них є явними – вони безпосередньо формулюються експертом або нормативним документом. Інша частина є неявними та проявляється через вибір компонентів, видів відмов, наслідків або значень параметрів.

Позначимо множину припущень як:

$M\_Asm = \{Asm_k\}$, $k = 1,\ldots,A$,

де A – загальна кількість ідентифікованих припущень.

Кожне припущення може бути представлено кортежем:

$Asm_k = \langle d_k, o_k, r_k, c_k \rangle$,

де d_k – опис припущення; o_k – об’єкт FMECA, якого воно стосується; r_k – результат, що залежить від припущення; c_k – критичність припущення.

До типових припущень належать:

– припущення щодо повноти множини компонентів;

– припущення щодо повноти множини видів відмов;

– припущення щодо повноти множини наслідків;

– припущення щодо незалежності відмов;

– припущення щодо імовірності відмов;

– припущення щодо тяжкості наслідків;

– припущення щодо діагностованості;

– припущення щодо коректності реалізації механізмів резервування;

– припущення щодо незалежності версій у багатоверсійній системі;

– припущення щодо відсутності спільних причин відмов;

– припущення щодо коректності результатів FIT.

Для кожного припущення необхідно визначити його вплив на результуючу оцінку.

Введемо множину залежних від припущення елементів:

$M\_Dep(Asm_k) = \{x \mid x \text{ залежить від } Asm_k\}$.

Тоді припущення є тим критичнішим, чим більша кількість елементів аналізу залежить від нього та чим суттєвіший вплив зміни припущення на результуючу оцінку безпечності.

У загальному випадку критичність припущення може бути представлена функцією:

$C\_Asm,_k = \Phi(I_k, S_k)$,

де I_k – рівень впливу припущення, S_k – значущість наслідків помилкового припущення.

Важливо розрізняти припущення та фактичні дані. Якщо значення параметра підтверджено експериментом або документованими даними, воно не повинно розглядатися як експертне припущення. Якщо ж воно вибране виключно на основі досвіду експерта, його необхідно включити до M_Asm.

Для аналізу припущень доцільно використовувати AMECA – Assumption Modes and Effects Criticality Analysis.

Для кожного Asm_k необхідно визначити:

$Asm_k \rightarrow Impact_k \rightarrow Criticality_k$.

Множина критичних припущень визначається як:

$M\_Asm^{cr} = \{Asm_k \in M\_Asm \mid C\_Asm,_k \geq C\_thr\}$,

де C_thr – встановлений поріг критичності.

Для якісного оцінювання може використовуватися трирівнева шкала:

$C\_Asm \in \{L, M, H\}$,

де L – низька критичність, M – середня, H – висока.

Для критичних припущень необхідно виконувати додаткову перевірку. Можливими способами перевірки є:

– використання документованих даних;

– повторне експертне оцінювання;

– залучення незалежного експерта;

– формальний аналіз;

– моделювання;

– ін’єктування дефектів;

– порівняння з результатами випробувань.

Таким чином, FMECA-аналіз перетворюється з одноразової процедури формування таблиці на ітеративний процес:

$FMT_0 \rightarrow AMECA \rightarrow M\_Asm^{cr} \rightarrow Validation \rightarrow FMT_1$.

Отримана модель FMT_1 повинна містити меншу кількість критичних неперевірених припущень.

2.2. Удосконалена модель FMECA/FMEDA аналізу видів і наслідків відмов із видаленням частини припущень

Базова FMECA/FMEDA-модель формується на основі множини припущень, частина з яких може мати суттєвий вплив на результати. Тому для підвищення повноти та достовірності оцінювання необхідно сформувати модель, у якій критичні припущення замінюються підтвердженими даними або процедурами перевірки.

Позначимо базову модель як:

$FMT_0 = \langle M\_F, M\_M, M\_E, M\_C \rangle$.

Нехай:

$M\_Asm^{cr} = \{Asm_1, \ldots, Asm\_R\}$

є множиною критичних припущень.

Для кожного критичного припущення формується модель:

$FMT_r = FMECA(FMT_0, Asm_r)$,

у якій відповідне припущення вилучається, уточнюється або замінюється результатом перевірки.

На відміну від базової моделі, EFMECA повинна забезпечувати трасування залежностей:

$Asm_k \rightarrow FMECA \rightarrow C_{ij} \rightarrow$ оцінювання безпечності.

Це дозволяє визначити, які саме припущення вплинули на кінцевий висновок.

У разі використання FIT результати тестування можуть бути використані для зміни відповідних елементів EFMECA. Якщо очікуваний результат FIT підтверджено, відповідне припущення отримує статус підтвердженого. Якщо результат не підтверджено, формується новий режим відмови або змінюється характеристика діагностованості.

Узагальнена модель представлена у вигляді схеми на рис. 2.1.

Рисунок 2.1 – Основні елементи узагальненої моделі аналізу

2.3. Показники для оцінювання функційної безпечності та повноти оцінювання

Результати FMECA/XMECA можуть бути представлені як сукупність оцінок і рішень, отриманих на основі аналізу елементів системи, видів відмов, наслідків, імовірностей та тяжкості. При цьому достовірність отриманої оцінки залежить не тільки від використаної математичної моделі, а й від повноти розгляду відмов, прийнятих припущень, експертних рішень та використаних засобів підтримки аналізу.

Під повнотою мається на увазі те, наскільки метод оцінювання охоплює всі суттєві дефекти, режими відмов, рівні системи, канали, версії, діагностичні механізми і небезпечні наслідки, під достовірністю – наскільки результат оцінювання є обґрунтованим, відтворюваним і не залежить від суб'єктивних припущень або помилок окремих експертів.

У моделі FMECA кожен елемент f_i характеризується множиною можливих видів відмов m_i, множиною наслідків e_i, імовірністю відмови p_i та тяжкістю наслідків s_i. Критичність відмови c_i визначається як функція імовірності та тяжкості:

$c_i = \varphi(p_i, s_i)$.

Імовірність p_i може задаватися якісно за допомогою нечіткої шкали, наприклад «низька – середня – висока», або кількісно у діапазоні від 0 до 1. Аналогічно тяжкість s_i може задаватися якісно або кількісно.

Таким чином, у базовій FMECA-моделі використовуються три взаємопов'язані характеристики:

p_i – імовірність відмови;

s_i – тяжкість наслідків;

c_i – критичність відмови.

Графічний взаємозв'язок між імовірністю, тяжкістю та критичністю наведено на рис. 2.2. Він демонструє, що критичність визначається спільним урахуванням імовірності виникнення відмови та тяжкості її наслідків.

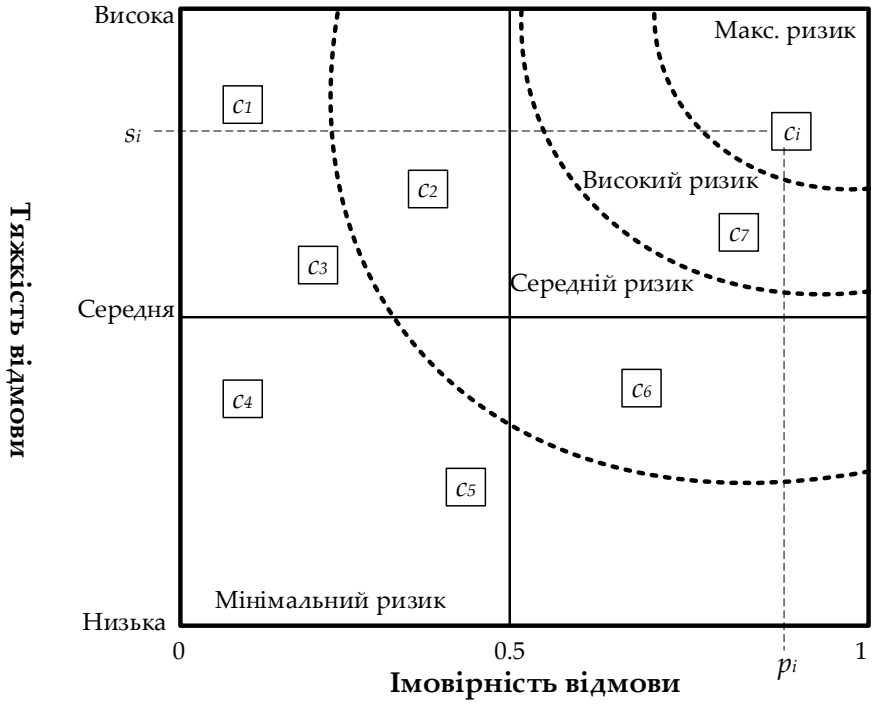


Рисунок 2.2 – Відношення між імовірністю, тяжкістю та критичністю

У розглянутій моделі критичність не задається незалежно від інших параметрів, а визначається функцією φ. Це дозволяє використовувати як кількісні, так і нечіткі значення параметрів.

Кількість розглянутих видів відмов для елемента і позначається k_i. Загальна кількість видів відмов визначається як:

$k = k_1 + k_2 + \ldots + k\_F$,

де F – кількість елементів, включених до FMECA-аналізу.

Також використовуються відомі показники функційної безпечності та надійності:

– інтенсивність відмов;

– доля безпечних відмов;

– діагностичне покриття;

– рівень повноти безпеки.

Для оцінювання зменшення впливу помилок та невизначеності в процесі XMECA призначена окрема групи метрик. Множину помилок позначається через E, а множина факторів невизначеності через U. На початковому етапі оцінювання відповідні множини позначаються E_0 та U_0.

Після виконання EUMECA формуються множини E_1 та U_1, які є відповідно підмножинами початкових множин:

$E_1 \subseteq E_0$;

$U_1 \subseteq U_0$.

Зменшення кількості помилок та факторів невизначеності оцінюється через відношення потужностей відповідних множин.

Загальна схема і приклад застосування удосконаленої моделі ілюструється рис.2.3.

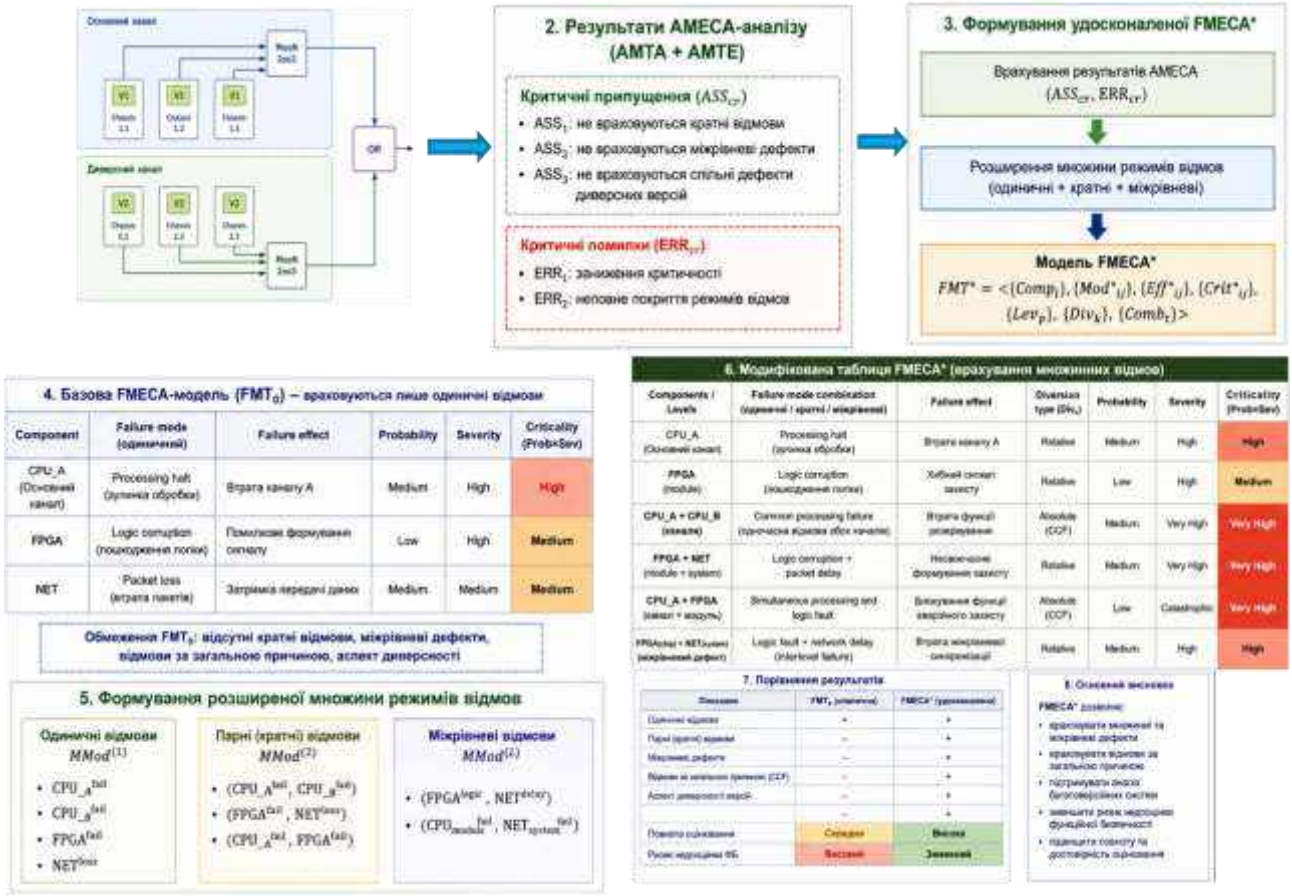


Рисунок 2.3 – Загальна схема і приклад застосування удосконаленої моделі FMECA

Показники для оцінювання представлено мають дворівневу структуру: на першому рівні надається узагальнена оцінка – метрики повноти для системи та двох методик (рис.2.4), на другому – вона деталізується з урахуванням різних множин і підмножин дефектів (рис.2.5).

Для системи

$$L_C = \frac{\text{Кількість перевірених вимог } (N_n)}{\text{Загальна кількість вимог } (N)}$$

Для FME(C,D)A

$$L_F = \frac{\text{Кількість проаналізованих дефектів } (n_{Fп})}{\text{Загальна кількість дефектів, які впливають на безпеку } (n_F)}$$

Для FIT

$$L_I = \frac{\text{Кількість ін'єктованих дефектів } (n_{In})}{\text{Загальна кількість дефектів, які впливають на безпеку } (n_I)}$$

Рисунок 2.4 – Узагальнений опис показників повноти оцінювання

Показник повноти FME(C,D)A

а) фізичні дефекти одиничні, рівень модуля

$$L_{F(d_{HW},d_{mod},d^{(1)}} == \frac{\sum_{i=1}^{n_{HW}} m_{HWi} - \sum_{j=1}^{\Delta n_{HW}} m_{HWj} - \sum_{i=1}^{n_{HW}} (m_{HWa} - \Delta m_{HWa} - \sum_{r=1}^{\Delta m_{HW2a}} q_{HWar})}{\sum_{i=1}^{n_{HW}} m_{HWi}} =$$

$$= \frac{N_{F(d_{HW},d_{mod},d^{(1)})п}}{N_{F(d_{HW},d_{mod},d^{(1)})}},$$

де: n_{HW} – кількість елементів модулю, які мають бути проаналізовано при оцінюванні безпечності;
m_{HWi} – кількість видів дефектів, які мають бути розглянуто для *i*–того елементу;
Δn_{HW} – кількість елементів модулю, які не були проаналізовано;
Δm_{HW1a} – кількість видів дефектів *a*-того елементу модулю, які не було проаналізовано;
Δm_{HW2a} – кількість видів дефектів a-того елементу модулю, для яких ризики (ймовірність, тяжкість) були визначено хибно;
q_{HWar} – імовірність хибного визначення ризиків відмов, обумовлених дефектами *a*-того елементу *r*-виду.

Рисунок 2.5 – Деталізація оцінки повноти для FME(C,A)

Використання даних показників повноти оцінювання надає змогу визначити ризики прихованих дефектів (РПД) та більш коректно і точно обчислити значення інтегральних показників функційної безпечності PFH (Probability of Dangerous Failure per Hour) та PFD (Probability of Failure on Demand) завдяки зменшення впливу РПД, врахуванню множинних відмов, міжрівневої взаємодії та помилок експертного оцінювання.

Кількісна оцінка підвищення повноти оцінювання визначається відносною кількістю ситуацій, які мають бути враховані при знятті відповідних припущень. Наприклад, відносною кількістю множинних дефектів (Nм) у порівнянні з сумою одиничних та множинних дефектів (Nм + Ns):

$$L = 1 - Nм / (Nм + Ns).$$

2.4. Висновки до розділу

1. Сформовано базову таблично-множинну модель FMECA/FMEDA для оцінювання функційної безпечності одноверсійних інформаційно-керуючих систем на програмовних платформах. Модель встановлює формальний зв’язок між компонентами системи, видами відмов, наслідками, імовірністю, тяжкістю, критичністю та діагностованістю відмов.

2. Розширено традиційне представлення FMECA/FMEDA з урахуванням особливостей програмовних платформ. До моделі включено апаратні, FPGA- та програмні компоненти, для яких сформовано узагальнену множину дефектів. Це дозволяє використовувати єдиний підхід до представлення дефектів різної природи та забезпечує їх простежуваність від рівня реалізації до відповідної функції безпеки.

3. Формалізовано таблично-множинне представлення множинних дефектів. Показано, що для оцінювання функційної безпечності програмовних платформ недостатньо розглядати лише одиничні види відмов, оскільки небезпечний стан системи може бути наслідком комбінації дефектів різних компонентів або рівнів реалізації.

4. Визначено множину припущень, що використовується під час формування та заповнення FMECA/FMEDA-таблиці. До неї віднесено припущення щодо повноти множин компонентів, видів відмов і наслідків, незалежності відмов, імовірності та тяжкості наслідків, діагностованості, резервування, незалежності версій, відмов за спільною причиною та результатів FIT. Показано, що такі припущення фактично є складовою моделі, на якій ґрунтується результуюча оцінка функційної безпечності.

5. Запропоновано підхід до визначення критичних припущень на основі їхнього впливу на результати FMECA/FMEDA. Для критичних припущень визначено необхідність додаткової перевірки із застосуванням документованих даних, повторного або незалежного експертного оцінювання, формального аналізу, моделювання, ін’єктування дефектів чи порівняння з

результатами випробувань. На цій основі FMECA-аналіз представлено як ітеративну процедуру уточнення початкової моделі.

6. Удосконалено модель FMECA/FMEDA шляхом формування розширеного представлення EFMECA, у якому забезпечується трасування залежностей між припущеннями, елементами FMECA та результуючою оцінкою безпечності. Це дозволяє встановлювати, які припущення вплинули на результати аналізу, та замінювати критичні неперевірені припущення підтвердженими даними або результатами додаткової перевірки.

7. Визначено основні показники, що використовуються для оцінювання функційної безпечності та повноти FMECA/FMEDA-аналізу: інтенсивність відмов, частка безпечних відмов, діагностичне покриття та рівень повноти безпеки. Показано, що повнота оцінювання характеризує охоплення суттєвих дефектів, видів відмов, рівнів системи, каналів, версій, діагностичних механізмів та небезпечних наслідків, тоді як достовірність пов’язана з обґрунтованістю та відтворюваністю отриманого результату.

8. Для оцінювання впливу експертних помилок і факторів невизначеності введено відповідні множини та визначено можливість оцінювання їх зменшення шляхом порівняння станів моделі до та після застосування процедур XMECA/EUMECA. Це створює основу для кількісного контролю ефективності подальших процедур експертного оцінювання.

9. Отримані результати формують математичну та інформаційну основу для розроблення в наступному розділі методу експертного оцінювання FMECA/FMEDA-FIT, у якому необхідно формалізувати множину експертів, експертних задач, можливих рішень, індивідуальних оцінок та процедур їх узгодження.

РОЗДІЛ 3.
МЕТОД ЕКСПЕРТНОГО ОЦІНЮВАННЯ FMECA/FMEDA-FIT

3.1. Постановка задачі експертного оцінювання FMECA/FMEDA-FIT

3.1.1. Особливості експертного оцінювання

Оцінювання безпечності експертами суттєво залежить від їх досвіду, заснованому на знаннях про особливості систем в цілому, можливі ризики в системах такого типу, типові відмови тощо [29]. На практиці експерт, як правило, якісно оцінює параметри безпечності, без явної та однозначної формалізації його міркувань на всіх етапах оцінювання [30].

Через те що більшість сучасних нормативних документів з безпечності вимагають імовірнісної оцінки ризику відмови, експерту доволі часто доводиться робити суб’єктивне оцінювання за відсутності повної всеохоплюючої моделі системи та достатньої кількості репрезентативних статистичних даних, що могли б бути використані як база для аналізу надійності та безпечності [31]. Однак безпосереднє вираження числових даних експертом іноді може призвести до упереджених значень. Такі упередження можуть бути обумовлені різними факторами [32]. Судження, винесені експертами на основі евристики, означають неофіційні міркування, що дозволяють експерту швидко отримати оцінку чи розрахунок, які необов’язково будуть найбільш точними та оптимальними [33]. У певній ситуації та для відповіді на конкретне запитання інформація експерта може бути основним джерелом інформації, але, з іншого боку, це також призводить до необхідності розроблення підходів до виявлення упередженості експерта та, якщо це можливо, до її зменшення [34-37].

Отже, вирішення задач експертного оцінювання, оброблення результатів експертного оцінювання на різних етапах тощо є актуальним.

На рисунку 3.1 представлено ролі, залучені до процесу експертного оцінювання, та потоки між цими ролями інформації.

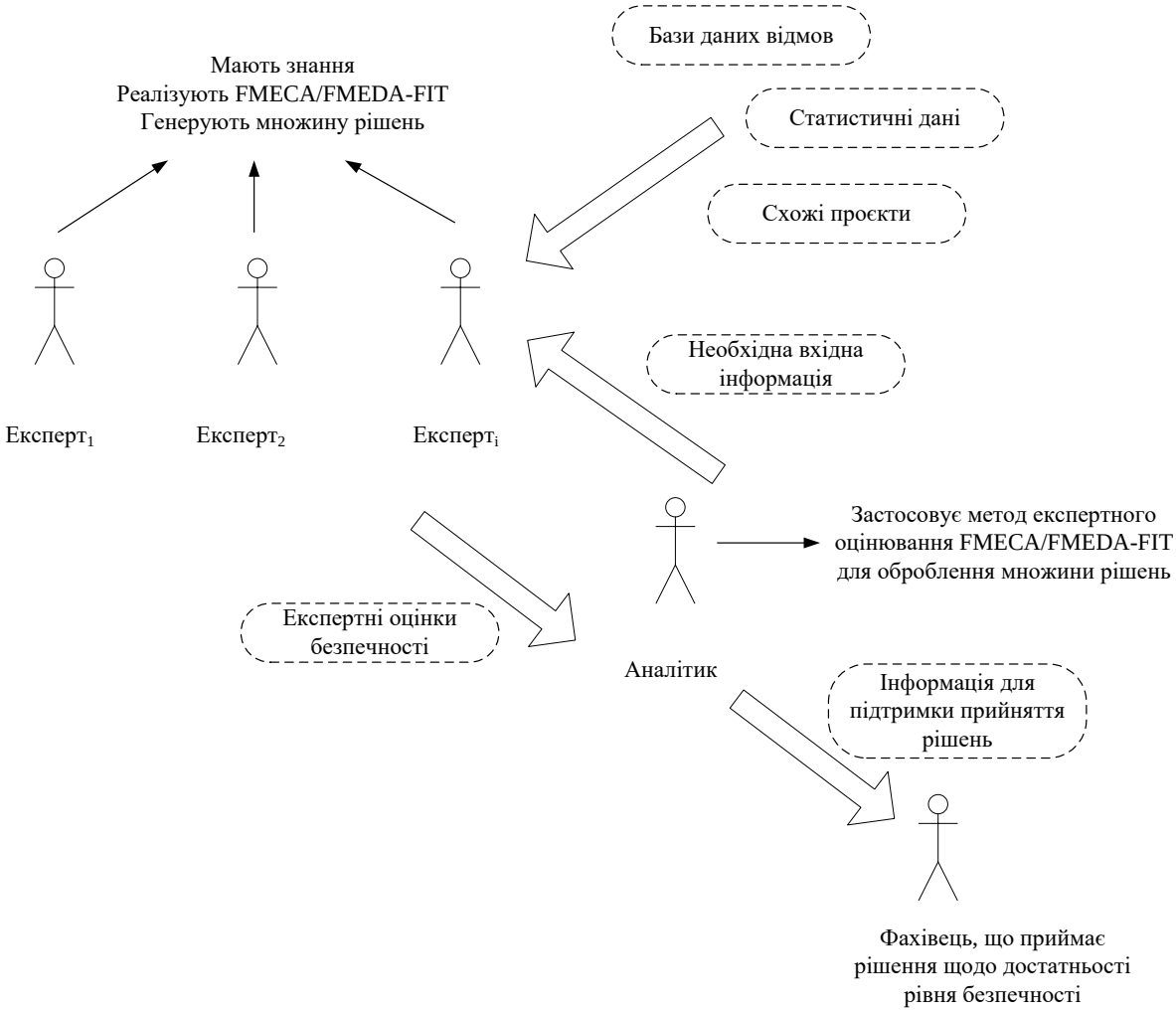


Рисунок 3.1 – Ролі, залучені до процесу експертного оцінювання, та потоки інформації

3.1.2. Задача експертного оцінювання FMECA/FMEDA (HW/FPGA, SW)

Задача оцінювання безпечності із застосуванням FMECA/FMEDA може бути вирішена множиною експертів E. Перед кожним експертом ставиться множина експертних задач ET, а для кожної експертної задачі існує множина рішень MS. Принципи та основні етапи експертного оцінювання за розробленим методом надано на рис. 3.2 і 3.3 відповідно.

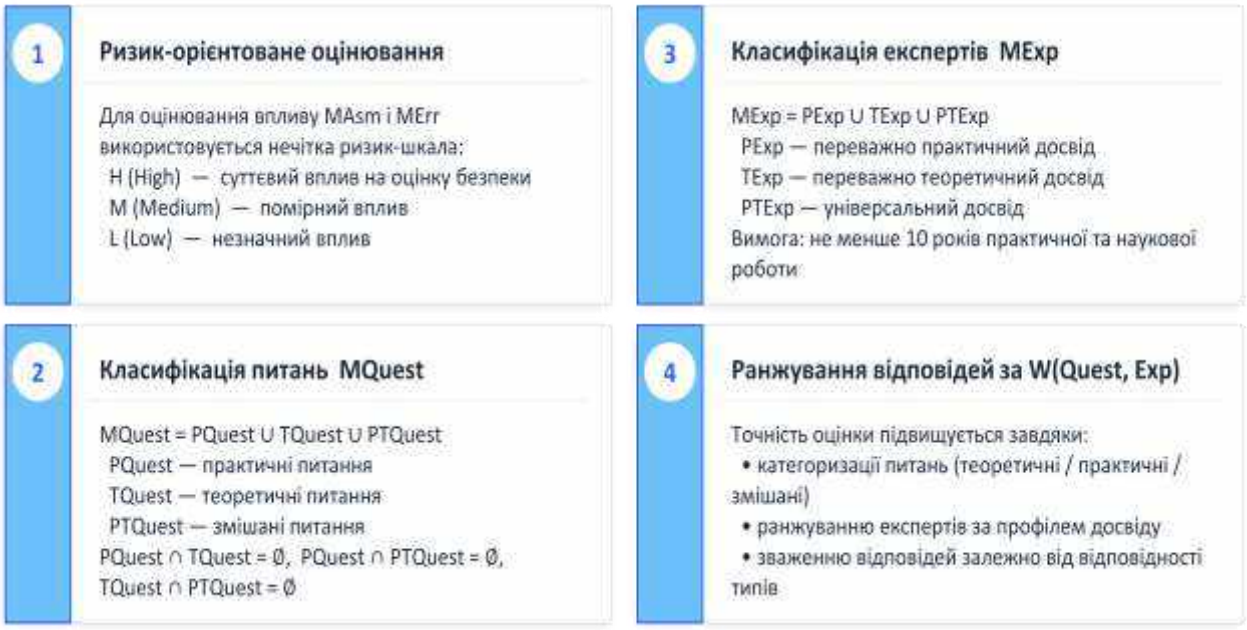


Рисунок 3.2 – Принципи експертного оцінювання за розробленим методом

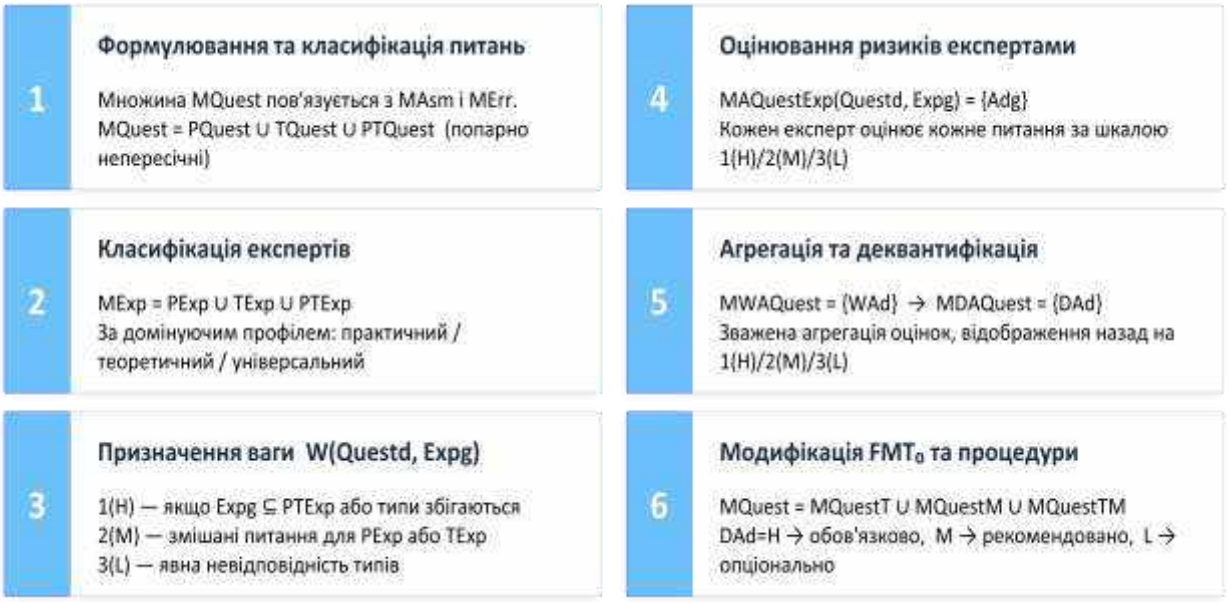


Рисунок 3.3 – Послідовність експертного оцінювання за розробленим методом

3.1.3. Задача експертного оцінювання FIT (HW/FPGA, SW)

Для виконання Multi-FIT оцінювання (рисунок 3.4) характеристик відмов та ефективності засобів їх виявлення не завжди може бути здійснено виключно автоматизованими засобами. Особливо це стосується характеристик, для визначення яких необхідні експертні знання щодо функціонування апаратних

засобів, FPGA-реалізації, програмного забезпечення, архітектури системи, механізмів діагностики та впливу відмов на виконання функцій безпеки.

Експертні рішення є одним із факторів, які можуть впливати на результати XMECA. Тому під час формування методу оцінювання доцільно формалізувати не тільки самі експертні оцінки, а й структуру експертних задач, множину можливих рішень та процедуру узгодження індивідуальних оцінок.

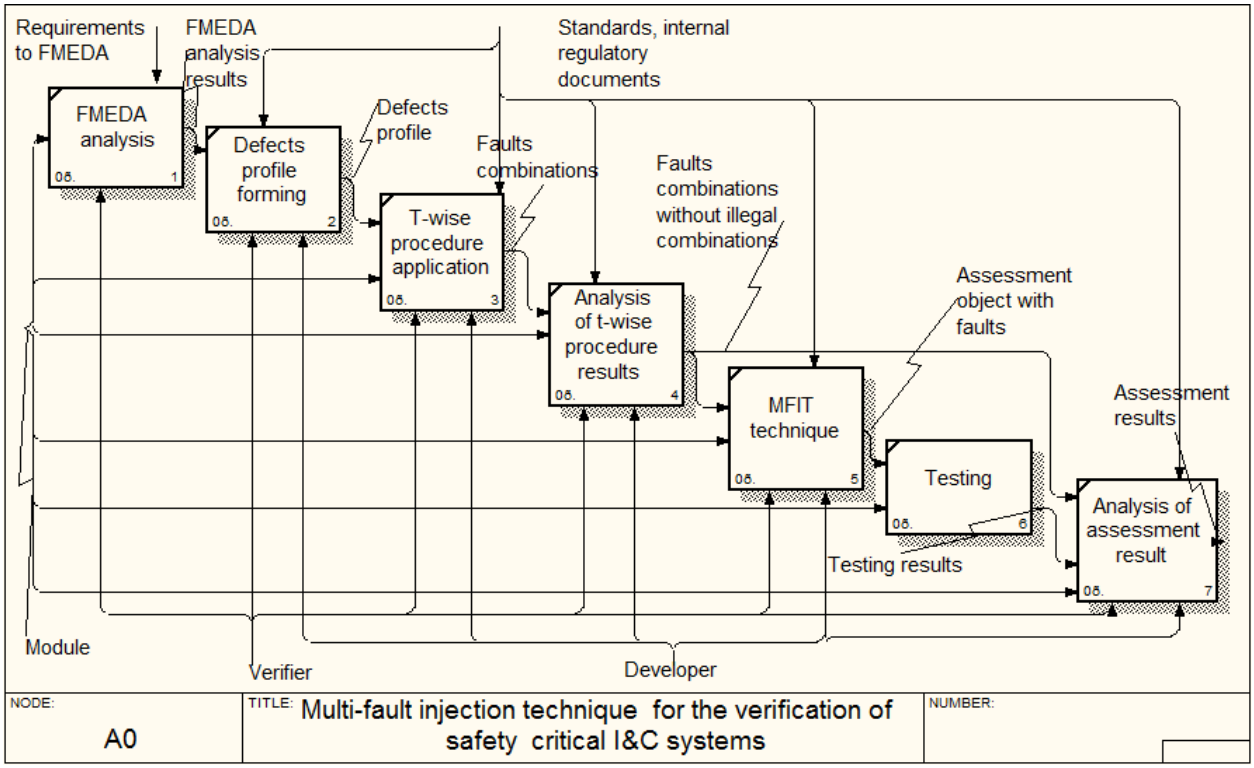


Рисунок 3.4 – Етапи виконання MultiFIT

3.2. Сценарії і процедури експертного оцінювання

3.2.1. Сценарії і процедури експертного оцінювання FMECA/FMEDA

У простішому випадку FMECA-таблицю можна представити як список FT_1, який є множиною з T кортежів:

$$FT_1 = <f_i, m_i = \{m_{ij}\}, e_i = \{e_{ij}\}, p_i = \{p_{ij}\}, s_i = \{s_{ij}\}, j = 1, \ldots, k_i >_{i=1}^{F}, \quad (3.1)$$

де f_i – елемент, що відмовив (причина відмови);

m_i – множина видів відмов; кількість видів відмов для елемента i дорівнює k_i; загальна кількість видів відмов

$K = k_1 + k_2 + \ldots + k_F$;

e_i – множина наслідків (проявів) відмов;

p_i, s_i – імовірність та тяжкість відмови відповідно, що можуть бути задані на нечіткій шкалі (наприклад, «висока» – «середня» – «низька»);

c_i – критичність відмови, $c_i = \varphi(p_i, s_i)$, що задається функцією нечітких змінних φ.

FMEDA-таблицю можна представити як список FT_2, який також є множиною з Т кортежів:

$$FT_2 = <f_i, m_i = \{m_{ij}\}, e_i = \{e_{ij}\}, d_i = \{d_{ij}\}, j = 1, \ldots, k_i >_{i=1}^{F}, \quad (3.2)$$

де f_i – елемент, що відмовив (причина відмови);

m_i – множина видів відмов; кількість видів відмов для елемента i дорівнює k_i; загальна кількість видів відмов

$K = k_1 + k_2 + \ldots + k_F$;

e_i – множина наслідків (проявів) відмов;

d_i – діагностованість відмови, що може бути задані на нечіткій шкалі (наприклад, «0%» – «90%» – «99%»);

c_i – критичність відмови, $c_i = \varphi(p_i, s_i)$, що задається функцією нечітких змінних φ.

Кількість рядків таблиці $F^* = F$, якщо $k_1 = k_2 = \ldots = k_F = 1$;

у загальному випадку $F^* = K$.

Під час виконання FMECA/FMEDA аналізу експерт послідовно визначає:

– елементи f_i (компоненти модуля, оператори програми, операції процесів,…), відмови яких мають бути враховані, тобто $f_i \in \Delta F$, $\Delta F \subset MF$, де MF – множина компонентів; ΔF – підмножина компонентів, що враховуються;

– види відмов m_{ij} елемента f_i, які мають бути враховані, тобто $m_{ij} \in \Delta M_i$, $\Delta M_i \subset MM_i$, де ΔM_i – множина видів відмов елемента, що враховуються f_i; MM_i – множина усіх видів відмов елемента f_i;

– наслідки e_{ij} відмови виду m_{ij} елементу f_i, які мають бути описані, тобто $e_{ij} \in \Delta E_i$, $\Delta E_i \subset ME_i$, де ΔE_i – множина наслідків відмов елемента f_{ii}, визначених експертом для виду відмов, що враховується m_{ij}; ME_i – множина усіх можливих наслідків для даного виду відмов даного елементу;

– імовірність та тяжкість відмови виду m_{ij} елементу f_i; імовірність p_{ij} обирається згідно з встановленою шкалою на множині значень $MP = \{p'_h\}$; тяжкість s_{ij} обирається згідно з встановленою шкалою на множині значень $MS = \{s'_g\}$;

– критичність c_{ij} відмови виду m_{ij} елементу f_i, яка або однозначно обчислюється експертом згідно з заданою функцією φ, або визначається ним самостійно на множині значень $MC = \{c'_g\}$.

3.2.1.1. Оцінювання за умови однакової кваліфікації (самооцінки) експертів

Якщо FMECA/FMEDA-оцінювання виконується групою з Q експертів, кваліфікація яких є ідентичною або не враховується, для оцінювання суджень різних експертів необхідно:

1) проаналізувати види розходжень, що відносяться до різних елементів моделей (3.1) та (3.2);

2) сформувати підсумковий варіант для кожного з розходжень;

3) отримати об'єднаний варіант FMECA/FMEDA;

4) провести її аналіз та дати остаточну оцінку безпеки.

3.2.1.2. Аналіз видів розходжень

При FMECA/FMEDA оцінюванні групою з Q експертів можливі такі розходження:

– визначені різні множини елементів f_i, відмови яких мають бути враховані, тобто маємо множину $M\Delta F$ множин $\Delta F^{(q)}$, $q = 1,\ldots, Q$, де $\Delta F^{(q)}$ – множина елементів, відмови яких враховуються q-м експертом;

– визначені різні множини видів відмов m_{ij} елементу f_i, які мають бути враховані, тобто маємо множину $M\Delta M_i$ множин $\Delta M_i{}^{(q)}$, причому для усіх q,

$\Delta M_i^{(q)}$ *с* MM_i, де $\Delta M_i^{(q)}$ – множина видів відмов елемента f_i, що враховуються q-м експертом;

– визначені різні множини наслідків e_{ij} відмови виду m_{ij} елементу f_i, що мають бути описані, тобто маємо множину $M\Delta E_i$ множин $\Delta E_i^{(q)}$, причому для усіх q, $\Delta E_i^{(q)}$ *с* ME_i, де $\Delta E_i^{(q)}$ – множина наслідків відмов елементу f_i, що враховуються q-м експертом;

– визначені різні імовірності відмов виду m_{ij} елементу f_i, тобто маємо множину $M\Delta P_{ij}$ множин $\Delta P_{ij}^{(q)}$, причому для усіх q, $\Delta P_{ij}^{(q)}$ *с* MP, де $\Delta P_{ij}^{(q)}$ – множина імовірностей відмов виду m_{ij} елементу f_i,, що враховуються q-м експертом;

– визначені різні тяжкості відмов виду m_{ij} елементу f_i, тобто маємо множину $M\Delta S_i$ множин $\Delta S_i^{(q)}$, причому для усіх q, $\Delta S_i^{(q)}$ *с* MS, де $\Delta S_i^{(q)}$ – множина тяжкостей відмов елементу f_i,, що враховуються q-м експертом;

– визначені різні критичності відмов виду m_{ij} елемента f_i, тобто маємо множину $M\Delta C_i$ множин $\Delta C_i^{(q)}$, причому для усіх q, $\Delta C_i^{(q)}$ *с* MC, критичність або однозначно обчислюється q-м експертом згідно з заданою функцією φ, або визначається ним самостійно. Ці два випадки можуть розглядатися окремо.

При цьому вважаємо справедливими припущення про те, що, по-перше, множини $M\Delta F, M\Delta M_i$ та $M\Delta E_i$ цілком покривають усі можливі судження експертів, та, по-друге, шкали (значення) для оцінювання імовірностей, тяжкостей та критичності відмов MP, MS та MC є спільними та не можуть змінюватися при оцінюванні.

3.2.1.3. Формування об’єднаної експертної оцінки

Можливі три сценарії оцінювання на базі суджень експертів:

– консервативний (ScC), коли формується найбільш повний обсяг видів відмов, а оцінювання наслідків та ризиків здійснюється за песимістичним варіантом;

– оптимістичний (ScO), коли формується мінімальний обсяг варіантів на базі перетину множин видів відмов, а при оцінюванні наслідків та ризиків обираються найкращі оцінки;

– зважений (ScW), коли формується спільна підмножина відмов та доповнюється такими видами, які сформували два та більше експертів; для оцінювання наслідків та ризиків обчислюються усереднені показники.

Сценарій ScC. У даному випадку маємо такі оцінки:

– множина елементів, відмови яких мають бути включені до таблиці згідно з (4.1) або (4.2) визначається формулою:

$$M\Delta F(ScC) = \mathrm{U}\Delta F^{(q)},\ q = 1,\ldots,\ Q;$$

– множини видів відмов для усіх елементів $f_i \in M\Delta F(ScC)$, які мають бути враховані згідно з формулою:

$$M\Delta M_i(ScC) = \mathrm{U}\Delta M_i^{(q)},\ q = 1,\ldots,\ Q;$$

– множини наслідків відмов e_{ij} виду m_{ij} елементу f_i, які мають бути враховані, представлені як:

$$M\Delta E_i(ScC) = \mathrm{U}\Delta E_i^{(q)},\ q = 1,\ldots,\ Q;$$

– імовірності відмов виду m_{ij} елементу f_i мають бути обчислені за формулою:

$$p_{ij}(ScC) = \max\ \{\Delta P_{ij}^{(q)}\}\ ,\ q = 1,\ldots,\ Q;$$

– тяжкості відмов виду m_{ij} елементу f_i можуть бути описані виразом:

$$s_{ij}(ScC) = \max\ \{\Delta S_{ij}^{(q)}\}\ ,\ q = 1,\ldots,\ Q;$$

– критичності відмов виду m_{ij} елементу f_i мають бути обчислені за формулою:

$$c_{ij}(ScC) = \max\ \{\Delta C_{ij}^{(q)}\}\ ,\ q = 1,\ldots,\ Q.$$

Сценарій ScO. У даному випадку застосовуються такі вирази:

– множина елементів, відмови яких мають бути включені до таблиці згідно з (4.1) або (4.2), визначається формулою:

$$M\Delta F(ScO) = \cap\Delta F^{(q)},\ q = 1,\ldots,\ Q;$$

– множини видів відмов для усіх елементів $f_i \in M\Delta F(ScO)$, які мають бути враховані згідно з формулою:

$$M\Delta M_i(ScO) = \cap \Delta M_i^{(q)},\ q = 1,\ldots,\ Q;$$

– множини наслідків e_{ij} відмов виду m_{ij} елемента f_i, які мають бути враховані, представлені як:

$$M\Delta E_i(ScO) = \cap \Delta E_i^{(q)},\ q = 1,\ldots,\ Q;$$

– імовірності відмов виду m_{ij} елемента f_i мають бути обчислені за формулою:

$$p_{ij}(ScO) = \min \{ \Delta P_{ij}^{(q)} \},\ q = 1,\ldots,\ Q;$$

– тяжкості відмов виду m_{ij} елементу f_i можуть бути описані виразом:

$$s_{ij}(ScO) = \min \{ \Delta S_{ij}^{(q)} \},\ q = 1,\ldots,\ Q;$$

– критичності відмов виду m_{ij} елементу f_i мають бути обчислені за формулою:

$$c_{ij}(ScO) = \min \{ \Delta C_{ij}^{(q)} \},\ q = 1,\ldots,\ Q.$$

Сценарій ScW. У даному випадку маємо такі оцінки:

– множина елементів, відмови яких мають бути включені до таблиці згідно з (4.1) або (4.2) визначається формулою:

$$M\Delta F(ScW) = \cap \Delta F^{(q)} \cup \Delta F^{(q)\,*},\ q = 1,\ldots,\ Q,$$

де $\Delta F^{(q)\,*}$ – множина елементів, відмови яких враховані двома та більш експертами;

– множини видів відмов для усіх елементів $f_i \in M\Delta F(ScW)$, які мають бути враховані згідно з формулою:

$$M\Delta M_i(ScW) = \cap \Delta M_i^{(q)} \cup \Delta M_i^{(q)\,*},\ q = 1,\ldots,\ Q,$$

де $\Delta M_i^{(q)\,*}$ – множина видів відмов елементів, які враховані двома та більш експертами;

– множини наслідків e_{ij} відмов виду m_{ij} елементу f_i, які мають бути враховані, представлені як:

$$M\Delta E_i(ScW) = \cap \Delta E_i^{(q)} \cup \Delta E_i^{(q)\,*},\ q = 1,\ldots,\ Q,$$

де $\Delta E_i^{(q)*}$ – множина наслідків відмов елементів, які враховані двома та більш експертами;

– імовірності відмов виду m_{ij} елементу f_i мають бути обчислені за формулою середнього, округленого до найближчого більшого:

$$p_{ij}(ScW) = \text{avermax}\{\Delta P_{ij}^{(q)}\},\ q = 1,\ldots, Q;$$

– тяжкості відмов виду m_{ij} елементу f_i можуть бути описані виразом:

$$s_{ij}(ScW) = \text{avermax}\{\Delta S_{ij}^{(q)}\},\ q = 1,\ldots, Q;$$

– критичності відмов виду m_{ij} елементу f_i мають бути обчислені за формулою:

$$c_{ij}(ScW) = \text{avermax}\{\Delta C_{ij}^{(q)}\},\ q = 1,\ldots, Q.$$

3.2.1.4 Оцінювання за умови різної кваліфікації (самооцінки) експертів

Якщо FMECA/FMEDA оцінювання виконується групою з Q експертів, кваліфікація (самооцінка) яких є різною та враховується, для оцінювання суджень різних експертів необхідно до розглянутих сценаріїв ScC, ScO, ScW додати сценарії множини MScD. Серед них запропонуємо такі:

Сценарії ScDT. Сценарії даної групи базуються на відкиданні оцінок, які надаються експертами з мінімальною або заданою (пороговою) кваліфікацією, та подальшим переходом до реалізації одного з сценаріїв ScC, ScO, ScW, які перетворюються у сценарії ScTC, ScTO, ScTW, коли кваліфікація експертів вже не враховується.

Сценарії ScDW. Сценарії даної групи базуються на сценарії консервативного оцінювання ScC у частині формування множин $M\Delta F(ScC)$, $M\Delta M_i(ScC)$ та $M\Delta E_i(ScC)$ та подальших зважених оцінок імовірності, тяжкості та критичності відмов з округленням у бік максимальних значень.

3.3 Удосконалення FMECA (XMECA)-процедур оцінювання безпеки

3.3.1 Основні принципи

У контексті аналізу безпеки складних систем, важливе значення має точне оцінювання ризиків, пов’язаних з можливими відмовами. Для оцінювання критичності впливу припущень з множини MAsm і помилок з множини MErr, пропонується використовувати нечітку шкалу ризиків, яка включає три рівні: 1 – високий (H, High), 2 – середній (M, Medium), і 3 – низький (L, Low). Такий підхід дозволяє врахувати непевність та варіативність впливу окремих факторів на загальну безпеку системи, забезпечуючи гнучкий та інтуїтивно зрозумілий інструментарій для визначення їх значення.

Другим ключовим компонентом у процесі оцінювання ризиків виступає експертне оцінювання. Для цього сформовано групу фахових експертів, які мають не менше десяти років практичної та наукової роботи в галузі безпеки інформаційних та комунікаційних систем (ІКС). Наявність такого значного досвіду забезпечує високий рівень об'єктивності та точності в оцінці ризиків. Для забезпечення високої точності (об’єктивності) оцінювання ризиків пропонується:

а) виконати диференціацію запитань стосовно визначення впливу припущень і помилок на групи залежно від їх спрямованості і особливостей;

б) визначати ранги (вагу) експертів з врахуванням пріоритетності їх теоретичного і практичного досвіду;

в) визначати вагу відповіді на кожне запитання з врахуванням їх типу та спрямованості досвіду експертів (рис. 3.5).

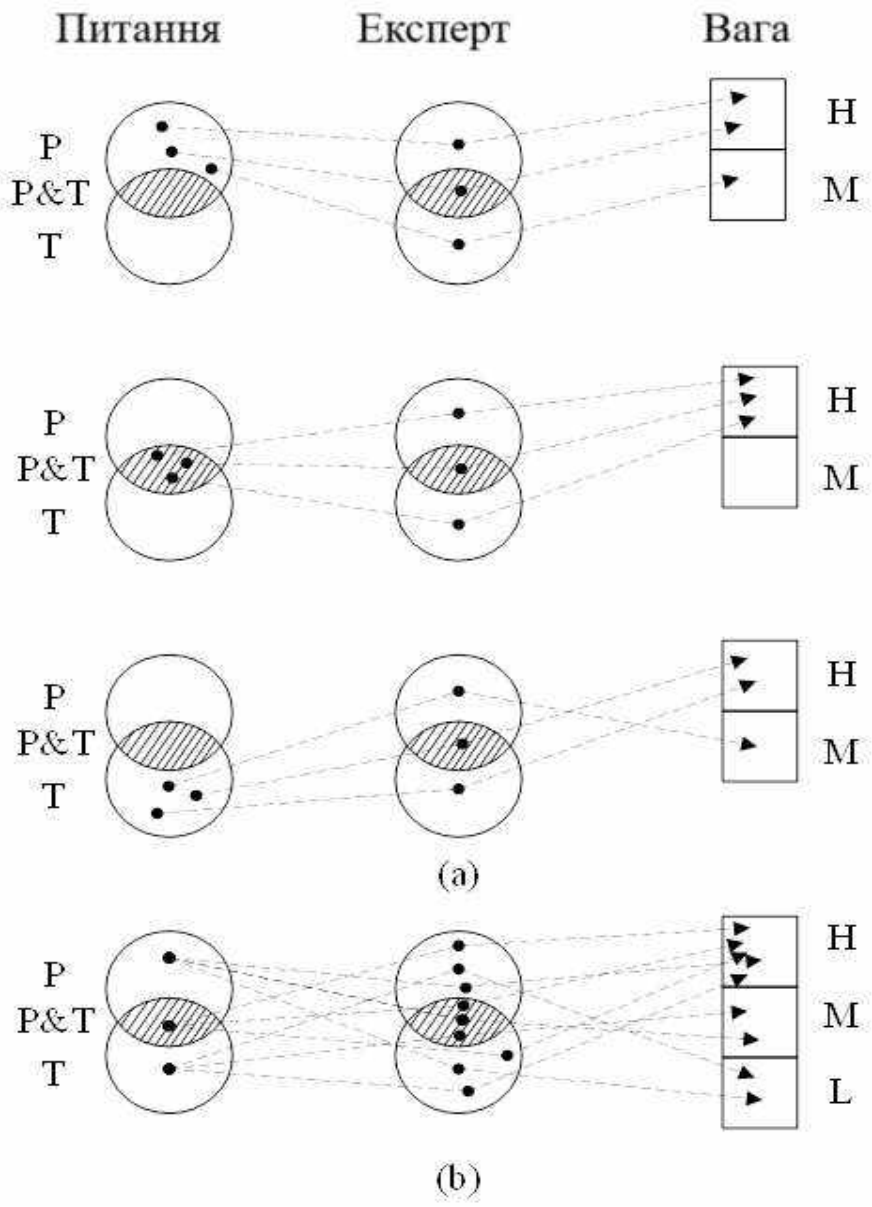


Рисунок 3.5 – Дво- та трирівневе ранжування експертів

Запропоновані принципи модифікації FMECA-таблиці з урахуванням критичності припущень та помилок забезпечують більш точний і гнучкий підхід до оцінювання ризиків. Динамічне адаптування експертних оцінок та використання нечіткої шкали ризиків дозволяє враховувати різноманітні аспекти впливу, тим самим підвищуючи загальний рівень безпеки і надійності аналізованих систем та сприяючи більш обґрунтованим рішенням з безпеки. Це, в свою чергу, надає можливість ефективного управління ризиками в умовах постійно змінного середовища технологій.

3.3.2. Послідовність (етапи)

Запропонований метод має такі етапи:

1) Формування і диференціація множини запитань, пов'язаних з множинами припущень MAsm і помилок MErr:

$MQuest = \{Quest_d\}$, $d = 1,\ldots,q$;

$MQuest = PQuest \cup TQuest \cup PTQuest$,

$PQuest \cap TQuest = \varnothing$, $PQuest \cap PTQuest = \varnothing$, $TQuest \cap PTQuest = \varnothing$,

де PQuest, TQuest, PTQuest – підмножини запитань практичного, теоретичного і змішаного спрямування.

2) Ранжування експертів з врахуванням пріоритетності практичного і теоретичного досвіду:

$MExp = \{Exp_g\}$, $g = 1,\ldots,h$;

$MExp = PExp \cup TExp \cup PTExp$,

$PExp \cap TExp = \varnothing$, $PExp \cap PTExpt = \varnothing$, $TExp \cap PTExp = \varnothing$,

де PExp, TExp, PTExp – підмножини експертів з більшим практичним, теоретичним і універсальним досвідом.

3) Формування ваги (рангу) експертів залежно від множин MQuest і MExp за шкалою:

1 (H), 2 (M), 3 (L) відповідно до правил (ілюструється рисунком 4.1):

$W(Quest_d, Exp_g) = H$, якщо $Exp_g \in PTExp$ незалежно від типу запитань, або

якщо $Quest_d \in PQuest$ і $Exp_g \in PExp$, або якщо $Quest_d \in TQuest$ і $Exp_g \in TExp$;

$W(Quest_d, Exp_g) = M$, якщо $Quest_d \in TPQuest$ і $Exp_g \in PExp \cup TExp$;

$W(Quest_d, Exp_g) = L$, якщо $Quest_d \in TQuest$ і $Exp_g \in PExp$ або якщо $Quest_d \in PQuest$ і $Exp_g \in TExp$.

4) Оцінювання експертами ризиків припущень MAsm і помилок MErr, формування множини оцінок за шкалою 1 (H), 2 (M), 3 (L):

$MAQuestExp(Quest_d, Exp_g) = \{A_{dg}\}$.

5) Формування множини значень загальних (квантифікованих) зважених оцінок:

MWAQuest = {WA_d}

та їх деквантифікація за шкалою 1 (H), 2 (M), 3 (L) і формування множини

MDAQuest = {DA_d}

6) Визначення варіантів модифікації FMT_0 та методу FMECA аналізу з врахуванням критичності впливу припущень з множини MAsm і помилок з множини MErr на результат оцінювання безпеки відповідно до множини MDAQuest:

- уточнення об'єкту модифікації – таблиці FMT_0 або послідовності методу FMECA. Для цього множина MQuest розділяється на підмножини на запитання, які можуть вимагати зміни таблиці MQuestT, послідовності методу MQuestM і зміни таблиці та послідовності MQuestTM:

MQuest = MQuestT U MQuestM U MQuestTM;

- уточнення типу модифікації для підмножин MQuestT, MQuestM, MQuestTM

- визначення рівня обов'язковості модифікації за правилом:

а) модифікація за запитанням $Quest_d$ обов'язкова, якщо DA_d = H;

б) модифікація за запитанням $Quest_d$ бажана, якщо DA_d = M;

в) модифікація за запитанням $Quest_d$ опціональна, якщо DA_d = L;

- проведення модифікації таблиці FMT_0 і відповідна зміна послідовності FMECA аналізу;

- проведення модифікації послідовності FMECA аналізу без зміни таблиці FMT_0.

3.3.3. Приклад використання

Таблиця 3.1 містить перелік помилок, а також можливі наслідки на результуючу оцінку функційної безпечності.

Таблиця 3.1 – Диференціація питань у частині наслідків на оцінку функційної безпечності

Види помилок	**Наслідки**
Не усі компоненти визначено для оцінки ФБ	Ризики переоцінки ФБ
Кількість компонентів, визначених для оцінки ФБ завищена	Ризики недооцінки ФБ
Не усі види відмов розглядаються	Ризики переоцінки ФБ
Розглядаються зайві види відмов	Ризики недооцінки ФБ
Критичність відмов (ймовірність, тяжкість) занижена	Ризики переоцінки ФБ
Критичність відмов (ймовірність, тяжкість) завищена	Ризики недооцінки ФБ
Відмова хибно визначається як така, що детектується засобами контролю	Ризики переоцінки ФБ
Відмова хибно визначається як така, що не детектується засобами контролю	Ризики недооцінки ФБ
Кратність відмов занижена	Ризики переоцінки ФБ
Кратність відмов завищена	Ризики недооцінки ФБ
Не розглядаються кратні дефекти різних компонентів одного рівня	Ризики переоцінки ФБ
Не розглядаються кратні дефекти компонентів різних рівнів	Ризики переоцінки ФБ
Не розглядаються кратні дефекти різних версій	Ризики переоцінки ФБ
Не всі рівні розглядаються	Ризики переоцінки ФБ
Розглядаються зайві рівні	Ризики недооцінки ФБ
Не враховується взаємодія між рівнями	Ризики переоцінки ФБ
Враховуються зайві взаємодії	Ризики недооцінки ФБ
Не всі дефекти ПЗ враховуються	Ризики переоцінки ФБ
Взято до уваги більше ніж потрібно дефектів ПЗ	Ризики недооцінки ФБ
Не всі дефекти апаратні враховуються (фізичні та проектні)	Ризики переоцінки ФБ
Взято до уваги більше ніж потрібно апаратних дефектів (фізичні та проектні)	Ризики недооцінки ФБ
Не розглядаються апаратні та програмні дефекти з точки зору атак	Ризики переоцінки ФБ

Рисунки 3.6, 3.7 ілюструють результати проведеного опитування експертів та оцінки критичності припущень і помилок відповідно до результатів використання програмного засобу (надано з використанням інтерфейсу розробленої програми).

Тест-опитування на тему впливу різних факторів на коректність і повноту оцінки функційної безпеки

*розставте в кожному пункті опитування ймовірність (від 1 до 3, де 1 - сама висока ймовірність) та їх тяжкість (1-3, де 1 - сама висока тяжкість);

ризики недооцінки - ризики ситуації, коли дійсний рівень небезпеки буде вищий за визначений, ризики переоцінки - коли дійсний рівень небезпеки буде нижчий за визначений;

Assumptions, limitations (припущення, обмеження)	Modes (види помилок)	Effects (наслідки)	Бабенко		Одинцова		Панарін		Куланов		Коваленко		СТОЮ		Харитонов		Бриннев		Андрашов		Лучков	
			Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)	Probability (Ймовірність)	Severity (Тяжкість)
Експертна оцінка (Expert assessment)	Не усі компоненти визначено для оцінки ФБ	Ризики переоцінки ФБ	2	3	2	1	1	1	1	2	2	2	1	1	3	1	3	3	3	1	3	1	2	3
	Кількість компонентів, визначених для оцінки ФБ завищена	Ризики недооцінки ФБ	3	3	2	2	3	3	3	3	2	2	2	2	3	3	2	2	3	1	2	2	2	3
	Не усі види відмов розглядаються	Ризики переоцінки ФБ	1	1	1	1	1	1	2	2	1	2	1	2	2	1	2	2	2	2	2	1	1	1
	Розглядаються зайві види відмов	Ризики недооцінки ФБ	3	3	1	2	3	3	3	3	2	2	3	3	3	3	1	2	2	2	2	3	3	3
	Критичність відмов (ймовірність, тяжкість) занижена	Ризики переоцінки ФБ	3	2	1	1	2	2	2	2	2	2	1	1	2	1	3	2	2	1	2	2	3	2
	Критичність відмов (ймовірність, тяжкість) завищена	Ризики недооцінки ФБ	3	3	1	2	3	3	2	2	2	2	2	2	3	3	2	3	2	1	2	2	3	3
	Відмова хибно визначається як така, що детектується засобами контролю	Ризики переоцінки ФБ	3	2	2	2	3	3	2	1	2	2	1	1	3	1	2	2	3	2	2	1	3	2
	Відмова хибно визначається як така, що не детектується засобами контролю	Ризики недооцінки ФБ	3	3	2	2	1	1	2	2	2	2	2	2	3	3	1	2	3	1	2	3	3	3
Одиничні/кратні дефекти (Single/multiple faults)	Кратність відмов занижена	Ризики переоцінки ФБ	1	2	1	1	3	3	1	1	1	1	1	1	2	1	2	2	2	1	2	1	1	2
	Кратність відмов завищена	Ризики недооцінки ФБ	1	2	1	2	3	3	2	2	2	2	3	3	2	3	2	2	2	2	2	1	1	2
	Не розглядаються кратні дефекти різних компонентів одного рівня	Ризики переоцінки ФБ	3	2	1	1	3	3	2	2	1	1	1	1	2	1	2	2	2	1	2	2	3	2
	Не розглядаються кратні дефекти компонентів різних рівнів	Ризики переоцінки ФБ	2	2	1	2	3	3	2	2	1	1	1	1	2	3	2	2	2	2	2	2	2	2
	Не розглядаються кратні дефекти різних версій	Ризики переоцінки ФБ	1	3	1	1	3	3	1	2	2	2	2	2	2	1	2	3	2	2	2	1	1	3
Рівні технічних засобів (System levels)	Не всі рівні розглядаються	Ризики переоцінки ФБ	2	3	3	2	1	1	2	3	1	1	1	1	3	1	3	3	3	1	3	1	2	3
	Розглядаються зайві рівні	Ризики недооцінки ФБ	3	3	3	2	3	3	2	3	2	2	2	2	3	3	1	2	2	3	3	2	3	3
	Не враховується взаємодія між рівнями	Ризики переоцінки ФБ	3	2	1	2	1	1	1	2	1	2	3	2	3	1	2	2	1	1	2	2	2	2
	Враховуються зайві взаємодії	Ризики недооцінки ФБ	3	3	2	2	3	3	2	3	2	3	3	3	3	3	1	1	2	2	2	2	3	3
Типи дефектів (Types of faults)	Не всі дефекти ПЗ враховуються	Ризики переоцінки ФБ	2	3	1	3	3	3	1	1	1	1	1	1	2	2	2	3	2	1	2	1	2	3
	Взято до уваги більше ніж потрібно дефектів ПЗ	Ризики недооцінки ФБ	3	3	1	3	3	3	2	3	3	3	2	2	3	3	1	2	2	1	3	3	3	3
	Не всі дефекти апаратні враховуються (фізичні та проектні)	Ризики переоцінки ФБ	2	2	2	2	3	3	1	1	1	1	1	1	2	1	3	3	2	1	2	1	2	2
	Взято до уваги більше ніж потрібно апаратних дефектів (фізичні та проектні)	Ризики недооцінки ФБ	3	3	2	2	3	3	2	3	3	3	1	2	3	3	1	2	1	3	2	3	3	3
	Не розглядаються апаратні та програмні дефекти з точки зору атак	Ризики переоцінки ФБ	2	2	1	3	3	3	2	2	2	2	1	3	1	2	3	1	1	2	1	2	2	2

Рисунок 3.6 – Результати опитування експертів

Assumptions, limitations (припущення, обмеження)	Modes (види помилок)	Effects (наслідки)	Dad	Ризик	Необх. оновл. FMECA
Експертна оцінка (Expert assessment)	Не усі компоненти визначено для оцінки ФБ	Ризики переоцінки ФБ	2,64	H	Обов'язково
	Кількість компонентів, визначених для оцінки ФБ завищена	Ризики недооцінки ФБ	3,18	M	Опційно
	Не усі види відмов розглядаються	Ризики переоцінки ФБ	2,00	H	Обов'язково
	Розглядаються зайві види відмов	Ризики недооцінки ФБ	4,09	M	Опційно
	Критичність відмов (ймовірність, тяжкість) занижена	Ризики переоцінки ФБ	2,73	H	Обов'язково
	Критичність відмов (ймовірність, тяжкість) завищена	Ризики недооцінки ФБ	3,27	M	Опційно
	Відмова хибно визначається як така, що детектується засобами контролю	Ризики переоцінки ФБ	3,09	M	Опційно
	Відмова хибно визначається як така, що не детектується засобами контролю	Ризики недооцінки ФБ	3,27	M	Опційно
Одиничні/кратні дефекти (Single/multiple faults)	Кратність відмов занижена	Ризики переоцінки ФБ	1,55	H	Обов'язково
	Кратність відмов завищена	Ризики недооцінки ФБ	2,82	H	Обов'язково
	Не розглядаються кратні дефекти різних компонентів одного рівня	Ризики переоцінки ФБ	2,18	H	Обов'язково
	Не розглядаються кратні дефекти компонентів різних рівнів	Ризики переоцінки ФБ	2,45	H	Обов'язково
	Не розглядаються кратні дефекти різних версій	Ризики переоцінки ФБ	2,55	H	Обов'язково
Рівні технічних засобів (System levels)	Не всі рівні розглядаються	Ризики переоцінки ФБ	3,55	M	Опційно
	Розглядаються зайві рівні	Ризики недооцінки ФБ	4,27	M	Опційно
	Не враховується взаємодія між рівнями	Ризики переоцінки ФБ	2,27	H	Обов'язково
	Враховуються зайві взаємодії	Ризики недооцінки ФБ	3,82	M	Опційно
Типи дефектів (Types of faults)	Не всі дефекти ПЗ враховуються	Ризики переоцінки ФБ	2,64	H	Обов'язково
	Взято до уваги більше ніж потрібно дефектів ПЗ	Ризики недооцінки ФБ	4,18	M	Опційно
	Не всі дефекти апаратні враховуються (фізичні та проектні)	Ризики переоцінки ФБ	2,18	H	Обов'язково
	Взято до уваги більше ніж потрібно апаратних дефектів (фізичні та проектні)	Ризики недооцінки ФБ	4,18	M	Опційно
	Не розглядаються апаратні та програмні дефекти з точки зору атак	Ризики переоцінки ФБ	2,73	H	Обов'язково

Рисунок 3.7 – Результати оцінки критичності припущень і помилок

Логіка прийняття рішень в цілому ілюструється рисунком 3.8.

Рисунок 3.8 – Логіка прийняття рішень

3.4. Послідовність оцінювання FMECA-FTA

3.4.1. Загальний алгоритм

Запропонований метод полягає у такій послідовності кроків:

Крок 1. Формування експертних суджень

Крок 2. Оброблення експертних суджень

Крок 3. Формування узгодженої експертної оцінки відповідно до обраного сценарію (консервативного, оптимістичного або зваженого).

Крок 4. Розрахунок показників функційної безпечності та формування підсумкового висновку щодо відповідності системи встановленим вимогам.

Алгоритм методу представлений на рисунку 3.9.

3.4.2. Створення опитувальників та автоматизація оброблення результатів

Автоматизація експертного оцінювання спрямована на зменшення обсягу ручної роботи під час підготовки експертних задач, збору індивідуальних оцінок, перевірки повноти отриманих відповідей, їх структурування та подальшого формування узгоджених результатів.

Приклад опитувальника наведено у Додатку В. Автоматизоване оброблення використовувалось для перевірки коректності отриманих даних.

Для кожної відповіді перевірялось:

– наявність відповіді;

– відповідність значення відповіді множині допустимих відповідей;

– завершеність експертного опитувальника.

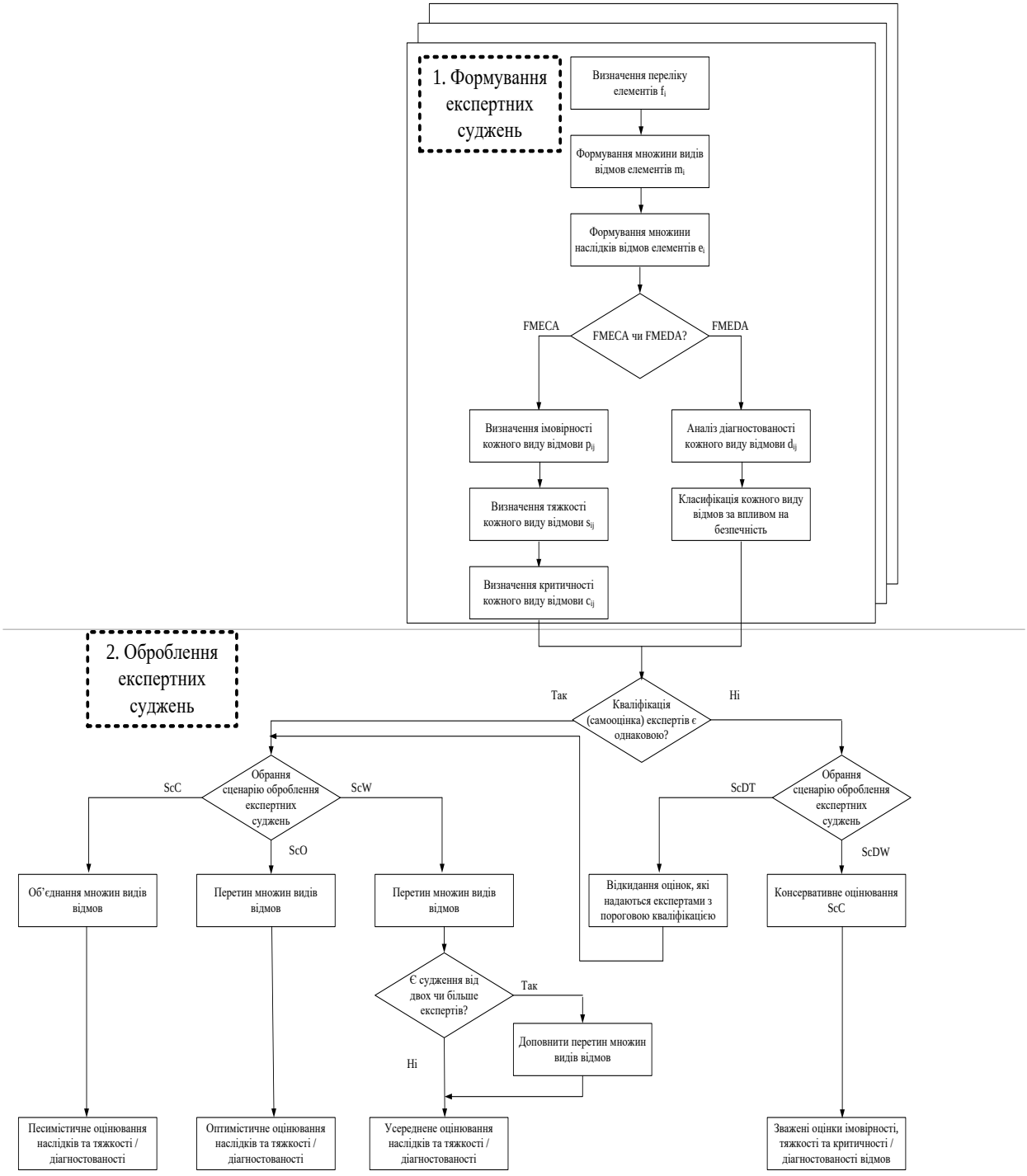


Рисунок 3.9 – Алгоритм методу експертного оцінювання FMECA/FMEDA

3.5. Висновки до розділу

1. Сформульовано задачу експертного оцінювання функційної безпечності ІКС із використанням FMECA/FMEDA-FIT як задачу формування та узгодження експертних рішень. Визначено множину експертів, множину експертних задач та множини можливих рішень для кожної задачі, що забезпечує формалізоване представлення процесу експертного оцінювання.

2. Формалізовано процедуру експертного оцінювання характеристик HW/FPGA та SW-компонентів ІКС. Визначено склад параметрів, що можуть встановлюватися експертом під час формування FMECA/FMEDA-таблиці, зокрема множини компонентів, видів відмов і наслідків, імовірність, тяжкість, критичність та діагностованість відмов.

3. Розроблено процедуру формування колективної експертної оцінки на основі індивідуальних суджень експертів. Визначено основні типи розбіжностей між експертними оцінками, що стосуються складу компонентів, видів відмов, наслідків, імовірності, тяжкості та критичності відмов.

4. Запропоновано три базові сценарії узгодження експертних оцінок: консервативний (ScC), оптимістичний (ScO) та зважений (ScW). Консервативний сценарій забезпечує формування найбільш повного набору об’єктів аналізу та використання граничних оцінок; оптимістичний – формування мінімального набору на основі перетину експертних множин; зважений – поєднання спільних та підтриманих декількома експертами елементів із використанням агрегованих оцінок параметрів.

5. Розширено процедуру узгодження експертних оцінок шляхом урахування відмінностей у кваліфікації та самооцінці експертів. Визначено сценарії, що передбачають вилучення оцінок експертів із недостатнім рівнем кваліфікації, а також сценарії зваженого врахування експертних оцінок залежно від їхнього профілю досвіду та типу експертного питання.

6. Розроблено процедуру оцінювання критичності припущень і помилок аналізу в межах FMECA/XMECA. Формалізовано множини запитань,

пов’язаних із припущеннями та помилками, множини експертів із різним профілем досвіду та правила визначення ваги відповіді залежно від відповідності типу питання профілю експерта.

7. Запропоновано процедуру ризик-орієнтованого оцінювання припущень і помилок із використанням трирівневої шкали H/M/L. Отримані індивідуальні оцінки експертів агрегуються з урахуванням визначених ваг, після чого результат деквантифікується до відповідного рівня критичності. На основі отриманого рівня визначається необхідність модифікації FMECA-таблиці або процедури її виконання.

8. Сформовано перелік типових помилок експертного FMECA/XMECA-аналізу та встановлено їхній можливий вплив на оцінку функційної безпечності. Показано, що неповне врахування компонентів, видів відмов, рівнів системи, дефектів або їхніх комбінацій може призводити до ризику переоцінювання функційної безпечності, тоді як включення надлишкових елементів аналізу може спричиняти ризик її недооцінювання.

9. Розроблено алгоритмічну процедуру експертного оцінювання FMECA/FMEDA, яка охоплює формування експертних задач, отримання індивідуальних оцінок, перевірку відповідей, формування узгодженої оцінки за обраним сценарієм та розрахунок показників функційної безпечності. Алгоритм забезпечує послідовне перетворення експертних суджень у результати, придатні для подальшого FMECA/FMEDA-аналізу.

10. Запропоновано автоматизацію створення опитувальників та оброблення результатів експертного оцінювання. Автоматизація передбачає формування питань на основі визначеної множини експертних задач, перевірку повноти та допустимості відповідей, їх структурування, визначення розбіжностей і підготовку даних для подальшого узгодження. Приклад опитувальника наведено в додатку В, а алгоритм методу представлено на рис. 3.9.

11. Отримані результати забезпечують зменшення залежності FMECA/FMEDA-оцінювання від окремих експертних суджень та створюють

формальну основу для відтворюваного узгодження експертних оцінок. Розроблений метод може бути використаний як складова процедури оцінювання функційної безпечності програмовних ІКС та як підготовчий етап для подальшого аналізу багатоверсійних систем.

Список використаних джерел

1. Kahneman. D., Slovic, P., Tversky, A. Judgement under Uncertainty, Heuristics and Biases // Science. 1974. – Vol. 185, Issue 4157. – P. 1124-1131. DOI: 10.1126/science.185.4157.1124

2. Morgan M.G., Henrion M. Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge University Press, 1992 – 346 p.

3. O'Hagan A., Buck C. E., Daneshkah A., Eiser J. R., Garthwaite P.H., Jenkinson D.J., Oakley J.E., Rakow T. Uncertain Judgments: Eliciting Experts' Probabilities. Wiley, 2006. – 338 p.

4. Cooke, R M. Experts In Uncertainty: Opinion and Subjective Probability in Science. Oxford University Press, 1991. – 336 p.

5. Goossens L.H.J., Harper F.T., Kraan B.C.P., Metivier H. Expert Judgement for a Probabilistic Accident Consequence Uncertainty Analysis // Radiation Protection Dosimetry. – Volume 90, Issue 3, 1 August 2000. – P. 295-301. DOI: 10.1093/oxfordjournals.rpd.a033151

6. Deng Y., Kang B.Y., Zhang Y.J., Deng X.Y., Zhang H.X. Aggregate experts' judgments in nuclear engineering management. *// Proceedings of Chinese Control and Decision Conference (CCDC)*. – Mianyang, China, 2011. P. 3236-3239. DOI: 10.1109/CCDC.2011.5968814.

7. Bouzaiene L., Billy F., Bocquet J-C., Haik P., Lannoy A., Peres F. Expert Judgement Methodology for Failure Anticipation in Nuclear Power Plants // Safety and Reliability: Proceedings of the ESREL 2003 Conference, Maastricht, the Netherlands. – 15-18 June 2003. – P. 195-200.

8. Kostogryzov A., Rybas A., Grigoriev L., Nistratov A., Nistratov G. Probabilistic Estimations of Increasing Expected Reliability and Safety for Intelligent Manufacturing // Proceedings of Global Smart Industry Conference (GloSIC), 2018. – P. 1-7. DOI: 10.1109/GloSIC.2018.8570124.

9. Jianxing Y., Haicheng C., Shibo W., Haizhao F. A Novel Risk Matrix Approach Based on Cloud Model for Risk Assessment Under Uncertainty. // *IEEE Access*, 2021. – Vol. 9. – P. 27884-27896. DOI: 10.1109/ACCESS.2021.3058392.

РОЗДІЛ 4.
МЕТОД ОЦІНЮВАННЯ ФУНКЦІЙНОЇ БЕЗПЕЧНОСТІ БАГАТОВЕРСІЙНИХ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ НА ПРОГРАМОВНИХ ПЛАТФОРМАХ. ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ

4.1. Модель дефектів програмно-апаратних компонентів багатоверсійних ІКС ППЛ

4.1.1. Модель дефектів компонентів за рівнями ієрархії

Для побудови моделі дефектів багатоверсійних інформаційно-керуючих систем, реалізованих на програмовних логічних платформах, необхідно виконати структуровану систематизацію можливих джерел дефектів та механізмів їх прояву. Така систематизація дозволяє формалізувати простір дефектів системи та встановити причинно-наслідкові зв’язки між фізичними процесами, помилками проєктування та системними відмовами.

Особливістю ІКС на базі програмовних платформ (FPGA, програмовних логічних контролерів тощо) є багаторівнева природа формування відмов. Первинні фізичні порушення, що виникають на рівні напівпровідникових структур або під впливом зовнішнього середовища, можуть трансформуватися у логічні помилки в конфігурації програмовної логіки, далі – у дефекти взаємодії компонентів платформи, і в кінцевому підсумку проявлятися як системні відмови на рівні функціонування багатоверсійної ІКС [20,23].

З урахуванням цього доцільно розглядати дефекти у вигляді ієрархічної моделі, що включає кілька взаємопов’язаних рівнів. У даній роботі виділяються чотири основні рівні формування дефектів:

L1 – фізичний рівень, що охоплює дефекти напівпровідникового кристала та вплив факторів зовнішнього середовища;

L2 – проєктно-логічний рівень, пов’язаний із дефектами HDL-описів, синтезу та інтеграції IP-ядер;

L3 – рівень інтеграції та платформи, що відображає дефекти взаємодії компонентів програмовної платформи;

L4 – системно-мережевий рівень, на якому дефекти проявляються у взаємодії між версіями системи та механізмах координації їх роботи.

Для кожного з зазначених рівнів формується структурована таблиця дефектів, яка включає причини виникнення дефектів, їх типи, параметри, що характеризують механізм прояву, а також оцінку їх потенційного впливу на функційну безпечність системи. Така формалізація є початковим етапом побудови математичної моделі дефектів, що надалі використовується для профілювання дефектів та кількісного оцінювання показників функційної безпечності багатоверсійних ІКС

4.1.1.1. Фізичний рівень внесення дефектів

Першим у цій ієрархії розглядається фізичний рівень формування дефектів (L1), який визначає фундаментальні механізми виникнення збоїв у програмовних логічних платформах, де дефекти зумовлені фізичними процесами в кремнії та впливом зовнішнього середовища. На фізичному рівні дефекти поділяються на дві великі категорії: детерміновані (зносні) та випадкові (індуковані середовищем) [20,23]. Систематизацію дефектів рівня L1 наведено в таблиці 4.1.

Таблиця 4.1 – Дефекти фізичного рівня L1

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
Ефекти деградації та старіння (Aging Effects)				
1	Старіння напівпровідникових структур (EM, NBTI, HCI)	Деградація логічних елементів	Δt – зміна затримки сигналу; ΔVth – дрейф порогової напруги	Призводить до порушення часових обмежень та переходу дефекту на рівень L2
Радіаційно-індуковані ефекти (SEE – Single Event Effects)				
1	Іонізуюче	SEU (Single	FIT(SEU),	Інверсія біта

	випромінювання	Event Upset)	σ_SEU, кількість критичних конфігураційних бітів	конфігурації змінює логічну топологію ПЛ
2		SET (Single Event Transient)	Частота імпульсів rate_SET, тривалість імпульсу	Короткочасний імпульс може бути зафіксований тригером як хибний сигнал
3		SEL (Single Event Latch-up)	Ймовірність SEL, час до відключення живлення	Може призвести до фізичного руйнування кристала без захисту
Термічні дефекти та вплив живлення				
1	Локальні перегріви та нерівномірне тепловиділення	Термічна деградація	ΔT – температурний градієнт; Tj – температура переходу	Підвищує інтенсивність відмов і кореляцію дефектів між каналами
2	Шум та транзієнти живлення	Помилкові логічні спрацювання	ΔV – амплітуда просадки; PSN – рівень шуму живлення	Може викликати синхронні збої у декількох каналах одночасно

4.1.1.2. Проєкто-логічний рівень внесення дефектів

Проєктно-логічний рівень є одним із найбільш критичних для багатоверсійних інформаційно-керуючих систем, реалізованих на програмовних платформах. На відміну від фізичного рівня (L1), де дефекти мають переважно стохастичний характер і обумовлені фізичними процесами в напівпровідникових структурах або впливом зовнішнього середовища, на рівні L2 основним джерелом дефектів є систематичні помилки, внесені на етапах проєктування, синтезу та інтеграції логічних компонентів.

Для програмовних логічних платформ (FPGA, PLC-based architectures) даний рівень охоплює опис функціональної логіки системи у вигляді мов

апаратного опису (HDL), зокрема VHDL або Verilog (System Verilog), а також інтеграцію стандартних і користувацьких IP-ядер. У цьому контексті дефект проєктно-логічного рівня визначається як невідповідність між формальною специфікацією функцій системи та її фактичною реалізацією у вигляді HDL-коду, конфігурації логічних блоків або параметрів синтезу.

Особливість дефектів рівня L2 полягає в тому, що вони можуть відтворюватися одночасно в кількох версіях багатоверсійної системи, якщо ці версії розробляються на основі спільної специфікації або з використанням однакових інструментальних засобів проєктування. У такому випадку виникає ризик появи корельованих систематичних помилок, які можуть призвести до одночасних відмов декількох каналів системи та зменшити ефективність механізмів мажоритарного голосування [38, 39, 41].

У подальшому дефекти проєктно-логічного рівня систематизуються у вигляді відповідної множини дефектів та їх параметрів, що дозволяє сформувати основу для побудови профілю дефектів рівня L2 та подальшого кількісного оцінювання показників функційної безпечності. Систематизацію дефектів рівня L2 наведено в таблиці 4.2.

Таблиця 4.2 – Дефекти проєктно-логічного рівня L2

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
Дефекти логічного синтезу та часових доменів				
1	Порушення часових обмежень під час синтезу та трасування	Timing Violation	Δt_{path} – перевищення затримки критичного шляху; slack; f_{clk}	Призводить до метастабільності, помилок фіксації даних та переходу дефекту на рівень L3
2	Некоректна взаємодія між тактовими доменами	CDC-defect (Clock Domain Crossing)	$MTBF_{CDC}$; кількість CDC переходів; τ_{meta}	Викликає випадкові збої передавання даних між модулями, що важко діагностуються

3	Некоректна оптимізація логіки засобами синтезу САПР (Vivado, Quartus, ін.)	Synthesis Optimization Defect	N_{opt} – кількість критичних оптимізацій; P_{opt} – ймовірність некоректної оптимізації; тип трансформації	САПР може видалити або модифікувати логічні елементи, які алгоритм синтезу вважає надлишковими (наприклад, дубльовані або резервні ланцюги безпеки). Це може призвести до втрати захисних механізмів, появи прихованих вразливостей та порушення функційної безпечності системи
Алгоритимічні та функційні дефекти				
1	Помилки проєктування автоматів станів	FSM-defect	N_{dead} – кількість тупикових станів; Nun def_ – кількість невизначених переходів	Може призвести до зависання алгоритму керування або переходу в небезпечний стан
2	Алгоритмічні та арифметичні помилки	Overflow / divide-by-zero / NaN / rounding defect	P_{alg} – імовірність алгоритмічної помилки; межі діапазону; розрядність n	Дає некоректні результати обчислень у функційно-критичних модулях
3	Невизначений порядок оброблення сигналів (логічні гонки)	Race Condition	N_{race} – кількість конфліктних пар сигналів; частота прояву	Формує нестійку логіку, коли результат залежить від послідовності приходу подій
Дефекти інтегрованих IP-ядер та повторного використання				
1	Недокументовані особливості поведінки IP-ядер (наприклад, контролерів	Black-box Defect	P_{ip} – імовірність прояву дефекту IP-ядра; кількість критичних IP	При критичних навантаженнях спричиняє відмови

	Ethernet або шин AXI)			
2	Невідповідність інтерфейсів між власною логікою та стандартними ядрами	Interface Mismatch	N_{if} – кількість невідповідностей; тип протокольного конфлікту	Призводить до втрати даних, блокування обміну або хибної інтерпретації сигналів

Головна небезпека проєктного рівня полягає в тому, що якщо різні версії (канали) ІКС розроблялися на основі однієї і тієї ж помилкової специфікації, вони міститимуть ідентичні дефекти на рівні L2. Це нівелює переваги мажоритування, оскільки всі три канали можуть видати однакову помилкову відповідь одночасно [38, 39, 41, 42].

Для мінімізації дефектів рівня L2 необхідно застосовувати не лише різні команди розробників, а й різні засоби синтезу (САПР) та різні стратегії верифікації (наприклад, поєднання Model Checking та Fault Injection).

4.1.1.3. Архітектурний рівень внесення дефектів

На цьому рівні розглядаються дефекти, що виникають внаслідок взаємодії між компонентами платформи, які окремо можуть функціонувати коректно. Є сполучною ланкою між програмною логікою та її фізичним втіленням. Цей розділ фокусується на тому, як окремі модулі (IP-ядра) об'єднуються в цілісну систему на кристалі (SoC) або друкованій платі. Основні проблеми цього рівня – конфлікти ресурсів та порушення цілісності сигналів, що виникають через складну топологію ПЛ [20, 21, 23]. Систематизацію дефектів рівня L3 наведено в таблиці 4.3.

Таблиця 4.3 – Дефекти архітектурного рівня L3

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
Дефекти внутрішньосистемних комунікацій (Bus & Interconnect)				
1	Помилки арбітражу внутрішньосистемних шин	Bus Arbitration Defect	P_{arb} – імовірність конфлікту арбітражу; час блокування	Може спричинити starvation «голодування» критичних модулів та втрату доступу до пам’яті
2	Порушення когерентності буферів/кешів/реєстрових копій	Data coherency defect	P_{coh} – імовірність неузгодженості; кількість розбіжностей	Некоректна робота кеш-пам'яті або буферів, через що різні обчислювальні ядра версії отримують різні значення однієї і тієї ж змінної.
3	Протокольні невідповідності	Protocol Mismatch	N_{prot} – кількість протокольних невідповідностей; error rate	Ситуації, коли «Master» та «Slave» пристрої по-різному інтерпретують сигнали готовності, що веде до втрати пакетів даних, зависання транзакцій або спотворення даних
Конфлікти фізичних ресурсів ПЛ				
1	Перевантаження трасування в ПЛ	Routing Congestion	utilization%; Δt_{route}; jitter	Формує непередбачувані затримки (jitter) та погіршує часову детермінованість
2	Паразитні	Crosstalk	рівень наведення	Викликає

	електромагнітні наведення		V_{xtalk}; частота помилок	спотворення логічних рівнів і помилкові спрацювання
3	Конфлікти спільного використання апаратних ресурсів	Resource Sharing Conflict	N_{share} – кількість конфліктів; коефіцієнт завантаження ресурсу	Може спричинити затримки, некоректні обчислення або взаємне блокування модулів
Дефекти підсистеми конфігурування та живлення				
1	Пошкодження або неповна коректність бітстріма	Bitstream integrity defect	$CRC_{error\ rate}$; P_{bit} – імовірність пошкодження; кількість помилкових бітів	Завантаження некоректної конфігурації змінює поведінку всієї ПЛ
2	Некоректна послідовність подачі напруги	Power sequencing issue	Δt_{seq}; кількість порушень старту	Спричиняє нестабільну ініціалізацію PLL, I/O та логічних блоків

На рівні L3 ключовим є вже не окремий логічний модуль, а взаємодія компонентів у межах платформи. Тут дефекти проявляються як конфлікти ресурсів, порушення протоколів і деградація цілісності обміну даними. Саме на цьому рівні логічний дефект L2 може трансформуватися у платформну відмову – наприклад, у блокування шини, deadlock або системну втрату синхронізації.

4.1.1.4. Системно-мережевий рівень внесення дефектів

На цьому рівні дефект визначається як порушення логіки взаємодії між незалежними обчислювальними каналами або між ІКС та об'єктом керування. Є вершиною ієрархії. Тут дефекти виникають не всередині окремих модулів чи кристалів, а в процесі кооперативної роботи декількох версій (каналів) ІКС. Для багатоверсійних систем цей рівень є критичним, оскільки саме тут реалізуються

механізми мажоритування та синхронізації, а мажоритарний орган (Voter) – це "вузьке місце" будь-якої багатоверсійної системи [21, 25, 41, 42].

Таблиця 4.4 – Дефекти системно-мережевого рівня L4

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
Дефекти механізмів голосування та арбітражу (Voter Defects)				
1	Неправильний вибір порогу узгодження між різними версіями системи (алгоритми обчислень можуть відрізнятись)	Tolerance issue	δ_{tol} – поріг допустимого розходження	Система може відхилити правильний результат або прийняти помилковий
2	Дефекти логіки 2oo3 / 2oo4	Voting logic defect	N_{vote} – кількість логічних помилок алгоритму голосування	Порушує правильне виключення дефектного каналу з контуру керування
3	Некоректна реалізація механізму голосування	Voter defect	P_{voter} – імовірність відмови voter; N_{disc} – кількість невірних рішень	Цей дефект відноситься до Common Cause Failure (CCF) органу мажоритування і призводить до повної відмови системи
Дефекти часової синхронізації та детермінізму				
1	Розсинхронізація каналів (часовий дрейф)	Clock Drift	Δt_{sync} – розбіжність у часі між каналами	Канали обробляють дані з різних часових квантів, що породжує хибні конфлікти і призводить до хибних спрацьовувань

				мажоритарного органу.
2	Варіації затримок у (дрижання фази) мережі	latency defect (середній час затримки) / Jitter (коливання значення затримки)	jitter; t_{lat}	Руйнує детермінізм роботи системи реального часу
3	Передавання несумісних або суперечливих значень різним вузлам (візантійські помилки)	Byzantine fault	P_{byz} – імовірність візантійського прояву	Ускладнює або унеможливлює досягнення консенсусу між версіями
Мережеві та протокольні дефекти(Safety Communication)				
1	Перевантаження мережного трафіку	Broadcast Storm / Traffic Overload	Throughput (пропускна здатність); Packet Loss Rate (коефіцієнт втрати пакетів); Queue L ength (довжина черги – кількість пакетів, які очикують оброблення)	Блокує обмін між каналами та призводить до втрати критичних повідомлень
2	Помилки ідентифікації або адресації даних	Data identification defect	P_{id} – імовірність помилки ідентифікації; кількість хибних кадрів	Застарілі або чужі дані можуть бути сприйняті як актуальні

На рівні L4 дефект уже проявляється як системна відмова версії або механізму координації між версіями. Для багатоверсійних ІКС цей рівень є критичним, оскільки саме тут реалізуються голосування, арбітраж, синхронізація та безпечний зв’язок. Відповідно, дефекти рівня L4 мають безпосередній вплив на підсумковий показник функційної безпечності системи.

Узагальнення дефектів за рівнями L2–L4 доповнює фізичний рівень L1 і формує повний багаторівневий простір дефектів багатоверсійної ІКС на програмовній платформі. Така систематизація є первинною формалізацією, на основі якої далі можуть бути побудовані множини дефектів D_{Lk}, профілі дефектів $П_{Lk}$ та математичні залежності для кількісного оцінювання показників функційної безпечності.

4.1.2 Модель дефектів багатоверсійності ІКС ППЛ

Багатоверсійні ІКС, що реалізуються на програмовних платформах (FPGA, PLC тощо), застосовуються для підвищення функційної безпечності за рахунок використання структурно-версійної надмірності. Основна ідея такого підходу полягає у використанні кількох незалежних реалізацій функціональної логіки (версій), результати яких порівнюються або узгоджуються за допомогою механізмів голосування. Однак сама архітектура багатоверсійності породжує новий клас дефектів, які не пов’язані безпосередньо з фізичними або логічними компонентами системи, а виникають через взаємозалежність версій, спільність вихідних припущень або інфраструктури виконання. Такі дефекти можуть призводити до відмов за спільною причиною, що є однією з основних загроз функційній безпечності багатоверсійних систем. У загальному випадку множину дефектів багатоверсійності (MV – Multi-Version Systems Defects) можна визначити як

$$D_{MVS} = \{d_{mvs,1}, d_{mvs,2}, ..., d_{mvs,m}\}, \qquad (4.1)$$

де:

- $d_{mvs,m}$ - дефект, пов’язаний із взаємодією або структурою багатоверсійної системи.

На відміну від дефектів рівнів L1–L4, які характеризують окремі компоненти системи, дефекти множини D_{MVS} описують властивості архітектури багатоверсійності, що можуть призводити до одночасних відмов кількох версій.

У даній роботі виділяються три основні класи дефектів багатоверсійності:

- дефекти спільної специфікації (Common Specification Faults);
- дефекти подібності реалізацій «ідентичності» (Similitude Faults);
- дефекти спільної інфраструктури виконання (Infrastructure CCF).

4.1.2.1 Дефекти спільної специфікації

Дефекти спільної специфікації належать до класу системних дефектів і виникають на етапі формування вимог до системи. У багатоверсійних ІКС усі версії розробляються на основі однієї і тієї ж функціональної специфікації, яка визначає логіку роботи системи [38, 39, 41, 42]. У разі наявності помилки у вихідній специфікації така помилка реплікується у всіх реалізаціях системи. У результаті різні версії можуть синхронно видавати однаковий неправильний результат, що нівелює ефект мажоритарного голосування. Дефекти спільної специфікації виникають на етапі формування вимог до системи. У багатоверсійних ІКС усі версії розробляються на основі однієї і тієї ж функціональної специфікації, яка визначає логіку роботи системи.

У разі наявності помилки у вихідній специфікації така помилка реплікується у всіх реалізаціях системи. У результаті різні версії можуть синхронно видавати однаковий неправильний результат, що нівелює ефект мажоритарного голосування. Систематизацію дефектів спільної специфікації наведено в таблиці 4.5.

Таблиця 4.5 – Дефекти спільної специфікації.

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
1	Неповне або неоднозначне формулювання вимог в ході опису функційної логіки	Logical Ambiguity	N_{amb} – кількість неоднозначних вимог; P_{amb} – ймовірність прояву	Неповне або неоднозначне формулювання вимог

2	Невизначеність поведінки системи у граничних режимах	Boundary Condition Defect	N_{bcd} – кількість невизначених граничних станів	При екстремальних режимах роботи всі версії можуть приймати однакове неправильне рішення
3	При екстремальних режимах роботи всі версії можуть приймати однакове неправильне рішення	Requirement Conflict	N_{conf} – кількість конфліктних вимог	Nconf – кількість конфліктних вимог
4	Некоректна математична модель об’єкта керування	Mathematical Model Defect	P_{model} – ймовірність помилки моделі; Δmodel – похибка моделювання	Усі версії використовують однакову помилкову модель процесу
5	Невірно визначені часові вимоги	Timing Specification Defect	Δt_{req} – відхилення часових параметрів	Призводить до некоректного синтезу логіки в усіх версіях FPGA
6	Помилки визначення інтерфейсів та одиниць вимірювання	Interface Specification Defect	N_{if} – кількість помилок інтерфейс	Невірна інтерпретація сигналів датчиків або виконавчих механізмів
7	Відсутність опису поведінки при недостовірних даних	Fault Handling Specification Defect	P_{fault} – ймовірність неправильного реагування	Система не має алгоритму оброблення помилкових або NaN-значень

Проведений аналіз показує, що дефекти спільної специфікації мають особливий механізм прояву у багатоверсійних інформаційно-керуючих системах. У традиційних одноканальних системах помилки специфікації зазвичай виявляються на етапах верифікації або під час експлуатації системи. Натомість у багатоверсійних структурах виникає так званий ефект «ілюзії

коректності». Оскільки всі версії системи розробляються на основі однієї і тієї ж специфікації, вони можуть поводитися однаково навіть у випадку наявності помилки у вимогах. У результаті всі канали формують ідентичний, але неправильний результат.

У таких умовах методи тестування, що базуються на порівнянні результатів різних версій (зокрема back-to-back testing), виявляються неефективними. Відсутність розбіжностей між каналами інтерпретується як ознака коректності роботи системи, хоча фактично всі версії реалізують одну й ту саму помилкову логіку.

Для мінімізації ризику виникнення дефектів спільної специфікації доцільно застосовувати комплекс методів підвищення якості вимог та їх формальної перевірки. До таких методів належать:

- формальна специфікація (Formal Methods) – використання математичних мов опису вимог (наприклад, Z-notation, B-Method, Event-B), що дозволяє виконувати автоматичну перевірку несуперечливості та повноти специфікації;

- різноманітність специфікацій (Specification Diversity) – розроблення альтернативних варіантів технічного завдання незалежними групами системних аналітиків з подальшим узгодженням результатів;

- виконувані специфікації (Executable Specifications) – створення високорівневих моделей поведінки системи (наприклад, у середовищах MATLAB/Simulink), що дозволяє перевіряти логіку вимог шляхом моделювання до початку реалізації на рівні HDL.

Таким чином, дефекти спільної специфікації є одним із ключових обмежень ефективності багатоверсійного підходу. За відсутності формальної верифікації вимог багатоверсійність забезпечує захист переважно від випадкових апаратних збоїв та помилок програмної реалізації, але не усуває фундаментальних помилок, закладених на рівні системної специфікації. Це особливо критично для систем з високими вимогами до функційної безпечності, зокрема для систем класу SIL 3–SIL 4.

4.1.2.2 Дефекти «ідентичності»

Дефекти ідентичності виникають внаслідок недостатньої глибини диверсності між версіями ІКС. Це ситуація, коли різні команди розробників несвідомо використовують однакові підходи, інструменти або структури, що призводить до появи ідентичних «слабких місць» у різних каналах системи [38, 39, 41]. Систематизацію дефектів «ідентичності» наведено в таблиці 4.6.

Таблиця 4.6 – Дефекти ідентичності

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
Інструментальна ідентичність (Tool-chain Similitude)				
1	Використання однієї САПР синтез	CAD Tool Correlation	P_{tool} – ймовірність дефекту інструменту	Одна і та сама помилка оптимізації може з’явитися у всіх версіях
2	Використання однакових бібліотек HDL	Library Correlation Defect	N_{lib} – кількість спільних бібліотек	N_{lib} – кількість спільних бібліотек
3	Використання однакових IP-ядер	Shared IP Defec	N_{ip} – кількість спільних IP; P_{ip} – ймовірність дефекту	Дефект IP-ядра миттєво стає спільним для всіх каналів
4	Ідентичні алгоритми синтезу логіки	Synthesis Correlation	P_{syn} – ймовірність однакової трансформації логіки	P_{syn} – ймовірність однакової трансформації логіки
Алгоритмічна подібність (Methodological Similitude)				
5	Використання однакових числових методів	Numerical Method Correlation	P_{alg} – імовірність алгоритмічної кореляції	Однакові помилки округлення або нестійкість алгоритму
6	Використання однакових алгоритмів оброблення	Algorithmic Similarity	N_{alg} – кількість однакових алгоритмів	Призводить до однакових помилок при певних

	сигналів			режимах роботи
7	Використання однакових шаблонів FSM	FSM Pattern Correlation	N_{fsm} – кількість ідентичних автоматів	Корельовані дефекти переходів між станами
Когнітивна подібність (Cognitive Diversity Gap)				
8	Однакові помилки програмістів у граничних умовах |	Boundary Logic Defect	P_{bound} – ймовірність помилки	Помилки оброблення крайових значень
9	Складні вкладені логічні конструкції	Nested Logic Error	N_{logic} – кількість складних умов	Помилки в умовах if–then–else
10	Неправильна інтерпретація складних алгоритмів	Cognitive Algorithm Defect	$_{Pcog}$ – ймовірність когнітивної помилки	Різні розробники повторюють однакову логічну помилку

Для мінімізації впливу даного виду дефектів пропонується впровадження примусової диверсності (Forced Diversity):

Гетерогенність САПР: синтез кожної версії різними версіями інструментів або використання альтернативних відкритих засобів синтезу (Y_{osys} тощо).

Стилістична диверсність коду: вимога до використання різних парадигм програмування (наприклад, одна версія базується на структурному описі, інша – на поведінковому).

Диверсність типів даних: використання фіксованої коми (Fixed-point) в одній версії та плаваючої коми (Floating-point) в іншій для рознесення помилок обчислень.

Дефекти ідентичності доводять, що багатоверсійність є ефективною лише тоді, коли вона забезпечує диверсифікацію помилок. Якщо версії залишаються ідентичними в методах оброблення даних або інструментах реалізації, вони

стають вразливими до одночасних відмов, що критично для систем класу безпеки SIL 3 та вище.

4.1.2.3 Дефекти середовища виконання та інфраструктури

Дефекти інфраструктурного рівня призводять до відмов за спільними причинами через вразливості в допоміжних підсистемах, які забезпечують життєдіяльність усіх версій ІКС. Такі дефекти здатні нівелювати переваги логічної диверсності, оскільки вони вражають «спільний ґрунт», на якому функціонують канали [38, 39, 41, 42]. Систематизацію дефектів середовища виконання та інфраструктури наведено в таблиці 4.7.

Таблиця 4.7 – Дефекти середовища виконання та інфраструктури.

#	**Причина дефекту**	**Тип дефекту**	**Параметр, що описує дефект**	**Пояснення / вплив на безпечність**
Дефекти системи тактування та синхронізації				
1	Використання спільного джерела опорної частоти	Clock Source Failure	P_{clock} – імовірність відмови генератора; Δf – відхилення частоти	Порушення синхронізації одночасно у всіх каналах системи
2	Фазове дрижання тактового сигналу	Clock Jitter	jitter; σt – стандартне відхилення фази	Порушення часових обмежень (timing constraints) у всіх версіях
3	Некоректна робота PLL/DCM	PLL Instability	P_{pll} – імовірність зриву синхронізаці	Синхронна нестабільність логічних блоків FPGA
Дефекти підсистеми електроживлення та заземлення				
5	Просадки або стрибки напруги	Voltage Transient |	ΔV – амплітуда просадки; Ppower – імовірність транзієнта	Викликає одночасні збої в роботі логічних блоків FPGA
6	Спільна система живлення каналів |	Power Supply Coupling	N_{ps} – кількість спільних ліній живлення	Помилки можуть виникати синхронно у всіх

				версіях
7	Некоректне заземлення	Ground Loop Defect	V_{noise} – рівень шуму заземлення	Викликає корельовані помилки вимірювання сигналів |
Дефекти інфраструктури комунікацій (Communication Infrastructure Defects)				
8	Перевантаження мережі передачі даних	Network Overload	Throughput; Packet Loss Rate	Втрата або затримка критичних повідомлень між каналами
9	Помилки роботи комутаторів або інтерфейсів |	Network Hardware Failure	P_{net} – імовірність відмови мережного вузла	Призводить до порушення координації між версіями
10	Дефекти протоколів безпечного зв’язку	Safety Communication Defect	P_{err} – імовірність помилки протокола	Може спричинити прийняття застарілих або некоректних даних
Дефекти апаратних засобів підтримки (Hardware Abstraction & Drivers)				
11	Дефекти мікропрограм периферійних контролерів	Firmware Infrastructure Defect	P_{firm} – імовірність помилки мікропрограми	Некоректна робота мережевих або шинних контролерів
12	Помилки завантаження конфігурації FPGA	Bitstream Load Defect	P_{bit} – імовірність пошкодження бітстріму	Некоректна ініціалізація всіх каналів після перезавантаження
13	Спільні інтерфейси конфігурування (JTAG, SPI)	Configuration Interface Defect	N_{cfg} – кількість спільних інтерфейсів	Може спричинити одночасні помилки конфігурації
Вплив факторів зовнішнього середовища, що викликають дефекти (Environmental Stress)				
14	Перегрів через спільну систему охолодження	Thermal Infrastructure Defect	ΔT – температурний градієнт; T_j	Зростання інтенсивності відмов усіх

				каналів
15	Зростання інтенсивності відмов усіх каналів	EMI Defec	EMI_{level}; P_{err}	Синхронні помилки у каналах зв'язку
16	Вібраційні або механічні впливи	Mechanical Stress Defect	P_{vib} – імовірність механічного впливу	Може викликати одночасні збої апаратних модулів

Для зменшення ймовірності виникнення інфраструктурних дефектів та пов'язаних із ними відмов за спільною причиною доцільно застосовувати комплекс технічних та архітектурних заходів, спрямованих на підвищення незалежності каналів багатоверсійної системи. До основних підходів належать:

Електрична ізоляція та незалежні контури живлення. Використання гальванічної розв'язки, індивідуальних стабілізаторів напруги та окремих джерел живлення для кожної версії системи дозволяє запобігти поширенню транзієнтів напруги та інших електричних збурень між каналами.

Гетерогенність джерел тактування. Для зменшення ризику синхронних збоїв доцільно застосовувати різні типи генераторів тактової частоти, що базуються на різних фізичних принципах (наприклад, Micro-Electro-Mechanical-Systems (MEMS – генератори) для одного каналу та кварцові генератори для іншого). Такий підхід знижує ймовірність одночасного порушення синхронізації у всіх версіях системи.

Просторове рознесення апаратних компонентів. Фізичне розміщення апаратури різних версій у незалежних шасі, стойках або навіть окремих приміщеннях дозволяє мінімізувати вплив спільних факторів середовища, таких як перегрів, електромагнітні завади або механічні впливи. Для критичних систем, зокрема в атомній енергетиці, подібне просторове рознесення є одним із ключових елементів підвищення функційної безпечності.

Проведений аналіз дефектів спільної специфікації, дефектів ідентичності та інфраструктурних дефектів дозволяє сформувати узагальнену модель вразливостей багатоверсійних інформаційно-керуючих систем. Отримані

результати підтверджують, що досягнення високого рівня функційної безпечності можливе лише за умови забезпечення диверсності на всіх рівнях системної архітектури – від математичних моделей та алгоритмів оброблення даних до фізичної реалізації апаратних компонентів і організації систем електроживлення.

Таким чином маємо:

$$D_{MVS} = D_{spec} \cup D_{sim} \cup D_{inf}, \quad (4.2)$$

де:

D_{spec} – дефекти специфікації;

D_{sim} – дефекти ідентичності;

D_{inf} – інфраструктурні дефекти.

4.1.3 Моделювання процесів трансформації дефектів

У багаторівневій архітектурі програмовних інформаційно-керуючих систем дефекти не проявляються ізольовано, а утворюють причинно-наслідкові ланцюги, в межах яких первинні порушення нижчих рівнів поступово трансформуються у системні відмови. Відповідно до ієрархічного опису дефектів, наведеного у підрозділі 4.1.1, процес формування відмови можна розглядати як послідовність переходів між рівнями:

$$L1 \Rightarrow L2 \Rightarrow L3 \Rightarrow L4, \quad (4.3)$$

де: L1 – фізичний рівень; L2 – проєктно-логічний рівень; L3 – архітектурно-платформний рівень; L4 – системний рівень взаємодії каналів.

Типовими прикладами такої трансформації є наступні.

Приклад 1.

$$SEU_{L1} \Rightarrow Timing Violation_{L2} \Rightarrow BusArbitrationDefect_{L3} \Rightarrow VoterDefect_{L4} \quad (4.4)$$

Етапність трансформації наступна:

1. SEU (Single Event Upset) – рівень L1 (фізичний). Іонізуюча частинка змінює стан біта конфігураційної пам’яті FPGA.

2. Timing Violation – рівень L2 (проєктно-логічний). Через зміну конфігурації логіки порушуються часові параметри критичного шляху сигналу.

3. Bus Arbitration Defect – рівень L3 (архітектурний). Некоректні сигнали керування призводять до блокування або конфлікту доступу до системної шини.

4. Voter Defect – рівень L4 (системно-мережевий). Мажоритарний орган отримує некоректні або несинхронізовані результати від каналів і приймає помилкове рішення.

Приклад 2.

$$\mathrm{SEU}_{L1} \Rightarrow \mathrm{FSM\_Defect}_{L2} \Rightarrow \mathrm{Protocol\_Mismatch}_{L3} \Rightarrow \mathrm{Byzantine\_Fault}_{L4} \quad (4.5)$$

Етапність трансформації наступна:

1. SEU (Single Event Upset) – рівень L1 (фізичний). Іонізуюча частинка змінює стан біта конфігураційної пам’яті FPGA, тобто така подія змінює реалізацію частини логічної схеми або умови переходу в автоматі станів.

2. FSM_Defect - рівень L2 (проєктно-логічний). На рівні L2 це може проявитися як дефект автомата станів, зокрема: перехід у невизначений стан; активація тупикового стану; порушення логіки переходів між станами; формування некоректної послідовності керуючих сигналів.

3. Protocol_Mismatch - рівень L3 (архітектурний). В наслідок прояву FSM_Defect на архітектурному рівні може бути порушено протокольну взаємодію між компонентами платформи. Наприклад, модуль, керований автоматом станів, починає передавати сигнали готовності, підтвердження або адресації у невірній послідовності, через що інші блоки платформи по-різному інтерпретують хід передачі. Це може призводити до втрати даних, зависання передачі або порушення синхронізації обміну.

4. Byzantine Fault - рівень L4 (системно-мережевий). На рівні L4 дефект Protocol_Mismatch може трансформуватися у Byzantine Fault, тобто ситуацію, коли один і той самий канал системи передає різним вузлам або механізмам узгодження несумісні, суперечливі або часово неузгоджені дані. Для багатоверсійної ІКС це особливо небезпечно, оскільки ускладнює або навіть

унеможливлює досягнення консенсусу між версіями, а отже, безпосередньо впливає на правильність мажоритарного рішення.

Для формалізації процесу поширення дефектів введемо множину дефектів кожного рівня ієрархії:

$$D_{Lk} = \{d_{k1}, d_{k2}, ...d_{kn_k}\}, \quad (4.6)$$

де: $k \in \{1,2,3,4\}$ – номер рівня ієрархії (L1…L4); n_k – кількість типів дефектів, що визначено на рівні L_k; d_{ki} – тип дефекту на рівні L_k.

d_{ki} можливо описати кортежом:

$$d_{nk} = \langle c_i, t_i, p_i \rangle, \quad (4.7)$$

де: c_i – клас причин (наприклад, SEE, старіння, шум живлення), t_i– тип/механізм дефекту (SEU, TimingViolation Bus, Arbitration Defect, Voter Defect тощо), p_i – параметри дефекту, що характеризують його інтенсивність, ймовірність або умови прояву (FIT, Δt, ΔV, $MTBF_{CDC}$, jitter та інш.).

Загальна множина дефектів D є об'єднанням множин дефектів, визначених на кожному рівні ієрархії.

$$D = \bigcup_{k=1}^{4} D_{Lk} \quad (4.8)$$

Для опису процесу переходу дефектів між рівнями введемо оператори трансформації

$$T_{Lk} \rightarrow L_{k+1}, \quad (4.9)$$

де $T_{Lk} \rightarrow L_{k+1}$ - оператор, що описує механізм переходу дефекту з рівня L_k на рівень L_{k+1}.

Тоді процес трансформації (поширення) дефекту можна подати у вигляді.

$$d_{L_{k+1}} = T_{L_k \rightarrow L_{k+1}}(d_{L_k}) \quad (4.10)$$

Для повного ланцюга трансформації дефекту від фізичного до системного рівня отримаємо.

$$d_{L_4} = T_{L_3 \to L_4}(T_{L_2 \to L_3}(T_{L_1 \to L_2}(d_{L1})) \quad (4.11)$$

Цей вираз відображає каскадний характер поширення дефектів у багаторівневій архітектурі ІКС.

З урахуванням імовірнісного характеру виникнення дефектів кожному оператору трансформації можна поставити у відповідність коефіцієнт переходу $P_{k,k+1}$, що оцінює ймовірність того, що дефект рівня L_k призведе до дефекту на рівні L_{k+1}.

Тоді узагальнена ймовірність трансформації дефекту від фізичного рівня до системної відмови може бути оцінена як:

$$P_{L_1 \to L_4} = P_{12} \cdot P_{23} \cdot P_{34}, \quad (4.12)$$

де:

- P_{12} – умовна імовірність переходу дефекту з рівня L_1 до рівня L_2;
- P_{23} – умовна імовірність переходу дефекту з рівня L_2 до рівня L_3;
- P_{34} – умовна імовірність переходу дефекту з рівня L_3 до рівня L4.

Якщо інтенсивність дефектів фізичного рівня характеризується параметром λ_{L1} (наприклад, у метриці FIT), то еквівалентна інтенсивність системної відмови може бути оцінена як:

$$\lambda_{L4} = \lambda_{L1} \cdot P_{12} \cdot P_{23} \cdot P_{34} \quad (4.13)$$

Запропонована модель дозволяє формалізувати механізм трансформації дефектів між рівнями архітектури програмовних ІКС та створює основу для подальшого профілювання дефектів і кількісного оцінювання показників функційної безпечності системи.

4.1.4 Профілювання дефектів

Профілювання дефектів полягає у формуванні структурованого набору параметрів, що характеризують інтенсивність виникнення дефектів, їх небезпечність, можливість виявлення та вплив на функційну безпечність

системи. Такий підхід дозволяє перейти від якісного опису дефектів до їх кількісного аналізу.

Профіль дефектів рівня L_k це:

$$П_{L_k} = \{(\lambda_{ki}, P_{D,ki}, DC_{ki}, \omega_{ki}, CCF_{ki}\}, \quad (4.15)$$

де:

- λ_{ki} – інтенсивність виникнення *i-го* дефекту рівня L_k;

- $P_{D,ki}$ – ймовірність того, дефект призведе до небезпечної відмови;

- DC_{ki} - коефіцієнт діагностичного покриття (Diagnostic Coverage), що характеризує здатність системи виявити дефект;

- ω_{ki} - ваговий коефіцієнт критичності дефекту для функційної безпечності;

- CCF_{ki} - коефіцієнт Common Cause Failure, що враховує можливість одночасної відмови декількох каналів системи.

Загальний профіль дефектів:

$$П = \bigcup_{k=1}^{4} П_{Lk} \quad (4.16)$$

Таким чином, профіль дефектів рівня L_k можна представити як набір параметризованих характеристик усіх типів дефектів, визначених на цьому рівні.

4.2. Модель вразливостей програмно-апаратних компонентів багатоверсійних ІКС ППЛ

4.2.1. Модель вразливостей компонентів за рівнями ієрархії

Попередньо розроблена ієрархічна модель дефектів програмно-апаратних компонентів інформаційно-керуючих систем дозволяє систематизувати джерела порушень функціонування програмовних платформ та описати

механізми їх трансформації у системні відмови [20, 21, 23]. Однак для повноцінного оцінювання функційної безпечності необхідно враховувати не лише наявність дефектів, але й структурні особливості системи, які визначають її чутливість до цих дефектів. Саме такі особливості формують вразливості системи.

У контексті даного дослідження вразливість програмно-апаратного компонента визначається як властивість архітектури або реалізації системи, яка створює умови для прояву дефекту або підвищує ймовірність його трансформації у функційно небезпечну відмову. Іншими словами, вразливість характеризує ті структурні або функціональні особливості системи, що визначають ступінь її сприйнятливості до внутрішніх або зовнішніх порушень.

На відміну від дефектів, які описують джерела порушень або механізми їх виникнення, вразливості відображають умови функціонування системи, за яких ці дефекти можуть призводити до небезпечних наслідків. Таким чином, дефекти та вразливості утворюють взаємопов’язану систему причинно-наслідкових залежностей, що визначає формування відмов у програмно-апаратних компонентах ІКС.

У загальному вигляді множину вразливостей системи можна визначити як

$$V = \{v_1, v_2, ..., v_n\}, \tag{4.17}$$

де v_i – окрема вразливість програмно-апаратного компонента ІКС.

Враховуючи багаторівневу архітектуру програмовних платформ, модель вразливостей доцільно будувати у відповідності до ієрархії рівнів, що була визначена для моделі дефектів. Такий підхід забезпечує узгодженість опису механізмів формування відмов і дозволяє безпосередньо пов’язати вразливості з відповідними множинами дефектів.

Таким чином, дане дослідження охоплює чотири основні рівні формування вразливостей:

– L1 – фізичний рівень, що охоплює апаратні характеристики програмовних логічних платформ та їх чутливість до фізичних впливів;

– L2 – проєктно-логічний рівень, що відображає вразливості, пов’язані з реалізацією алгоритмів та структур логічного оброблення даних;

– L3 – архітектурно-платформний рівень, на якому вразливості виникають у процесі інтеграції компонентів платформи;

– L4 – системно-мережевий рівень, що характеризує вразливості механізмів взаємодії між версіями системи.

На фізичному рівні (L1) основними джерелами вразливостей є фізичні властивості напівпровідникових структур та особливості реалізації програмовних логічних платформ. До таких вразливостей належать висока чутливість конфігураційної пам’яті FPGA до радіаційно-індукованих подій, температурна залежність характеристик логічних елементів, а також нестабільність параметрів живлення. У результаті навіть одиничні фізичні події, такі як SEU або електромагнітні збурення, можуть призводити до зміни конфігурації логічної схеми або порушення часових характеристик сигналів.

На проєктно-логічному рівні (L2) вразливості формуються внаслідок особливостей реалізації алгоритмів керування та структури HDL-описів системи. Серед основних факторів цього рівня можна виділити недостатню перевірку переходів у автоматах станів, використання складних вкладених логічних конструкцій, обмежені часові запаси критичних шляхів, а також недостатню формальну верифікацію алгоритмів. Такі особливості можуть створювати умови, за яких навіть незначні порушення конфігурації або синхронізації здатні призвести до помилкових переходів між станами або порушення алгоритму керування.

На архітектурно-платформному рівні (L3) вразливості пов’язані з інтеграцією окремих модулів у межах програмовної платформи. Основними джерелами таких вразливостей є конфлікти доступу до спільних ресурсів, обмеження пропускної здатності внутрішньосистемних шин, порушення когерентності даних, а також складна топологія міжмодульних з’єднань. У

результаті локальні дефекти окремих модулів можуть поширюватися на рівень платформи та проявлятися у вигляді блокування ресурсів, втрати даних або порушення протоколів взаємодії.

На системно-мережевому рівні (L4) вразливості пов’язані з особливостями організації взаємодії між незалежними версіями багатоверсійної інформаційно-керуючої системи. До них належать залежність роботи системи від синхронізації каналів, централізованість механізмів мажоритарного голосування, обмеження механізмів досягнення консенсусу між версіями, а також можливість появи часових розбіжностей між каналами. У таких умовах навіть локальні порушення у роботі одного з каналів можуть призводити до помилкових рішень органу мажоритування або втрати узгодженості між версіями системи. Систематизацію вразливостей за рівнями ієрархії наведено в таблиці 4.8.

Таблиця 4.8 – Вразливості компонентів за рівнями ієрарії.

#	**Рівень ієрархії**	**Вразливість**	**Причина**	**Параметр**
1	L1	Configuration Memory Sensitivity	велика кількість конфігураційних бітів	N_{conf}
2	L1	Thermal Sensitivity	висока щільність логіки	ΔT
3	L2	FSM Robustness Weakness	відсутність перевірки переходів	N_{state}
4	L2	Timing Margin Deficit	мінімальний slack	slack
5	L3	Bus Contention Vulnerability	вузьке місце арбітражу	P_{arb}
6	L3	Resource Contention	Вузьке місце арбітражу	N_{share}
7	L4	Voter Single Point of Failure	Централізований voter	P_{voter}
8	L4	Synchronization Vulnerability	Часовий дрейф каналів	N_{state}

Таким чином, модель вразливостей дозволяє формалізувати структурні умови, за яких дефекти різних рівнів можуть трансформуватися у системні відмови. Поєднання моделей дефектів і моделей вразливостей формує узагальнену причинно-наслідкову схему формування відмов у багатоверсійних інформаційно-керуючих системах на програмовних платформах.

Отримана модель створює основу для подальшого профілювання вразливостей та їх кількісного оцінювання, що дозволяє враховувати їх вплив під час виконання аналізу видів і наслідків відмов, а також при побудові методів ін’єктування дефектів і вразливостей, які розглядаються у наступних підрозділах даної роботи.

4.2.2. Модель вразливостей багатоверсійної ІКС ППЛ

Багатоверсійні ІКС на програмовних платформах використовують структурно-версійну надмірність для підвищення функційної безпечності. Основна ідея такого підходу полягає у використанні декількох незалежних реалізацій функціональної логіки, результати яких узгоджуються за допомогою механізмів голосування або інших процедур досягнення консенсусу. Незважаючи на підвищення стійкості системи до окремих дефектів, сама архітектура багатоверсійності формує специфічний клас структурних вразливостей, які можуть знижувати ефективність надмірності або призводити до одночасних відмов декількох каналів системи [38, 39, 41, 42].

Такі вразливості виникають у випадках, коли різні версії системи мають спільні залежності або використовують однакові припущення щодо поведінки об’єкта керування, алгоритмів оброблення даних або інфраструктури виконання. У таких умовах дефект, що проявляється в одному каналі, може з високою ймовірністю проявитися і в інших каналах системи.

У загальному вигляді множину вразливостей багатоверсійності можна визначити як

$$V_{MVS} = \{v_{mvs,1}, v_{mvs,2}, ..., v_{mvs,n}\}, \qquad (4.18)$$

де $v_{mvs,I}$ – вразливість, пов’язана із структурою або взаємодією версій у багатоверсійній системі.

Відповідно до класифікації дефектів багатоверсійності, розглянутої вище, вразливості багатоверсійних систем доцільно розділити на три основні класи:

- вразливості спільної специфікації (Specification Vulnerabilities);
- вразливості подібності реалізацій (Similitude Vulnerabilities);
- інфраструктурні вразливості (Infrastructure Vulnerabilities).

Вразливості спільної специфікації виникають у випадку, коли всі версії системи розробляються на основі однієї функціональної специфікації або математичної моделі об’єкта керування. У разі наявності помилки у специфікації така помилка може бути відтворена у всіх реалізаціях системи. У результаті різні версії можуть синхронно генерувати однаковий неправильний результат, що нівелює ефективність мажоритарного голосування.

Вразливості подібності реалізацій пов’язані з недостатнім рівнем диверсності системи. Навіть за умови використання різних команд розробників або різних мов програмування, розробники можуть застосовувати однакові алгоритмічні підходи, бібліотеки або інструментальні засоби синтезу. У таких випадках зростає ймовірність появи корельованих помилок у різних каналах системи.

Вразливості інфраструктури виконання виникають через спільне використання допоміжних підсистем, що забезпечують функціонування всіх каналів системи. До таких підсистем належать джерела живлення, генератори тактової частоти, мережеві комутатори, системи охолодження та інші елементи апаратної інфраструктури. У разі відмови або нестабільної роботи таких компонентів можуть виникати синхронні порушення у роботі всіх каналів системи.

Таким чином, модель вразливостей багатоверсійності описує структурні фактори, які можуть призводити до відмов за спільною причиною. Урахування таких вразливостей є необхідною умовою для коректного оцінювання функційної безпечності багатоверсійних інформаційно-керуючих систем.

Формально множину вразливостей багатоверсійності можна подати як

$$V_{MVS} = V_{spec} \cup V_{sim} \cup V_{inf}\ , \qquad (4.19)$$

де:

- V_{spec} – множина вразливостей спільної специфікації;
- V_{sim} – множина вразливостей подібності реалізацій;
- V_{inf} – множина інфраструктурних вразливостей.

Отримана модель дозволяє систематизувати фактори, що знижують ефективність багатоверсійної надмірності, та створює основу для їх кількісного аналізу під час оцінювання функційної безпечності систем.

4.2.3. Профілювання вразливостей

Розроблена модель вразливостей дозволяє ідентифікувати структурні особливості програмно-апаратних компонентів багатоверсійних ІКС, які визначають їх чутливість до дефектів. Однак для подальшого використання у процедурах аналізу і оцінювання функційної безпечності необхідно перейти від якісного опису вразливостей до їх формалізованого кількісного представлення.

Для переходу від якісного опису вразливостей до їх кількісного аналізу вводиться поняття профілю вразливостей рівня L_k, який позначається як G_{Lk}. На відміну від множини вразливостей V_{Lk}, що відображає лише перелік структурних особливостей системи, профіль G_{Lk} є параметризованим представленням вразливостей, яке включає їх імовірність прояву, критичність, здатність до виявлення та ваговий вплив на функційну безпечність системи.

Визначення 1. *Профіль вразливостей***,** це сукупність параметрів, що характеризують вплив кожної вразливості на процес формування відмов у системі.

Профілювання вразливостей полягає у формуванні структурованого набору характеристик, що описують:

- імовірність прояву вразливості в процесі експлуатації;
- ступінь її впливу на функційну безпечність;
- здатність системи виявляти або компенсувати наслідки її прояву;

- зв’язок вразливості з відповідними дефектами системи.

Профіль вразливостей рівня L_k визначається як множина параметризованих характеристик:

$$G_{L_k} = \{v_{ki}, P_{e_{ki}}, c_{ki}, d_{ki}, \omega_{ki}\}, \quad (4.20)$$

де:

- v_{ki} – і-та вразливість рівня L_k;

- Pe_{ki} – імовірність експлуатаційного прояву вразливості;

- c_{ki} – коефіцієнт критичності (ступінь впливу на безпечність);

- d_{ki} – коефіцієнт виявлення (detectability);

- ω_{ki} – ваговий коефіцієнт, що враховує значущість вразливості в архітектурі системи.

Таким чином, кожна вразливість описується як багатопараметричний об’єкт, що дозволяє враховувати її вплив у подальших розрахунках показників безпечності.

З урахуванням ієрархічної структури системи загальний профіль вразливостей визначається як об’єднання профілів усіх рівнів і профіля вразливостей багатоверсійності:

$$G_L = \bigcup_{k=1}^{4} G_{Lk} \cup G_{MVS}, \quad (4.21)$$

де

- G_{Lk} – профіль вразливостей L_k;

- G_{MVS} – профіль вразливостей багатоверсійності.

4.3. Метод аналізу видів і наслідків відмов багатоверсійних ІКС ППЛ

4.3.1. Узагальнена послідовність методу

Розроблені моделі дефектів програмно-апаратних компонентів багатоверсійних ІКС ППЛ та моделі вразливостей створюють формалізовану

основу для переходу до аналізу відмов багатоверсійних ІКС. На відміну від класичних підходів FMEA/FMECA, які орієнтовані переважно на апаратні компоненти, для програмовних платформ необхідно враховувати [27, 43]:

– багаторівневу природу дефектів (L1–L4);

– наявність трансформацій дефектів між рівнями;

– вплив вразливостей як «підсилювачів» дефектів;

– ефекти багатоверсійності (CCF, correlation, voter effects).

З урахуванням цього пропонується модифікований метод аналізу видів і наслідків відмов багатоверсійних ІКС ППЛ (MVSD-FMEA – Multi-Version Systems Defects FMEA).

Основні етапи метода наступні.

Етап 1. Формування множини дефектів.

На першому етапі методу визначається множина дефектів, що підлягають аналізу, яка формується як об’єднання дефектів розглянутих вище рівнів ієрархії та дефектів багатоверсійності:

$$D = \bigcup_{k=1}^{4} D_{Lk} \cup D_{MVS}, \qquad (4.22)$$

де:

- D_{Lk} – множина дефектів k-го рівня ($L_1 \div L_4$);

- D_{MVS} – множина дефектів, пов’язаних із багатоверсійною архітектурою системи.

Формування множини D здійснюється за наступною процедурою:

- ідентифікація джерел дефектів на кожному рівні ієрархії L1÷L4 (фізичному, проєктно-логічному, архітектурному та системному) на основі аналізу структури програмно-апаратної платформи;

- систематизація типів дефектів відповідно до їх механізмів виникнення (фізичні ефекти, помилки проєктування, інтеграційні конфлікти, мережеві порушення);

- формування множин D_{Lk} у вигляді переліків типізованих дефектів із визначеними параметрами (таблиці 4.1–4.4);

- виділення дефектів багатоверсійності D_{MVS}, що пов’язані зі спільною специфікацією, подібністю реалізацій та інфраструктурою виконання;

- об’єднання отриманих множин у єдину множину дефектів D, яка використовується як вхідні дані для подальших етапів методу.

Таким чином, формування множини дефектів базується на структурно-ієрархічному аналізі системи та забезпечує повноту охоплення можливих джерел відмов.

Етап 2. Формування множини вразливостей.

На другому етапі методу формується множина вразливостей системи, яка відображає структурні та функціональні особливості програмно-апаратної платформи, що визначають її чутливість до дефектів.

Множина вразливостей визначається як:

$$V = \bigcup_{k=1}^{4} V_{Lk} \cup V_{MVS}, \tag{4.23}$$

де:

- V_{Lk} – множина вразливостей k-го рівня ($L_1 \div L_4$);

- V_{MVS} – множина вразливостей, пов’язаних із багатоверсійною архітектурою системи.

Формування множини V здійснюється на основі:

- аналізу архітектури системи;

- виявлення структурних слабких місць (single points of failure, ресурсні конфлікти, часові залежності);

- встановлення відповідності між дефектами та умовами їх прояву.

Таким чином, множина вразливостей визначає умови активації дефектів та є необхідною складовою подальшого аналізу відмов.

Етап 3. Формування профілю дефектів.

На третьому етапі методу визначається профіль дефектів, який описує параметризовані характеристики кожного дефекту, включеного до множини D:

$$\Pi_{L_k} = \{\lambda_{ki}, P_{D,ki}, DC_{ki}, \omega_{ki}, CCF_{ki}\}, \tag{4.24}$$

де:

- λ_{ki} – інтенсивність прояву дефекту;

- $P_{D,ki}$ – ймовірність небезпечного прояву небезпечного дефекту, що може призвести до небезпечної відмови (в ідентифікаторі ймовірності використано означення D – danger (небезпека));

- DC_{ki} – коефіцієнт діагностичного покриття (DC - diagnostic coverage);

- ω_{ki} – ваговий коефіцієнт критичності;

- CCF_{ki} – коефіцієнт відмов за спільною причиною.

Профіль дефектів формується на основі аналітичних моделей та, за необхідності, уточняється експериментально.

Загальний профіль дефектів визначається як:

$$\Pi = \bigcup_{k=1}^{4} \Pi_{Lk} \cup \Pi_{MVS} \tag{4.25}$$

Формування профілю дефектів здійснюється на основі:

- аналітичних моделей дефектів (розділ 4.1);

- статистичних даних експлуатації (за наявності);

- результатів експериментальних досліджень;

- експертного оцінювання (для початкових етапів).

Вирази для визначення параметрів профілю дефектів наступні.

1. Інтенсивність прояву дефектів визначається як частота, а саме:

$$\lambda_{ki} = \frac{N_{ki}}{T} \tag{4.26}$$

де N_{ki} – кількість реалізацій (проявів), дефектів типу d_{ki} за час спостереження T.

2. Ймовірність небезпечного прояву.

$$P_{D,ki} = \frac{N_{ki}^{danger}}{N_{ki}} \quad (4.27)$$

де N_{ki}^{danger} – кількість реалізацій (проявів) небезпечних дефектів типу d_{ki}.

3. Діагностичне покриття.

$$DC_{ki} = \frac{N_{ki}^{det}}{N_{ki}} \quad (4.28)$$

де N_{ki}^{det} – кількість виявлених дефектів типу d_{ki}.

4. Ваговий коефіцієнт критичності - $\omega \in [0,1]$.

5. Коефіцієнт відмов за спільною причиною.

$$CCF_{ki} = \frac{N_{ki}^{ccf}}{N_{ki}} \quad (4.29)$$

де N_{ki}^{ccf} – кількість випадків одночасної відмови кількох каналів в наслідок прояву дефектів типу d_{ki}.

Показник CCF або β-фактор [X]:

$$\beta_{ki} = \frac{\lambda_{CCF}}{\lambda_{total}} \quad (4.30)$$

Етап 4. Формування профілю вразливостей.

На четвертому етапі визначається профіль вразливостей системи, який відображає структурні фактори, що впливають на прояв дефектів:

$$G_{Lk} = \{v_{ki}, Pe_{ki}, c_{ki}, d_{ki}, \varphi_{ki}\}, \quad (4.31)$$

де:

- v_{ki} – і-та вразливість рівня L_k;
- Pe_{ki} – ймовірність прояву вразливості;
- c_{ki} – ваговий коефіцієнт критичності вразливості;
- d_{ki} – коефіцієнт виявлення;

- φ_{ki} – ваговий коефіцієнт значущості.

Маємо загальний профіль:

$$G = \bigcup_{k=1}^{4} G_{Lk} \cup G_{MVS}, \tag{4.32}$$

де G_{MVS}– профіль вразливостей багатоверсійності.

Вирази для визначення параметрів профілю вразливостей наступні.

1. Ймовірність прояву вразливості доцільно визначати як відносну частоту випадків, у яких відповідна структурна слабкість реально активується в процесі функціонування або випробувань:

$$P_{e,ki} = \frac{N_{ki}^{act}}{N_{ki}^{obc}}, \tag{4.33}$$

де: N_{ki}^{act} – кількість випадків активації прояву вразливості; N_{ki}^{obs} - загальна кількість спостережень, випробувань або сценаріїв, у яких ця вразливість могла проявитися. Якщо $P_{e,ki} \to 0$ – вразливість практично не проявляється, $P_{e,ki} \to 1$ – вразливість проявляється в кожному релевантному сценарії.

2. Коефіцієнт критичності доцільно пов’язати з тяжкістю наслідків, до яких може призвести прояв вразливості. У нормованому вигляді:

$$c_{ki} = \frac{S_{ki}}{S_{max}}, \tag{4.34}$$

де: S_k – оцінка тяжкості наслідків прояву вразливості; S_{max} – максимально можливе значення шкали тяжкості.

Наприклад.

Якщо використовується 5-рівнева шкала:

1 – незначний вплив;

2 – малий вплив;

3 – помірний вплив;

4 – суттєвий вплив;

5 – критичний вплив.

то:

$$c_{ki} = \in \{\frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, 1\}$$

3. Коефіцієнт виявлення, dki ∈[0,1] - – коефіцієнт виявлення вразливості і-го типу на рівні L_k, що характеризує ймовірність своєчасного виявлення засобами діагностики, моніторингу або верифікації до моменту його трансформації у небезпечну відмову.

4. Ваговий коефіцієнт значущості.

Цей коефіцієнт відображає відносну важливість вразливості в межах відповідного рівня ієрархії або всієї системи. Його доцільно вводити як нормовану вагу:

$$\varphi_{ki} = \frac{\omega_{ki}}{\sum_{i=1}^{n_k} \omega_{ki}}, \quad (4.35)$$

де: ω_{ki} – ненормована оцінка значущості вразливості; n_k – кількість вразливостей на рівні L_k.

Етап 5. Моделювання трансформації дефектів.

На п’ятому етапі методу здійснюється моделювання процесів трансформації дефектів між рівнями ієрархії системи, що дозволяє встановити причинно-наслідкові ланцюги формування системних відмов.

Процес переходу дефектів між рівнями описується операторами трансформації:

$$T_{k,k+1} : D_{L_k} \to D_{L_{k+1}} \quad (4.36)$$

Для окремого дефекту:

$$d_{k+1,i} = T_{L_k} \to_{L_{k+1}} (d_{k,i}), \quad (4.37)$$

де: $d_{k,i}$ – дефект рівня L_k; $d_{k+1,I}$ – трансформований дефект рівня

L_{k+1}.

Трансформація дефектів має стохастичний характер, оскільки: не кожен дефект активується; не кожна вразливість проявляється; архітектура системи може локалізувати дефект; механізми діагностики можуть перервати ланцюг трансформації.

Тому кожному переходу ставиться у відповідність умовна ймовірність:

$$P_{k,k+1} = P(L_{k+1} | L_k), \quad (4.38)$$

де $P_{k,k+1}$ – ймовірність того, що дефект рівня L_k трансформується у дефект рівня L_{k+1}.

Етап 6. Формування видів відмов.

Головна ідея етапу полягає в тому, що не кожен дефект або вразливість призводить до відмови системи. Відмова виникає лише у випадку активації вразливості, яка формується на основі одного або сукупності дефектів (трансформації дефектів). Таким чином, кожна відмова є результатом реалізації дефектів через відповідні вразливості за певних умов функціонування системи.

Не кожен дефект і не кожна вразливість призводять до відмови. Відмова є результатом реалізації одного або комбінації дефектів, умови прояву яких формуються відповідними вразливостями системи. Тобто, дефекти визначають потенційні джерела порушень; вразливості визначають умови їх активації; механізми трансформації визначають шлях поширення дефектів; відмова є кінцевим системним ефектом.

Множина видів відмов системи задається:

$$F = \{f_j\}, \quad (4.39)$$

де f_j – j -та відмова системи, j=1,…,N_f.

Кожна відмова формується як результат відображення:

$$f_j = \Phi\{\Pi, G, T\}, \quad (4.40)$$

де: *П* - профіль дефектів (етап 3); *G* – профіль вразливостей (етап 4), *T* – оператор трансформації дефектів (етап 5).

Маємо декартовий добуток множин, а саме:

$$\Pi \times G \times T = \{(d, v, t) |\ d \in D, v \in G, t \in T\} \qquad (4.41)$$

Тобто це множина всіх можливих комбінацій: профілю дефектів; профілю вразливостей; механізму трансформації.

Таким чином відмова є композицією трьох факторів: наявності профілю дефектів; наявністю профілю вразливостей; реалізації шляху трансформації.

На основі багаторівневої моделі дефектів та моделі багатоверсійності вводиться класифікація відмов.

Можливі два варіанти відображень.

Етап 6.1.

Варіант 1. Детерміноване відображення.

$$(d, v, t) \to f_j \qquad (4.42)$$

Тобто кожна комбінація дає одну відмову

Варіант 2. Стохастичне відображення.

$$\Phi(d, v, t) = P(f_j |\ d, v, t\} \qquad (4.43)$$

Етап 6.2.

Відмови одиничного каналу (Single Channel Failures). Формуються внаслідок прояву дефектів і вразливостей рівнів L1-L4 в одному з каналів багатоверсійної системи. Формально маємо:

$$F_{SC} = \{f_{sc,i}\}, \qquad (4.44)$$

де $f_{sc,\,i}$ – відмова окремого каналу (Single Channel).

Дефекти мають локальний характер і, як праило, компенсуються механізмами багатоверсійності, а саме: мажоритарним голосуванням; резервуванням; реконфігурацією каналу; діагностико тощо.

Етап 6.3.

- Відмови координації (Coordination Failures). Формуються внаслідок прояву дефектів voter, розсинхронізації, помилки протоколів. Впливають на узгодженість каналів. Компенсуються механізмами забезпечення узгодженості, а саме: механізмами синхронізації; діагностикою; timeout-механізмами; механізмами реконфігурації.

$$F_{coord} = \{f_{coord,i}\}, \tag{4.45}$$

де $f_{coord,\,i}$ – відмова координації окремого каналу.

Етап 6.4.

- Відмови за спільною причиною (Common Cause Failures, CCF). Такі відмови є найбільш небезпечним класом відмов багатоверсійних ІКС. Вони формуються внаслідок: дефектів спільної специфікації; дефектів «ідентичності»; спільної інфраструктури; спільного живлення; спільного тактування; спільних IP-ядер тощо. Формально маємо:

$$F_{CCF} = \{f_{ccf,i}\} \tag{4.46}$$

де $f_{ccf,\,i}$ – відмова за спільною причиною.

CCF не компенсуються класичними механізмами резервування (мажоритуванням). Їх можна лише зменшити (mitigate), але не повністю компенсувати.

Етап 6.5.

- Каскадні відмови (Cascading Failures). Відмови накопичення ефектів між рівнями.

$$F_{cascad} = \{f_{cas,i}\} \tag{4.47}$$

Механізм формування наступний: L1→L2→L3→L4→*f*.

Тоді маємо узагальнену модель множини відмов.

$$F = F_{SC} \cup F_{coord} \cup F_{ccf} \cup F_{cascad} \quad (4.48)$$

Таким чином, запропонована класифікація відмов дозволяє формалізувати різні механізми порушення функціонування багатоверсійних ІКС та встановити їх внесок у показники функційної безпечності. На відміну від класичних FMEA-моделей, запропонований підхід враховує не лише локальні дефекти компонентів, але й механізми координації, багаторівневі процеси трансформації дефектів та відмови за спільною причиною, що є критичними для систем класу SIL3–SIL4.

Етап 7. Класифікація наслідків відмов.

Після визначення множини можливих відмов багатоверсійної ІКС виконується аналіз їх наслідків. Метою цього етапу є визначення ступеня впливу кожної відмови на виконання функцій безпеки системи та формування вихідних даних для подальшого оцінювання критичності. На відміну від класичного FMEA, де аналізуються переважно локальні наслідки окремих відмов компонентів, у запропонованому методі MVSD-FMEA наслідки оцінюються з урахуванням багаторівневої архітектури програмовних платформ та механізмів багатоверсійності. Для кожної відмови $f_i \in F$ визначається множина наслідків

$$C(f_i) = \{c_{i1}, c_{i2}, ..., c_{im}\}, \quad (4.49)$$

де c_{ij} – j -й наслідок відмови f_i.

Наслідки можливо класифікувати за наступними ознаками.

1. Локальні наслідки (Local Effects).

Відмова впливає лише на окремий функціональний модуль (unit) або один канал багатоверсійної ІКС.

2. Платформені або архітектурні наслідки (Platform Effects).

Відмова поширюється на рівень програмовної платформи та порушує взаємодію між компонентами. Прикладами таких наслідків є: блокування системної шини; порушення протоколів обміну тощо.

3. Системні наслідки (System Effects).

Відмова призводить до порушення функціонування всієї багатоканальної ІКС. Прикладами системних наслідків є наступні: відмова механізму голосування; втрата синхронізації каналів.

4. Наслідки для функційної безпечності (Safety Effects).

Найбільш критичним класом є наслідки, що безпосередньо впливають на виконання функцій безпеки, а саме: небезпечна невиявлена відмова (Dangerous Undetected Failure); небезпечна виявлена відмова (Dangerous Detected Failure); безпечна відмова (Safe Failure) - помилкове спрацювання захисту; невиконання функції захисту.

Приклад підходу до кількісної оцінки тяжкості наслідків наведено в ході опису етапу 4 даного методу.

Таким чином, результатом етапу 7 методу є формування множини наслідків відмов.

$$C = \bigcup_{i=1}^{n} C(f_i), \qquad (4.50)$$

яка використовується для визначення критичності відмов та побудови підсумкової таблиці MVSD-FMEA.

Етап 8. Формування таблиці MVSD-FMEA.

На восьмому етапі результати формування множини дефектів, профілювання дефектів і вразливостей, моделювання трансформацій, формування видів відмов та класифікації їх наслідків інтегруються в узагальнену таблицю MVSD-FMEA (таблиця 4.9). На відміну від традиційної таблиці FMEA, запропонована таблиця враховує: багаторівневу модель дефектів; модель вразливостей; механізми трансформації дефектів; багатоверсійність системи; відмови за спільною причиною; показники

функційної безпечності. Для кожного елемента системи маємо набір компонент таблиці MVSD-FMEA, а саме:

e_i – компонент системи;

d_i – дефект;

v_i – відповідна вразливість;

f_i – сформована відмова;

c_i – наслідок відмови;

Si – тяжкість наслідків;

P_i – імовірність виникнення;

Di – можливість виявлення;

CCF_i – коефіцієнт відмов за спільною причиною;

RPN_i – інтегральний показник ризику і-го виду відмови (Risk Priority Number), який комплексно враховує тяжкість наслідків відмови, ймовірність її виникнення, складність виявлення, а також, залежно від запропонованої моделі MVSD-FMEA, додаткові фактори взаємодії множинних відмов. Значення RPN_i використовується для кількісного ранжування ризиків і визначення пріоритетності і заходів щодо їх усунення або зниження.

Таблиця 4.10 надає пояснення до всіх елементів узагальненої таблиці.

Для класичних випадків маємо:

$$RPN_i = S_i \times P_i \times D_i, \tag{4.51}$$

де:

- e_i – компонент системи визначає де саме розглядається дефект $e_i \in E$. Це може бути функціональний модуль, FPGA-компонент, канал, voter тощо;
- L_k – показує положження дефекту в багаторівневій моделі L_k, k=1,…,4;

Таблиця 4.9 – Узагальнена таблиця MVSD-FMEA

Ідентифікація та структура						Трансформація та формування відмови			Наслідки та функційна безпечність					Виявлення та CCF			Інтегральна оцінка		
№	e_i	L_k	d_i	v_i	$P_{v,i}$	τ_i	$P_{T,i}$	f_i	λ_{fi}	P_i	c_i	S_i	$P_{D,i}$	DC_i	D_i	CCF_i	ω_i	RPN$_i$	Клас відмови

Таблиця 4.10 – Складові узагальненої таблиці MVSD-FMEA

№	**Складова**	**Позначення**	**Що означає**	**Звідки береться**
1	Компонент системи	e_i	Елемент ІКС, у якому проявляється дефект	Етапи 1–2
2	Рівень дефекту	L_k	Рівень багаторівневої моделі L_1-L_4	Етап 1
3	Дефект	d_i	Конкретний тип дефекту	Етап 2
4	Вразливість	v_i	Структурна або функційна умова, що сприяє прояву дефекту	Етап 4
5	Імовірність прояву вразливості	$P_{v,i}$	Імовірність активації вразливості	Етап 4
6	Шлях трансформації	τ_i	Послідовність переходів дефекту між рівнями	Етап 5

№	Складова	Позначення	Що означає	Звідки береться
7	Імовірність трансформації	$P_{T,i}$	Імовірність реалізації відповідного шляху трансформації	Етап 5
8	Вид відмови	f_i	Сформована відмова системи	Етап 6
9	Інтенсивність системної відмови	λ_{fi}	Інтенсивність (прояву) формування конкретної системної відмови	Етапи 3–6
10	Імовірність виникнення	P_i	Імовірність виникнення f_i за заданий час T	Етапи 3–6
11	Наслідок	c_i	Наслідок відмови для компонента, платформи, системи або функції безпеки	Етап 7
12	Тяжкість наслідку	S_i	Нормована характеристика тяжкості наслідку	Етап 7
13	Імовірність небезпечного прояву	$P_{D,i}$	Імовірність того, що прояв дефекту призведе до небезпечної відмови	Етап 3
14	Діагностичне покриття	DC_i	Частка / імовірність виявлення дефекту	Етап 3
15	Коефіцієнт невиявлення	D_i	Частина відмов, яка залишається невиявленою; Di=1-DCi	Етап 8

№	Складова	Позначення	Що означає	Звідки береться
16	CCF	CCF_i	Коефіцієнт відмови за спільною причиною	Етап 3 / Етап 6
17	Ваговий коефіцієнт критичності	ω_i	Вага критичності дефекту / відмови для функційної безпечності	Етап 3
18	Інтегральний показник ризику	RPN_i	Узагальнена оцінка пріоритетності відмови	Етап 8
19	Клас відмови	–	Single Channel, Coordination, CCF, Cascading; Safe / Dangerous; Detected / Undetected	Етапи 6–7

- d_i – конкретний дефект, визначений на відповідному рівні: $d_i \in D$. Він є початковою точкою причинно-наслідкового ланцюга;

- v_i – вразливість $v_i \in V$. Вразливість визначає умову, за якою дефект може проявитися;

- $P_{v,i}$ - імовірність прояву вразливості, визначається через частоту активації вразливості;

- τ_i – шлях трансформації $L_1 \rightarrow L_2 \rightarrow L_3 \rightarrow L_4$;

- $P_{T,i}$ – імовірність реалізації шляху. Для шляху $L_1 \rightarrow L_2 \rightarrow L_3 \rightarrow L_4$ маємо $P_{T,i} = P_{12}P_{23}P_{34}$;

- f_i – вид відмови. Це результат реалізації дефекту через вразливість та трансформацію;

- λ_{fi} – інтенсивність системної відмови. Це кількісний зв'язок із профілем дефектів. Формується із інтенсивності початкового дефекту (λ_{di}), ймовірностей його прояву через вразливості і шлях трансформації. Зазначимо, що не кожний прояв d_i призводить до системної відмови (він повинен активувати відповідну вразливість, пройти відповідний механізм трансформації, досягнути стану, який буде класифіковано як відмову f_i, тобто в загальному випадку $\lambda_{di} \neq \lambda_{fi}$);

- P_i – імовірність виникнення відмови, де $P_i = P(f_i \leq T)$, за експоненційною моделлю маємо $P_i = 1 - e^{-\lambda fiT}$;

- c_i – наслідок відмови, показує, що відбувається внаслідок f_i;

- S_i – тяжкість наслідку, нормована характеристика тяжкості наслідку $0 \leq S_i \leq$;

- $P_{D,i}$ – імовірність небезпечного прояву $P_{D,ki} = N_{ki}^{danger} / N_{ki}$, $P_{D,ki} \neq P_i$;

- DC_i – діагностичне покриття, показує здатність системи (підсистеми) діагностування виявити відповідний дефект або відмову;

- Di - коефіцієнт невиявлення. Важливо розуміти, що чим гірше відмова виявляється тим більший пріоритет її ризику;

- CCF_i - коефіцієнт відмови за спільною причиною. Характеризує частку випадків, у яких прояв дефекту призводить до одночасної відмови кількох каналів;

- ω_i - ваговий коефіцієнт критичності $\omega_i \in [0,1]$;

- RPN_i – інтегральний показник ризику, обчислюється:

$$RPN_i = S_i P_i D_i (1 + \omega_i CCF_i), \quad (4.52)$$

Таким чином, метод описуэться наступним ланцюгом:

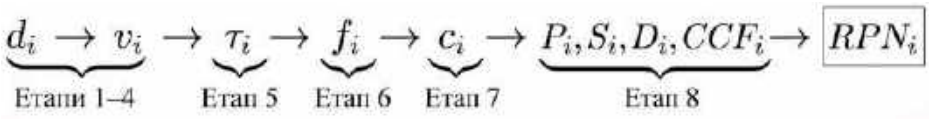


Рисунок 4.1 – Узагальнена послідовність методу аналізу видів і наслідків відмов багатоверсійних ІКС ППЛ

4.3.2. Кількісне оцінювання показників функційної безпечності

Завершальним результатом етапу 8 запропонованого методу є інтегрована таблиця MVSD-FMEA, яка об'єднує результати аналізу дефектів, вразливостей, механізмів їх трансформації, сформованих видів відмов та наслідків для багатоверсійної ІКС. На основі сформованої таблиці здійснюється подальший перехід від оцінювання критичності окремих відмов до кількісного оцінювання функційної безпечності системи. Такий перехід є необхідним, оскільки отриманий на попередньому етапі показник RPN_i характеризує пріоритетність відмови та використовується для їх ранжування, але сам по собі не визначає кількісні показники функційної безпечності.

Для реалізації такого переходу таблиця MVSD-FMEA розширюється показниками, безпосередньо пов'язаними з функційною безпечністю. До кожного виду відмови fi, поряд із параметрами Si, P_i, Di, CCFi та інтегральним показником RPN_i, додаються її класифікація за режимом відмови, інтенсивність формування відмови λ_{fi}, а також відповідні складові інтенсивності небезпечних і безпечних відмов. Це дозволяє безпосередньо використовувати результати MVSD-FMEA для подальшого розрахунку DC, SFF, PFH та PFDavg.

Таким чином, формується розширена таблиця MVSD-FMEA з оцінюванням функційної безпечності, яка є основним інформаційним носієм

переходу від аналізу видів і наслідків відмов до кількісних показників безпечності. Її структура забезпечує простежуваність результатів за ланцюгом:

дефект→вразливість→шлях трансформації→відмова→ RPN_i→режим відмови→ λ_{fi} →показники функційної безпечності.

При цьому RPN_i зберігає свою функцію пріоритезації відмов, тоді як кількісні параметри λ_{fi}, DU/DD/SU/SD, DC, SFF, PFH та PFDavg [] використовуються для безпосереднього оцінювання функційної безпечності.

Для переходу від множини відмов F до показників функційної безпечності кожна відмова класифікується відповідно до її впливу на виконання функції безпеки. Вводиться множина класів (режимів):

$$K = \{DU, DD, SU, SD\}, \tag{4.53}$$

де:

- DU – Dangerous Undetected – небезпечна невиявлена відмова;
- DD – Dangerous Detected – небезпечна виявлена відмова;
- SU – Safe Undetected – безпечна невиявлена відмова;
- SD – Safe Detected – безпечна виявлена відмова.

Для кожної відмови f_i визначається відображення:

$$k : F \to K, \tag{4.54}$$

яке встановлює її належність до одного з чотирьох режимів.

На основі класифікації відмов визначаються сумарні інтенсивності для кожного класу (режиму):

$$\lambda_{DU} = \sum_{f_i \in F_{DU}} \lambda_{f_i}, \tag{4.55}$$

$$\lambda_{DD} = \sum_{f_i \in F_{DD}} \lambda_{f_i}, \tag{4.56}$$

$$\lambda_{SU} = \sum_{f_i \in F_{SU}} \lambda_{f_i}, \tag{4.57}$$

$$\lambda_{SD} = \sum_{f_i \in F_{SD}} \lambda_{f_i}, \tag{4.58}$$

При цьому:

$$\lambda_D = \lambda_{DU} + \lambda_{DD}, \tag{4.59}$$

$$\lambda_S = \lambda_{SU} + \lambda_{SD}, \tag{4.60}$$

а загальна інтенсивність відмов визначається як:

$$\lambda_S = \lambda_{SU} + \lambda_{SD}, \tag{4.61}$$

Такий поділ дозволяє безпосередньо пов'язати результати MVSD-FMEA з показниками функційної безпечності.

Для оцінювання архітектурної здатності системи локалізувати небезпечні відмови вводиться показник Safe Failure Fraction (SFF):

$$SFF = 1 - \frac{\lambda_{DU}}{\lambda_{SU} + \lambda_{SD} + \lambda_{DU} + \lambda_{DD}}, \tag{4.62}$$

Для багатоверсійної ІКС особливе значення має відмова за спільною причиною CCF, оскільки вона може одночасно порушити функціонування декількох незалежних версій.

Для кількісного оцінювання використовується вираз:

$$\lambda_{CCF} = \sum_{f_i \in F_{CCF}} \lambda_{f_i}, \tag{4.62}$$

Тоді сумарна інтенсивність небезпечних відмов системи може бути представлена як:

$$\lambda_{D,sys} = \lambda_{D,ind} + \lambda_{D,CCF} + \lambda_{D,coord} + \lambda_{D,cas}, \quad (4.64)$$

де:

- $\lambda_{D,ind}$ – внесок незалежних небезпечних відмов каналів;

- $\lambda_{D,CCF}$ – внесок небезпечних відмов за спільною причиною;

- $\lambda_{D,coord}$ – внесок небезпечних відмов механізмів координації, зокрема voter та синхронізації;

- $\lambda_{D,cas}$ - внесок небезпечних відмов, що виникають унаслідок послідовної трансформації первинної відмови в наступні відмови компонентів або каналів.

Це є принципово важливим саме для запропонованого методу, оскільки в даній CCF визначено як найбільш небезпечний клас відмов багатоверсійної ІКС, який не компенсується звичайним мажоритуванням.

Для режиму низької частоти запитів до виконання функції безпеки основним показником є середня ймовірність небезпечної відмови при виконанні вимоги – PFDavg.

У загальному вигляді маємо:

$$PFD_{avg} = \frac{1}{T}\int_0^T P_{DF}(t)dt, \quad (4.65)$$

де:

- T – інтервал між proof-test. Це спеціально заплановане випробування (тестування) Safety Instrumented Function (SIF) або safety system, яке проводиться через певні інтервали часу T, щоб виявити відмови, які не виявляються автоматично діагностикою;

- $P_{DF}(t)$ – імовірність того, що система перебуває у небезпечному стані в момент t.

Для найпростішого випадку одиничної функції з постійною інтенсивністю небезпечних невиявлених відмов і періодичним тестуванням маєм:

$$PFD_{avg} \approx \frac{\lambda_{DU} T}{2} \tag{4.66}$$

Однак для багатоверсійної ІКС ця залежність повинна бути розширена, оскільки система має структурну надмірність, механізми голосування та CCF. Тому для запропонованого методу доцільно визначати:

$$PFD_{avg,sys} = \frac{1}{T}\int_0^T P_{DF,sys}(t)dt, \tag{4.67}$$

де $P_{DF,sys}(t)$ формується з урахуванням структури багатоверсійної системи, одиничних відмов каналів, відмов координації та CCF.

Для режиму високої частоти вимог або безперервної роботи основним показником є PFH – Probability of dangerous Failure per Hour. PFH використовується IEC 61508 як показник імовірності небезпечної відмови для high-demand/continuous mode.

$$PFH_{sys} = \lambda_{D,sys}, \tag{4.68}$$

де $\lambda_{D,sys}$ визнається виразом (4.64), тоді маємо:

$$PFH_{sys} = \sum_{i \notin F_{DU}} \lambda_{DU,i} + \lambda_{D,CCF} + \lambda_{D,coord} + \lambda_{D,cas}, \tag{4.69}$$

де:

- $\sum_{i \notin F_{DU}} \lambda_{DU,i}$ - сумарна інтенсивність незалежних небезпечних невиявлених відмов окремих каналів або компонентів системи. Кожна $\lambda_{DU,i}$ визначається для відповідного виду відмови f_i, класифікованого як DU (Dangerous Undetected). Така класифікація та сумування $\lambda_{DU,i}$ безпосередньо передбачені поточною MVSD-FMEA;

- $\lambda_{D,CCF}$ - інтенсивність небезпечних відмов за спільною причиною (Common Cause Failure, CCF), які можуть одночасно впливати на декілька незалежних версій системи;

- $\lambda_{D,coord}$ - інтенсивність небезпечних відмов механізмів координації багатоверсійної системи, зокрема voter, механізмів синхронізації та інших функцій взаємодії між каналами;

- $\lambda_{D,cas}$ - інтенсивність небезпечних каскадних відмов, що виникають унаслідок послідовної трансформації первинної відмови в наступні відмови компонентів або каналів і в результаті призводять до небезпечної системної відмови.

Таблиці 4.11, 4.12 надають детальну інформацію для кількісного оцінювання показників функційної безпечності ІКС, а таблиця 4.13 представляє результати аналізу відповідного якісного ефекту від застосування методу. Отже, якісний ефект застосування метода BMVSD-FMEA полягає у розширенні та поглибленні аналізу за рахунок врахування не лише окремих причин відмов, а й механізмів їх трансформації, системних вразливостей та взаємозалежності версій. Це дозволяє виявляти такі сценарії відмов, які можуть залишатися поза межами традиційного FMEA/FMECA, зокрема корельовані, спільні та каскадні відмови. Результати аналізу при цьому безпосередньо використовуються для подальшого кількісного оцінювання функційної безпечності за показниками DC, SFF, PFH та PFDavg.

Науковий результат полягає у формуванні інтегрованого методу оцінювання функційної безпечності багатоверсійних ІКС на програмовних платформах, який об’єднує багаторівневе моделювання дефектів, моделювання вразливостей, аналіз механізмів трансформації, урахування багатоверсійності та кількісне оцінювання показників функційної безпечності. На відміну від підходів, у яких аналіз дефектів, FMEA та кількісна оцінка безпечності розглядаються як відносно відокремлені процедури, запропонований метод встановлює між ними формальний причинно-наслідковий зв’язок. Це підвищує повноту аналізу потенційних сценаріїв відмов та забезпечує більш обґрунтоване визначення їх впливу на функційно безпечну поведінку багатоверсійної ІКС.

Таблиця 4.11 – Розширена таблиця MVSD-FMEA з оцінюванням функційної безпечності

№	RPN	Пріоритет	Failure ModeDU/DD/SU/SD	λf_i	$\lambda_{DU,i}$	$\lambda_{DD,i}$	$\lambda_{SU,i}$	$\lambda_{SD,i}$	DC
1	RPN_1	High	DU	λ_{f1}	$\lambda_{DU,1}$	0	0	0	DC_1
2	RPN_2	Medium	DD	λ_{f2}	0	$\lambda_{DD,2}$	0	0	DC_2
3	RPN_3	Medium	SU	λ_{f3}	0	0	$\lambda_{SU,3}$	0	–
4	RPN_4	Critical	SD	λ_{f4}	0	0	0	$\lambda_{SD,4}$	–

Таблиця 4.12 – Складові розширеної таблиці MVSD-FMEA та підсумкові показник функційної безпечності

Показник	Позначення	Розрахунок/джерело
Сумарна інтенсивність небезпечних невиявлених відмов	λ_{DU}	$\Sigma \lambda_{DU,i}$
Сумарна інтенсивність небезпечних виявлених відмов	λ_{DD}	$\Sigma \lambda_{DD,i}$
Сумарна інтенсивність безпечних невиявлених відмов	λ_{SU}	$\Sigma \lambda_{SU,i}$
Сумарна інтенсивність безпечних виявлених відмов	λ_{SD}	$\Sigma \lambda_{SD,i}$
Діагностичне покриття	DC	$\lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$
Частка безпечних відмов	SFF	$1 - (\lambda_{DU} / (\lambda_{SU}+\lambda_{SD}+\lambda_{DU}+\lambda_{DD})$
Небезпечна інтенсивність відмов	λ_D	$\lambda_{DU} + \lambda_{DD}$
Імовірність небезпечної відмови за годину	PFH	За структурною моделлю системи
Середня ймовірність небезпечної відмови при вимозі	PFDavg	За моделлю режиму low demand
Досягнутий рівень функційної безпечності	SIL 1-4	За PFH / PFDavg з урахуванням архітектурних обмежень

Таблиця 4.13 – Якісна оцінка ефекту застосування методу MVSD-FMEA

Критерій	**Традиційний FMEA/FMECA**	**Запропонований MVSD-FMEA**	**Якісний ефект**
Джерела дефектів	Переважно окремі компоненти	L1–L4 + дефекти багатоверсійності	Розширення простору аналізу
Взаємозв'язок дефектів	Переважно «причина - відмова»	Ланцюги трансформації L1 → L2 → L3 → L4	Виявлення прихованих шляхів формування відмов
Вразливості	Не виділяються або враховуються опосередковано	Вразливість є окремим елементом моделі та метода	Врахування умов, що підсилюють прояв дефекту
Багатоверсійність	Обмежене врахування	Кореляція, similitude, CCF, voter effects	Виявлення одночасних відмов каналів
Каскадні відмови	Обмежене представлення	Формалізуються через трансформацію дефектів	Виявлення системних наслідків
Пріоритезація	RPN	RPN + CCF + критичність + параметри функційної безпечності	Більш обґрунтоване ранжування
Кількісна оцінка	Потребує окремого переходу	Безпосередній перехід до DC, SFF, PFH, PFDavg	Замикання ланцюга «дефект - відмова - показник функційної безпечності»

4.4. Аналіз результатів впровадження

Напрями практичного впровадження результатів досліджень в індустрії ілюструється рисунками 4.2 (розроблення та оцінка), 4.3 (сертифікація).

Рисунок 4.2 – Напрями, за якими виконано практичне впровадження при розробленні і верифікації платформних рішень ІКС АЕС

Рисунок 4.3 – Напрями, за якими виконано практичне впровадження при сертифікації і експлуатації ІКС АЕС

. На рисунку 4.4 представлено зразки апаратури та засобів для верифікації методом інєктування дефектів.

Рисунок 4.4 – Зразки модулів сертифікованої платформи RadICS та елементів стенда для її верифікації шляхом інєктування дефектів

Отримані наукові й практичні результати використовувались впродовж 2012-2026 років при розробленні інформаційно-керуючих систем АЕС на НВП «Радій» на базі програмовної платформи RadICS. Для оцінювання відповідних платформних рішень на базі результатів досліджень розроблено відповідні FMECA-FMEDA методики та їх модифікації для двохверсійних систем. Розроблено та впроваджено відповідні стандарти підприємства. Крім того, запропоновані моделі та методи використовувалися в процесі сертифікації програмовних платформ інформаційно-керуючих систем на відповідність вимогам стандартів IEC 61508 та вимог американського ядерного регулятора (US Nuclear Regulatory Committee).

Використання наукових результатів надало змогу забезпечити повноту і достовірність оцінок, якість процесів верифікації і валідації платформних

рішень для ІКС АЕС. Вторинним ефектом є зменшення часових витрат на проходження сертифікаційниз процедур. Кінцевим результатом є підвищення безпеки завдяки зменшення ризиків прихованих дефектів і дефектів, які можуть бути джерелом відмов за загальною причиною.

Кількісні оцінки підвищення повноти оцінюються додатковими ситуаціями можливих відмов, які перевіряються, і помилками експертів, які не впливатимуть на кінцеву оцінку функційної безпечності. За оцінками на базі метрик, представлених в розділі 2, таке підвищення повноти і достовірності оцінювання може досягати 25-30% (відносне зменшення ймовірності прихованих дефектів і помилок).

Крім того, результати досліджень впроваджено в низці курсів, які викладалися на кафедрі кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «ХАІ» впродовж 2017-2026 років для бакалаврів, магістрів і аспірантів за спеціальностями «Комп’ютерна інженерія» та «Кібербезпека і захист інформації».

4.5. Висновки до розділу

1. Сформовано багаторівневу модель дефектів програмно-апаратних компонентів багатоверсійних ІКС на програмовних логічних платформах, яка охоплює фізичний (L1), проєктно-логічний (L2), архітектурно-платформний (L3) та системно-мережевий (L4) рівні. Для кожного рівня визначено типи дефектів, причини їх виникнення, параметри прояву та потенційний вплив на функційну безпечність. Такий підхід дозволяє перейти від розгляду окремих компонентних відмов до системного представлення простору дефектів та їх причинно-наслідкових зв’язків.

2. Розроблено модель дефектів і вразливостей багатоверсійності, яка доповнює традиційне представлення відмов специфічними для багатоверсійних ІКС факторами: дефектами спільної специфікації, подібністю реалізацій та спільною інфраструктурою виконання. Показано,

що багатоверсійність сама по собі не гарантує підвищення функційної безпечності, якщо різні версії мають спільні систематичні дефекти або залежності, здатні спричинити корельовані та спільні відмови.

3. Формалізовано механізм трансформації дефектів між рівнями ієрархії. Запропоноване представлення описує причинно-наслідковий ланцюг від первинного фізичного або проєктного дефекту до системної відмови через послідовність переходів L1→L2→L3→L4. У результаті дефект розглядається не як ізольована подія, а як початок потенційного каскадного процесу формування небезпечної відмови. Це створює формальну основу для визначення ймовірності трансформації та інтенсивності системної відмови.

4. Розроблено модель профілювання дефектів і вразливостей, яка забезпечує перехід від їх якісного опису до параметризованого представлення. До профілю включено інтенсивність виникнення дефекту, імовірність небезпечного прояву, діагностичне покриття, критичність та коефіцієнт відмов за спільною причиною. Для вразливостей додатково враховуються ймовірність їх прояву, критичність та можливість виявлення.

5. Запропоновано метод MVSD-FMEA (Multi-Version Systems Defects FMEA) для аналізу видів і наслідків відмов багатоверсійних ІКС. На відміну від традиційних FMEA/FMECA, метод інтегрує багаторівневу модель дефектів, модель вразливостей, механізми трансформації дефектів, особливості багатоверсійної архітектури, корельовані та CCF-відмови.

6. Сформовано інтегровану структуру таблиці MVSD-FMEA, яка встановлює безпосередній зв’язок між компонентом системи, рівнем і типом дефекту, вразливістю, шляхом трансформації, сформованою відмовою, її наслідками, можливістю виявлення, CCF та інтегральним показником ризику RPN. Таким чином, запропонований метод забезпечує простежуваний ланцюг «дефект → вразливість → трансформація → відмова → наслідок → критичність → показник функційної безпечності».

7. Обґрунтовано якісний ефект застосування MVSD-FMEA порівняно з традиційними FMEA/FMECA. Запропонований метод розширює простір

аналізу за рахунок L1–L4 та дефектів багатоверсійності, дозволяє виявляти приховані шляхи трансформації дефектів, враховувати системні вразливості, кореляцію версій, CCF та ефекти механізму голосування. Це забезпечує виявлення сценаріїв корельованих, спільних і каскадних відмов, які можуть бути недостатньо представлені у традиційному аналізі.

8. Встановлено формальний перехід від аналізу критичності відмов до кількісної оцінки функційної безпечності. Показник RPN використовується для ранжування та визначення пріоритетності відмов, але не підміняє кількісні показники функційної безпечності. На основі інтегрованої таблиці MVSD-FMEA визначаються складові інтенсивностей безпечних і небезпечних відмов, після чого розраховуються DC, SFF, PFH та PFDavg і визначається досягнутий рівень SIL з урахуванням архітектурних обмежень.

9. Проаналізовано результати впровадження нових наукових положень досліджень.

ВИСНОВКИ

1. Проведено аналіз нормативної бази, методів і засобів оцінювання і забезпечення функціональної безпеки інформаційно-керуючих систем на різних етапах їх життєвого циклу. В дисертації **поставлене і вирішене актуальне наукове завдання** розроблення та удосконалення моделей, методів і засобів оцінювання функційної безпечності одно- і багатоверсійних інформаційно-керуючих систем на програмовних платформах з урахуванням розширеної номенклатури одиничних та множинних дефектів та їх комбінацій та зниження залежності помилок аналізу експертів.

2. Удосконалено моделі і показники для оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з використанням табличного методу аналізу видів і наслідків відмов (FMECA/FMEDA), шляхом визначення і зменшення кількості критичних припущень і обмежень при формуванні і заповненні таблиць, а також детермінованого представлення і перебору причин відмов і рівнів небезпеки внаслідок різних дефектів, що дозволяє збільшити повноту оцінки.

3. Удосконалено метод експертного оцінювання функційної безпечності інформаційно-керуючих систем на програмовній логіці при використанні процедур FMECA/FMEDA шляхом зменшення кількості операцій із залученням експертів та впровадження спеціальних сценаріїв узгодження експертних оцінок у вигляді вербальної, нечіткої і кількісної інформації, що дозволяє підвищити достовірність оцінки.

4. Вперше розроблено метод оцінювання функційної безпечності двохверсійних інформаційно-керуючих систем на програмовних платформах з використанням комбінованих процедур аналізу дефектів версій, який відрізняється від відомих тим, що при аналізі видів та наслідків відмов формуються профілі відносних і абсолютних дефектів, а також використовуються регресійні процедури ін’єктування множинних дефектів з урахуванням їхнього самомаскування і блокування системи, що дозволяє

зменшити час і підвищити достовірність оцінки ризиків відмов за загальною причиною.

5. Достовірність отриманих результатів підтверджується обґрунтованістю допущень, коректним обранням математичного апарату та результатами практичних впроваджень.

6. Практичне значення отриманих результатів полягає у доведенні теоретичних положень дисертації до алгоритмів, програмно-апаратних засобів, методичних рекомендацій та їх безпосередньому використанні на підприємствах при створенні ІКС АЕС. Зокрема розроблено алгоритми AMECA аналізу критичності припущень, експертного оцінювання результатів FMECA/FMEDA, формування узгоджених експертних оцінок, програмні засоби підтримки процедур оцінювання функційної безпечності та ін.

7. Отримані наукові й практичні результати використовувались при виконанні навчального процесу Національного аерокосмічного університету «ХАІ» та виконанні науково-дослідних проєктів і навчальному процесі, при розробленні інформаційно-керуючих систем АЕС на НВП «Радій»; при сертифікації програмовних платформ інформаційно-керуючих систем на відповідність вимогам стандартів та американського ядерного регулятора на НВП «Радікс», що підтверджується відповідними актами.

8. Подальші дослідження доцільно спрямувати на розроблення моделей готовності ІКС АЕС з врахуванням запропонованих методів аналіза функційної безпечності, можливих кібервтручань та різних стратегій відновлення, а також адаптацію цих методів для інших критичних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

оформлено відповідно до ДСТУ 8302:2015

1. Babeshko E., Kharchenko V., Kovalenko A., Leontiiev K. Cyber security assurance approaches for FPGA-based safety platform configuration tool // Proceedings of the International Conference on Information and Digital Technologies (IDT 2017). 2017. P. 160–163.

2. Kharchenko V., Brezhniev I., Kovalenko A., Leontiiev K. Secure Environment Establishment for FPGA-based Safety-Critical Systems: Quality Management System Context // Proceedings of the 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2017). San Francisco, California, USA, June 11–15, 2017. P. 434–441.

3. Andrashov A., Leontiiev K., Kovalenko A., Bakhmach I., Kharchenko V. NPP I&C Modernization Approaches Using FPGA-based RadICS Platform // Fourth International Conference on Nuclear Power Plant Life Management. Lyon, France, October 23–27, 2017. P. 14.

4. Kharchenko V., Babeshko E., Leontiiev K., Ruchkov E., Sklyar V. Reliability assessment of safety critical system considering different communication architectures // Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT 2018). 2018. P. 17–20.

5. Kharchenko V., Kovalenko A., Leontiiev K., Panarin A., Duzhy V. Multi-Diversity for FPGA Platform Based NPP I&C Systems: New Possibilities and Assessment Technique // Proceedings of the International Conference on Nuclear Engineering (ICONE 2018). 2018. Paper ID: ICONE26-82377.

6. Babeshko E., Kharchenko V., Leontiiev K., Odarushchenko O., Strjuk O. NPP I&C Safety Assessment by Aggregation of Formal Techniques // Proceedings of the International Conference on Nuclear Engineering (ICONE 2018). 2018. Paper ID: ICONE26-82270.

7. Gordieiev O., Kharchenko V., Leontiiev K. Usability, Security and Safety Interaction: Profile and Metrics Based Analysis // Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing. Vol. 761. Springer, 2018. P. 238–247.

8. Andrashov A., Bakhmach I., Leontiiev K., Kovalenko A., Kharchenko V., Babeshko E. Diversity in FPGA-Based Platform and Platform Based I&Cs Applications: Strategy and Implementation // Proceedings of the 11th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019). Orlando, Florida, USA, February 9–14, 2019. P. 174–182.

9. Babeshko I., Kovalenko A., Tokarev V., Leontiiev K. FPGA Technology and Platforms for NPP I&C Systems // Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems. Hershey, PA, USA : IGI Global, 2020. Chapter 16. P. 419–457. DOI: 10.4018/978-1-7998-3277-5.ch016.

10. Odarushchenko O., Striuk O., Leontiiev K., Odarushchenko E. Software Fault Insertion Testing for SIL Certification of Safety PLC-Based System // Proceedings of the 11th IEEE International Conference «DEpendable Systems, SERvices and Technologies» (DESSERT’2020). Kyiv, Ukraine, May 14–18, 2020. P. 80–84.

11. Leontiiev K., Babeshko I., Kharchenko V. Assumption Modes and Effect Analysis of XMECA: Expert Based Safety Assessment // Proceedings of the 11th IEEE International Conference «DEpendable Systems, SERvices and Technologies» (DESSERT’2020). Kyiv, Ukraine, May 14–18, 2020. P. 90–94.

12. Гордєєв О. О., Лєонтієв К. П. Модель сценарію оцінювання якості програмного забезпечення // Технічні науки та технології. 2020. № 3(21). С. 209–219. DOI: 10.25140/2411-5363-2020.

13. Гордєєв О. О., Лєонтієв К. П. Модель життєвого циклу дефекту програмного забезпечення // Математичне та комп’ютерне моделювання. Серія: Технічні науки. 2020. Вип. 21. С. 51–60.

14. Babeshko E., Kharchenko V., Leontiiev K., Ruchkov E. Practical Aspects of Operating and Analytical Reliability Assessment of FPGA-Based I&C Systems // Радіоелектронні і комп'ютерні системи. 2020. № 3(95). С. 75–83.

15. Babeshko I., Leontiiev K., Kharchenko V., Brezhniev E. Application of Assumption Modes and Effects Analysis to XMECA // Theory and Engineering of Dependable Computer Systems and Networks. Proceedings of the Sixteenth International Conference on Dependability of Computer Systems (DepCoS-RELCOMEX 2021). Advances in Intelligent Systems and Computing. Vol. 1389. Springer Nature Switzerland AG, 2021. P. 1–11. DOI: 10.1007/978-3-030-76773-0.

16. Kliushnikov I., Kharchenko V., Fesenko H., Leontiiev K., Illiashenko O. UAV Fleet with Battery Recharging for NPP Monitoring: Queuing System and Routing Based Reliability Models // New Advances in Dependability of Networks and Systems. DepCoS-RELCOMEX 2022. Lecture Notes in Networks and Systems. Vol. 484. Springer, Cham, 2022. P. 133–143. DOI: 10.1007/978-3-031-06746-4_11.

17. Babeshko I., Illiashenko O., Kharchenko V., Leontiiev K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques // Mathematics. 2022. Vol. 10, No. 13. Article 2297. 25 p. DOI: 10.3390/math10132297.

18. Babeshko I., Kharchenko V., Leontiiev K. Enhancing FMECA(XMECA)-based Safety Assessment Considering Criticality of Assumptions and Analysis Errors. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2024, pp. 1-5, doi: 10.1109/DESSERT65323.2024.11122229.

19. Babeshko I., Kharchenko V., Leontiiev K. Method for enhancing FMECA (XMECA) safety assessment procedures considering the criticality of assumptions and analysis errors. *Computer Systems and Information Technologies*, (4), 96–102. https://doi.org/10.31891/csit-2025-4-10.

20. ДСТУ EN 61508-1:2019. Функційна безпечність електричних, електронних, програмованих електронних систем, пов’язаних із безпекою. Частина 1. Загальні вимоги (EN 61508-1:2010, IDT; IEC 61508-1:2010, IDT).

21. ДСТУ EN 61513:2022. Атомні електростанції. Контрольно-вимірювальні прилади та системи управління, важливі для безпеки. Загальні вимоги до систем (EN 61513:2013, IDT; IEC 61513:2011, IDT).

22. IEC 61513:2026. Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. Geneva : International Electrotechnical Commission, 2026.

23. ДСТУ EN 60880:2022. Атомні електростанції. Контрольно-вимірювальні прилади та системи управління, важливі для безпеки. Аспекти програмного забезпечення для комп’ютерних систем, що виконують функції категорії A (EN 60880:2009, IDT; IEC 60880:2006, IDT).

24. ДСТУ EN IEC 62138:2022. Атомні електростанції. Контрольно-вимірювальні прилади та системи управління, важливі для безпеки. Аспекти програмного забезпечення для комп’ютерних систем, що виконують функції категорії B або C (EN IEC 62138:2019, IDT; IEC 62138:2018, IDT).

25. ДСТУ EN IEC 61226:2022. Атомні електростанції. Контрольно-вимірювальні прилади та системи управління, важливі для безпеки. Класифікація контрольно-вимірювальних та керівних функцій (EN IEC 61226:2020, IDT; IEC 61226:2020, IDT).

26. IEEE 7-4.3.2-2016 - IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations

27. IEC 60300-3-1:2003. Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology. Geneva : International Electrotechnical Commission, 2003.

28. IEC 61165:2006. Application of Markov techniques. Geneva : International Electrotechnical Commission, 2006

29. Kahneman. D., Slovic, P., Tversky, A. Judgement under Uncertainty, Heuristics and Biases // Science. 1974. – Vol. 185, Issue 4157. – P. 1124-1131. DOI: 10.1126/science.185.4157.1124

30. Morgan M.G., Henrion M. Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge University Press, 1992 – 346 p.

31. O'Hagan A., Buck C. E., Daneshkah A., Eiser J. R., Garthwaite P.H., Jenkinson D.J., Oakley J.E., Rakow T. Uncertain Judgments: Eliciting Experts' Probabilities. Wiley, 2006. – 338 p.

32. Cooke, R M. Experts In Uncertainty: Opinion and Subjective Probability in Science. Oxford University Press, 1991. – 336 p.

33. Goossens L.H.J., Harper F.T., Kraan B.C.P., Metivier H. Expert Judgement for a Probabilistic Accident Consequence Uncertainty Analysis // Radiation Protection Dosimetry. – Volume 90, Issue 3, 1 August 2000. – P. 295-301. DOI: 10.1093/oxfordjournals.rpd.a033151

34. Deng Y., Kang B.Y., Zhang Y.J., Deng X.Y., Zhang H.X. Aggregate experts' judgments in nuclear engineering management. *// Proceedings of Chinese Control and Decision Conference (CCDC)*. – Mianyang, China, 2011. P. 3236-3239. DOI: 10.1109/CCDC.2011.5968814.

35. Bouzaiene L., Billy F., Bocquet J-C., Haik P., Lannoy A., Peres F. Expert Judgement Methodology for Failure Anticipation in Nuclear Power Plants // Safety and Reliability: Proceedings of the ESREL 2003 Conference, Maastricht, the Netherlands. – 15-18 June 2003. – P. 195-200.

36. Kostogryzov A., Rybas A., Grigoriev L., Nistratov A., Nistratov G. Probabilistic Estimations of Increasing Expected Reliability and Safety for Intelligent Manufacturing // Proceedings of Global Smart Industry Conference (GloSIC), 2018. – P. 1-7. DOI: 10.1109/GloSIC.2018.8570124.

37. Jianxing Y., Haicheng C., Shibo W., Haizhao F. A Novel Risk Matrix Approach Based on Cloud Model for Risk Assessment Under Uncertainty. // *IEEE Access*, 2021. – Vol. 9. – P. 27884-27896. DOI: 10.1109/ACCESS.2021.3058392.

38. 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.

39. 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.

40. 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.

41. Multi-Version Systems and Technologies for Critical Applications / A. Volkovoj, I. Lysenko, V. Kharchenko, O. Shurygin ; ed. V. Kharchenko. Kharkiv : National Aerospace University «KhAI», 2009. 231 p.

42. 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.

43. Bluvband Z., Zilberberg E. Knowledgebase approach to integrated FMEA. Annual Quality Congress: proceedings of the 52nd Congress. Philadelphia, PA, USA, 1998. P.535–545.

44. 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. Žilina, 2015. P. 17–22.

45. 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. Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT’2018). Kyiv, 2018. P. 202–206.

46. Nolte B, Stein A, Vietor T. Designing a Method for Identifying Functional Safety and Cybersecurity Requirements Utilizing Model-Based Systems Engineering. *Applied System Innovation*. 2025; 8(2):45. https://doi.org/10.3390/asi8020045

47. Peserico G., Morato A., Tramarin F., Vitturi S. Functional Safety Networks and Protocols in the Industrial Internet of Things Era. Sensors. 2021. Vol. 21, No. 18. Art. 6073. DOI: https://doi.org/10.3390/s21186073.

48. Wu J., Ren J., Ravn O., Nalpantidis L. A Risk-Informed Design Framework for Functional Safety System Design of Human-Robot Collaboration Applications. Safety. 2025. Vol. 11, No. 1. Art. 24. DOI: https://doi.org/10.3390/safety11010024.

49. Sterniczuk D., Zaklika W., Kozłowski M. Identification Tests of Modern Vehicles' Electromagnetic Environment as Part of the Assessment of Their Functional Safety. Sensors. 2025. Vol. 25, No. 1. Art. 7. DOI: https://doi.org/10.3390/s25010007.

50. Barua N., Hitosugi M. A Multi-Modal AI System for Detecting Pedestrians Lying on the Road: Simulation-Based Safety and Injury Risk Analysis. Vehicles. 2026. Vol. 8, No. 6. Art. 136. DOI: https://doi.org/10.3390/vehicles8060136.

51. Kosmowski K. T., Piesik E., Piesik J., Śliwiński M. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. Energies. 2022. Vol. 15, No. 10. Art. 3610. DOI: https://doi.org/10.3390/en15103610.

52. Kizgin U. V., Stein A., Esapathi J., Vietor T. Systematic Method for Identifying Safety and Security Requirements in Autonomous Driving: Case Study of Autonomous Intersection System. Applied System Innovation. 2025. Vol. 8, No. 6. Art. 168. DOI: https://doi.org/10.3390/asi8060168.

53. Bondarenko I., Campisi T., Tesoriere G., Neduzha L. Using Detailing Concept to Assess Railway Functional Safety. Sustainability. 2023. Vol. 15, No. 1. Art. 18. DOI: https://doi.org/10.3390/su15010018.

54. Meng K., Zhou R., Li Z., Zhang K. A Quantitative Approach of Generating Challenging Testing Scenarios Based on Functional Safety Standard. Applied Sciences. 2023. Vol. 13, No. 6. Art. 3494. DOI: https://doi.org/10.3390/app13063494.

55. Chen L., Fan D., Zheng J., Xie X. Functional Safety Analysis and Design of Sensors in Robot Joint Drive System. Machines. 2022. Vol. 10, No. 5. Art. 360. DOI: https://doi.org/10.3390/machines10050360.

56. Nioata A., Țăpirdea A., Chivu O. R., Feier A., Enache I. C., Gheorghe M., Borda C. Workplace Safety in Industry 4.0 and Beyond: A Case Study on Risk Reduction Through Smart Manufacturing Systems in the Automotive Sector. Safety. 2025. Vol. 11, No. 2. Art. 50. DOI: https://doi.org/10.3390/safety11020050.

57. Kharchenko V., Shchehlov V., Ivasiuk O., Morozova O. Digital Twin-Based Lifecycle Methodology for Ensuring Safety of NPP/SMR I&C Systems. Technologies. 2026. Vol. 14, No. 1. Art. 46. DOI: https://doi.org/10.3390/technologies14010046.

58. Khalaquzzaman M., Lee S. J., Hossen M. M. Reliability Assessment of NPP Safety Class Equipment Considering the Manufacturing Quality Assurance Process. Journal of Nuclear Engineering. 2023. Vol. 4, No. 2. P. 421-435. DOI: https://doi.org/10.3390/jne4020030.

59. Sun Q., Han Y., Mao J., Shen H., Liu J. Mechanism-Aligned Nuclear Power Plant Accident Diagnosis via Physically Guided Concepts and Evidence Paths. Applied Sciences. 2026. Vol. 16, No. 12. Art. 5930. DOI: https://doi.org/10.3390/app16125930.

60. Yin X., Zhao M., Yang W., Zhang J., Li J. Seismic Safety Analysis of Nuclear Power Plant Pumping Stations Using the Compact Viscous-Spring Boundary via Maximum Initial Time-Step Method. Buildings. 2025. Vol. 15, No. 16. Art. 2951. DOI: https://doi.org/10.3390/buildings15162951.

61. Zhang J., Xia Y., Zhong H., Lu W., Deng Q., Wan C. A Safety and Security-Centered Evaluation Framework for Large Language Models via Multi-

Model Judgment. Mathematics. 2026. Vol. 14, No. 1. Art. 90. DOI: https://doi.org/10.3390/math14010090.

62. Pena-Molina A. E., Larrondo-Petrie M. M. Safety and Security Considerations for Online Laboratory Management Systems. Journal of Cybersecurity and Privacy. 2025. Vol. 5, No. 2. Art. 24. DOI: https://doi.org/10.3390/jcp5020024.

63. Kharchenko V., Illiashenko O., Sklyar V. Invariant-Based Safety Assessment of FPGA Projects: Conception and Technique. Computers. 2021. Vol. 10, No. 10. Art. 125. DOI: https://doi.org/10.3390/computers10100125.

64. El-Hajj M., Mirza Z. A. Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool. Electronics. 2024. Vol. 13, No. 19. Art. 3910. DOI: https://doi.org/10.3390/electronics13193910.

65. Luo M., Tao C., Liu Y., Chen S., Chen P. An Endogenous Security-Oriented Framework for Cyber Resilience Assessment in Critical Infrastructures. Applied Sciences. 2025. Vol. 15, No. 15. Art. 8342. DOI: https://doi.org/10.3390/app15158342.

66. Liu C., He X., Zhou D., Huang B. Safety Assessment for Dynamic Systems: A Survey. Cybernetics and Intelligence. 2026. Vol. 1, No. 1. Art. 9390001. DOI: 10.26599/CAI.2024.9390001.

67. Wang K., Zhang Q., Li H. Software Safety Level Comprehensive Assessment Approach Based on the Multidimensional System Risk Index // 2022 14th International Conference on Signal Processing Systems (ICSPS). Jiangsu, China, 2022. P. 556-561. DOI: 10.1109/ICSPS58776.2022.00103.

68. Nyakundi N. B. N., Reza H. Development of an Effective Safety Assessment Capable of Measuring the Safety of AI-Based Systems // 2024 IEEE International Conference on Electro Information Technology (eIT). Eau Claire, WI, USA, 2024. P. 1-8. DOI: 10.1109/eIT60633.2024.1060983.

69. Bhosale P., Kastner W., Sauter T. AutomationML Meets Bayesian Networks: A Comprehensive Safety-Security Risk Assessment in Industrial

Control Systems. IEEE Open Journal of the Industrial Electronics Society. 2024. Vol. 5. P. 823-835. DOI: 10.1109/OJIES.2024.3439388.

70. Wang H., Margellos K., Papachristodoulou A. Assessing Safety for Control Systems Using Sum-of-Squares Programming // Polynomial Optimization, Moments, and Applications / eds. M. Kočvara, B. Mourrain, C. Riener. Cham : Springer, 2023. DOI: https://doi.org/10.1007/978-3-031-38659-6_7.

71. Poorhadi E., Troubitsyna E. Integrating Graphical and Formal Modelling to Analyse the Impact of Cyberattacks on Safety of Networked Control Systems. Systems. 2026. Vol. 14, No. 8. Art. 936. DOI: https://doi.org/10.3390/systems14080936.

72. Krichen M. Formal Methods and Validation Techniques for Ensuring Automotive Systems Security. Information. 2023. Vol. 14, No. 12. Art. 666. DOI: https://doi.org/10.3390/info14120666.

73. Hosseini A. M., Sauter T., Kastner W. Formal Verification of Safety and Security Properties in Industry 4.0 Applications // 2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA). Sinaia, Romania, 2023. P. 1-8. DOI: 10.1109/ETFA54631.2023.10275690.

74. Mishra A. D., Mustafa K. A Survey on Formal Specification of Security Requirements // 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). Greater Noida, India, 2021. P. 1453-1456. DOI: 10.1109/ICAC3N53548.2021.9725779.

75. Kang E.-Y., Hacks S. Safety & Security Analysis of a Manufacturing System using Formal Verification and Attack-Simulation // 2023 12th Mediterranean Conference on Embedded Computing (MECO). Budva, Montenegro, 2023. P. 1-8. DOI: 10.1109/MECO58584.2023.10154960.

76. Abdulsamad A. A., Répás S. R. Application of FPGA Devices in Network Security: A Survey. Electronics. 2025. Vol. 14, No. 19. Art. 3894. DOI: https://doi.org/10.3390/electronics14193894.

77. Sledevič T., Andriukaitis D. Hardware-Assisted Security Enhancements for an FPGA-ARM Embedded Vision System in IoT Applications. Electronics. 2026. Vol. 15, No. 9. Art. 1887. DOI: https://doi.org/10.3390/electronics15091887.

78. Yavuz S., Naroska E., Daniel K. Comprehensive Investigation of Security and Quality Metrics for Lightweight Double Arbiter PUF on FPGAs: Design and Analysis. Electronics. 2025. Vol. 14, No. 8. Art. 1510. DOI: https://doi.org/10.3390/electronics14081510.

79. Hussein Y. M., Hassan R. F., Chisab R. F. FPGA-Based Reconfigurable SoCs for Safety-Critical AI Inference: A Systematic Literature Review. Electronics. 2026. Vol. 15, No. 12. Art. 2695. DOI: https://doi.org/10.3390/electronics15122695.

80. Silva Neto A. V., Silva H. L., Camargo J. B. Jr., Almeida J. R. Jr., Cugnasca P. S. Design and Assurance of Safety-Critical Systems with Artificial Intelligence in FPGAs: The Safety ArtISt Method and a Case Study of an FPGA-Based Autonomous Vehicle Braking Control System. Electronics. 2023. Vol. 12, No. 24. Art. 4903. DOI: https://doi.org/10.3390/electronics12244903.

81. Mani P., Komarasamy P. R. G., Rajamanickam N., Shorfuzzaman M., Abdelfattah W. M. Enhancing Sustainable Transportation Infrastructure Management: A High-Accuracy, FPGA-Based System for Emergency Vehicle Classification. Sustainability. 2024. Vol. 16, No. 16. Art. 6917. DOI: https://doi.org/10.3390/su16166917.

82. He J., Zhang Y., Lu W., Liu Y., Xu C., Liao X., Yang Y. HCCA-SAFE: A Hybrid Cascaded Control Architecture for FPGA-Based Fault Injection in Safety-Critical Automotive SoCs. Micromachines. 2026. Vol. 17, No. 2. Art. 185. DOI: https://doi.org/10.3390/mi17020185.

83. Węgrzyn M., Kochan O., Maikiv I. Fault Injection Tool for FPGA Reliability Testing: A Novel Method and Discovery of LUT-Specific Logical Redundancies. Electronics. 2025. Vol. 14, No. 23. Art. 4600. DOI: https://doi.org/10.3390/electronics14234600.

84. Zhu H., Lai Q. Research on FPGA-Based Functional Safety Diagnosis System // 2025 9th International Conference on Robotics, Control and Automation (ICRCA). Shanghai, China, 2025. P. 88-92. DOI: 10.1109/ICRCA64997.2025.11011193.

85. Uğuz O., Çiçek İ. Design of an FPGA-Based System-on-Module for Safety-Critical Applications // 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES). Veliko Tarnovo, Bulgaria, 2024. P. 1-6. DOI: 10.1109/CIEES62939.2024.10811198.

86. Sun Y., Wang Z., Huang Z., Liang L. An FPGA-Based Emulation Platform for Functional Safety Verification in Automotive SoC Systems // 2024 IEEE 33rd Asian Test Symposium (ATS). Ahmedabad, India, 2024. P. 1-6. DOI: 10.1109/ATS64447.2024.10915395.

87. Wang Y., Hu Y., Li Y., Ge H. Analysis and Software Development of System Failure Probability Correction Considering Common Cause Failure. Modelling. 2025. Vol. 6, No. 4. Art. 162. DOI: https://doi.org/10.3390/modelling6040162.

88. Li B., Li J., Huang X. Improving Software Reliability in Nuclear Power Plants via Diversity in the Requirements Phase: An Experimental Study. Energies. 2025. Vol. 18, No. 18. Art. 4794. DOI: https://doi.org/10.3390/en18184794.

89. Zhao Q. Q., Kim J. W., Chung I. H., Yun W. Y. Optimal Redundancy Allocation in Multi-Indenture Systems Considering Human Error-Induced Common Cause Failures. Machines. 2026. Vol. 14, No. 6. Art. 627. DOI: https://doi.org/10.3390/machines14060627.

90. Jesus T. C., Portugal P., Costa D. G., Vasques F. Reliability and Detectability of Emergency Management Systems in Smart Cities under Common Cause Failures. Sensors. 2024. Vol. 24, No. 9. Art. 2955. DOI: https://doi.org/10.3390/s24092955.

ДОДАТОК А.
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

1. Babeshko E., Kharchenko V., Kovalenko A., Leontiiev K. Cyber security assurance approaches for FPGA-based safety platform configuration tool // Proceedings of the International Conference on Information and Digital Technologies (IDT 2017). 2017. P. 160–163.

2. Kharchenko V., Brezhniev I., Kovalenko A., Leontiiev K. Secure Environment Establishment for FPGA-based Safety-Critical Systems: Quality Management System Context // Proceedings of the 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies (NPIC & HMIT 2017). San Francisco, California, USA, June 11–15, 2017. P. 434–441.

3. Andrashov A., Leontiiev K., Kovalenko A., Bakhmach I., Kharchenko V. NPP I&C Modernization Approaches Using FPGA-based RadICS Platform // Fourth International Conference on Nuclear Power Plant Life Management. Lyon, France, October 23–27, 2017. P. 14.

4. Kharchenko V., Babeshko E., Leontiiev K., Ruchkov E., Sklyar V. Reliability assessment of safety critical system considering different communication architectures // Proceedings of the 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT 2018). 2018. P. 17–20.

5. Kharchenko V., Kovalenko A., Leontiiev K., Panarin A., Duzhy V. Multi-Diversity for FPGA Platform Based NPP I&C Systems: New Possibilities and Assessment Technique // Proceedings of the International Conference on Nuclear Engineering (ICONE 2018). 2018. Paper ID: ICONE26-82377.

6. Babeshko E., Kharchenko V., Leontiiev K., Odarushchenko O., Strjuk O. NPP I&C Safety Assessment by Aggregation of Formal Techniques // Proceedings of the International Conference on Nuclear Engineering (ICONE 2018). 2018. Paper ID: ICONE26-82270.

7. Gordieiev O., Kharchenko V., Leontiiev K. Usability, Security and Safety Interaction: Profile and Metrics Based Analysis // Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018. Advances in Intelligent Systems and Computing. Vol. 761. Springer, 2018. P. 238–247.

8. Andrashov A., Bakhmach I., Leontiiev K., Kovalenko A., Kharchenko V., Babeshko E. Diversity in FPGA-Based Platform and Platform Based I&Cs Applications: Strategy and Implementation // Proceedings of the 11th International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2019). Orlando, Florida, USA, February 9–14, 2019. P. 174–182.

9. Babeshko I., Kovalenko A., Tokarev V., Leontiiev K. FPGA Technology and Platforms for NPP I&C Systems // Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems. Hershey, PA, USA : IGI Global, 2020. Chapter 16. P. 419–457. DOI: 10.4018/978-1-7998-3277-5.ch016.

10. Odarushchenko O., Striuk O., Leontiiev K., Odarushchenko E. Software Fault Insertion Testing for SIL Certification of Safety PLC-Based System // Proceedings of the 11th IEEE International Conference «DEpendable Systems, SERvices and Technologies» (DESSERT’2020). Kyiv, Ukraine, May 14–18, 2020. P. 80–84.

11. Leontiiev K., Babeshko I., Kharchenko V. Assumption Modes and Effect Analysis of XMECA: Expert Based Safety Assessment // Proceedings of the 11th IEEE International Conference «DEpendable Systems, SERvices and Technologies» (DESSERT’2020). Kyiv, Ukraine, May 14–18, 2020. P. 90–94.

12. Гордєєв О. О., Лєонтієв К. П. Модель сценарію оцінювання якості програмного забезпечення // Технічні науки та технології. 2020. № 3(21). С. 209–219. DOI: 10.25140/2411-5363-2020.

13. Гордєєв О. О., Лєонтієв К. П. Модель життєвого циклу дефекту програмного забезпечення // Математичне та комп’ютерне моделювання. Серія: Технічні науки. 2020. Вип. 21. С. 51–60.

14. Babeshko E., Kharchenko V., Leontiiev K., Ruchkov E. Practical Aspects of Operating and Analytical Reliability Assessment of FPGA-Based I&C Systems // Радіоелектронні і комп'ютерні системи. 2020. № 3(95). С. 75–83.

15. Babeshko I., Leontiiev K., Kharchenko V., Brezhniev E. Application of Assumption Modes and Effects Analysis to XMECA // Theory and Engineering of Dependable Computer Systems and Networks. Proceedings of the Sixteenth International Conference on Dependability of Computer Systems (DepCoS-RELCOMEX 2021). Advances in Intelligent Systems and Computing. Vol. 1389. Springer Nature Switzerland AG, 2021. P. 1–11. DOI: 10.1007/978-3-030-76773-0.

16. Kliushnikov I., Kharchenko V., Fesenko H., Leontiiev K., Illiashenko O. UAV Fleet with Battery Recharging for NPP Monitoring: Queuing System and Routing Based Reliability Models // New Advances in Dependability of Networks and Systems. DepCoS-RELCOMEX 2022. Lecture Notes in Networks and Systems. Vol. 484. Springer, Cham, 2022. P. 133–143. DOI: 10.1007/978-3-031-06746-4_11.

17. Babeshko I., Illiashenko O., Kharchenko V., Leontiiev K. Towards Trustworthy Safety Assessment by Providing Expert and Tool-Based XMECA Techniques // Mathematics. 2022. Vol. 10, No. 13. Article 2297. 25 p. DOI: 10.3390/math10132297.

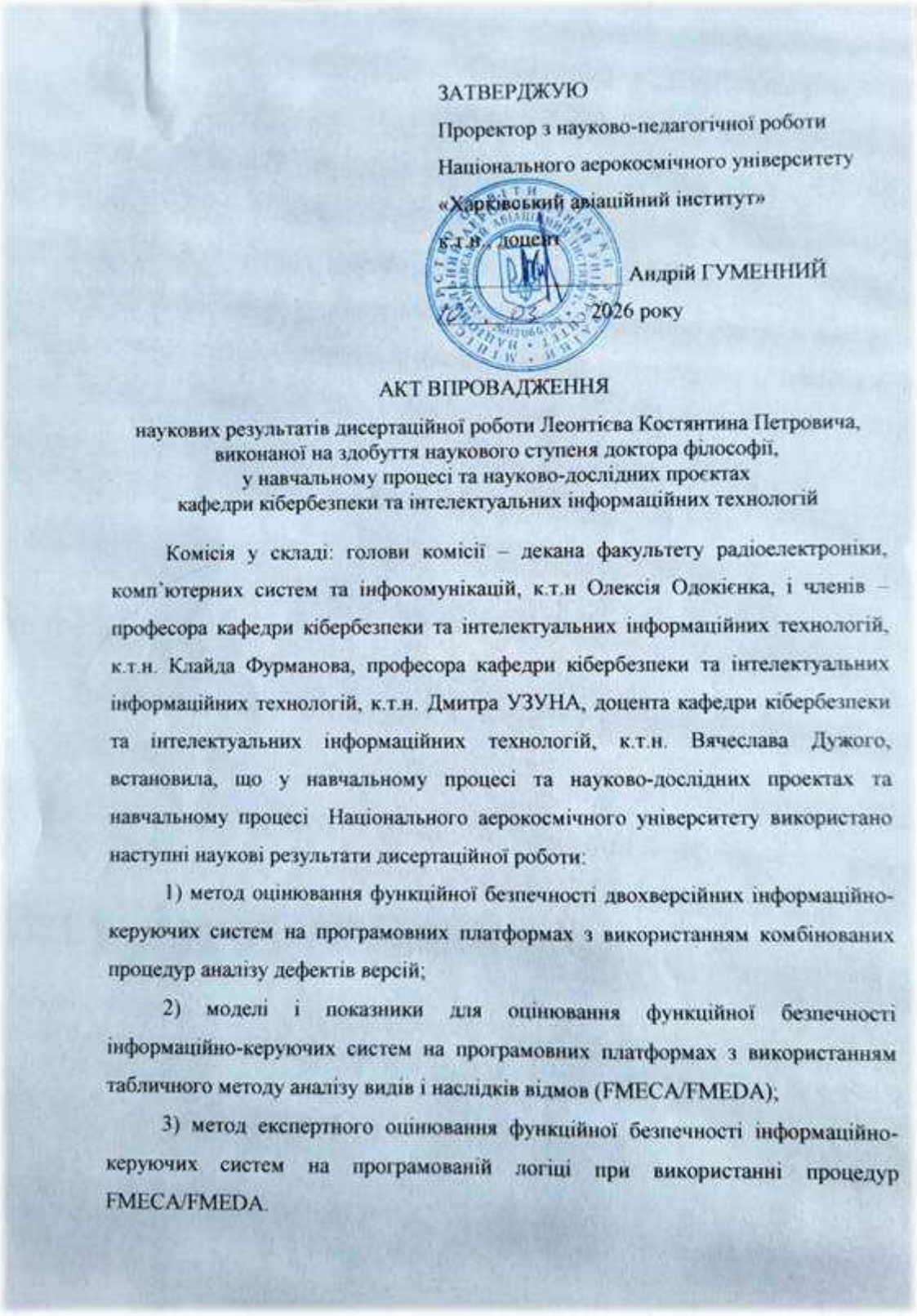
18. Babeshko I., Kharchenko V., Leontiiev K. Enhancing FMECA(XMECA)-based Safety Assessment Considering Criticality of Assumptions and Analysis Errors. *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2024, pp. 1-5, doi: 10.1109/DESSERT65323.2024.11122229.

19. Babeshko I., Kharchenko V., Leontiiev K. Method for enhancing FMECA (XMECA) safety assessment procedures considering the criticality of assumptions and analysis errors. *Computer Systems and Information Technologies*, (4), 96–102. https://doi.org/10.31891/csit-2025-4-10.

ДОДАТОК Б.

АКТИ ВПРОВАДЖЕННЯ

Акт впровадження наукових результатів у навчальному процесі та науково-дослідних проєктах Національного аерокосмічного університету від 10.03.2026



ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
Національного аерокосмічного університету
«Харківський авіаційний інститут»
к.т.н., доцент
Андрій ГУМЕННИЙ
10.03 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Леонтієва Костянтина Петровича,
виконаної на здобуття наукового ступеня доктора філософії,
у навчальному процесі та науково-дослідних проєктах
кафедри кібербезпеки та інтелектуальних інформаційних технологій

Комісія у складі: голови комісії – декана факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій, к.т.н Олексія Одокієнка, і членів – професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Клайда Фурманова, професора кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Дмитра УЗУНА, доцента кафедри кібербезпеки та інтелектуальних інформаційних технологій, к.т.н. Вячеслава Дужого, встановила, що у навчальному процесі та науково-дослідних проектах та навчальному процесі Національного аерокосмічного університету використано наступні наукові результати дисертаційної роботи:

1) метод оцінювання функційної безпечності двохверсійних інформаційно-керуючих систем на програмовних платформах з використанням комбінованих процедур аналізу дефектів версій;

2) моделі і показники для оцінювання функційної безпечності інформаційно-керуючих систем на програмовних платформах з використанням табличного методу аналізу видів і наслідків відмов (FMECA/FMEDA);

3) метод експертного оцінювання функційної безпечності інформаційно-керуючих систем на програмованій логіці при використанні процедур FMECA/FMEDA.

Використання зазначених наукових результатів в курсах «Надійність та відмовостійкість комп'ютерних систем», «Надійність та функційна безпечність інформаційно-керуючих систем», «Сучасні технології комп'ютерної інженерії», при виконанні кваліфікаційних робіт бакалаврів і магістрів сприяло покращенню фундаментальності та практичної спрямованості навчання, а також забезпечило підвищення точності та достовірності оцінювання функційної безпечності інформаційно-керуючих систем при виконанні науково-дослідних проєктів.

Голова комісії — Олексій ОДОКІЄНКО

Члени комісії — Клайд ФУРМАНОВ

Дмитро УЗУН

Вячеслав ДУЖИЙ

Акт впровадження наукових результатів у ТОВ «НВП «Радікс» від 12.05.2026

ЗАТВЕРДЖУЮ

Генеральний директор
ТОВ "НВП "РАДІКС"

Катерина БАХМАЧ

12.05 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи

Леонтієва Костянтина Петровича,

виконаної на здобуття наукового ступеня доктора філософії, у науково-дослідних проєктах та розробках ТОВ "НВП "РАДІКС"

Комісія у складі: голови комісії – операційного директора ТОВ "НВП "РАДІКС", к.т.н. Олександра ІВАСЮКА, і членів - заступника операційного директора ТОВ "НВП "РАДІКС", к.т.н. Наталії РВАЧОВОЇ, провідного наукового співробітника ТОВ "НВП "РАДІКС", к.т.н Вікторії КУЛІНІЧ встановила, що у ТОВ "НВП "РАДІКС" під час проведення оцінювання функційної безпечності платформи RadICS для інформаційно-керуючих систем на програмовній логіці використано нові наукові результати дисертаційної роботи, а саме метод аналізу видів і наслідків відмов шляхом скорочення кількості операцій із залученням експертів та впровадження спеціальних сценаріїв узгодження експертних оцінок.

При цьому застосовано запропрновані автором процедури до оброблення та узгодження експертної інформації у вербальній, нечіткій і кількісній формах, а також методики регресійного ін'єктування множинних дефектів для аналізу відмов багатоверсійних систем.

Застосування зазначених результатів забезпечує:

- зменшення трудомісткості та суб'єктивності експертних процедур, підвищення відтворюваності та достовірності результатів оцінювання функційної безпечності;
- можливість автоматизації процесів аналізу відмов і підвищення ефективності контролю безпечності інформаційно-керуючих систем на програмованій логіці.

Результати досліджень були використані в процесах сертифікації платформи RadICS на відповідність вимогам IEC 61508 за рівнем SIL-3 в одному каналі та вимогам US NRC для перевірки експертного висновку FMEDA та вдосконалення процесу FMEA.

Голова комісії Олександр ІВАСЮК

Члени комісії Наталія РВАЧОВА

Вікторія КУЛІНІЧ

Акт впровадження наукових результатів у ТОВ «НВП «Радій» від 12.05.2026

ЗАТВЕРДЖУЮ

Генеральний конструктор
конструкторського бюро
автоматизованих систем
управління технологічними
процесами ПАТ "НВП "Радій"
канд.техн.наук

_____ Віктор ТОКАРЄВ

12 05 2026 року

АКТ ВПРОВАДЖЕННЯ

наукових результатів дисертаційної роботи Леонтієва Костянтина Петровича, виконаної на здобуття наукового ступеня доктора філософії, у проєктах ПАТ "НВП "Радій"

Комісія у складі: голови комісії – директора виконавчого ПАТ "НВП "Радій" к.т.н. Олександра СІОРИ, і членів – начальника конструкторського відділу КБ АСУ ТП ПАТ "НВП "Радій", к.т.н. Віктора ГОЛОВІРА, начальника відділу програмування КБ АСУ ТП ПАТ НВП "Радій", к.т.н. Олександра БЄЛОГО, встановила, що у ПАТ "НВП "Радій" використано наукові результати дисертаційної роботи, а саме:

- моделі та методи оцінки функційної безпечності інформаційно-керуючих систем з використанням аналізу видів і наслідків відмов, що базуються на детермінованому представленні та переборі причин відмов, визначенні критичних припущень і обмежень моделей, а також урахуванні дефектів і вразливостей апаратно-програмної реалізації;
- метод оцінювання функційної безпечності багатоверсійних інформаційно-керуючих систем із використанням ін'єктування дефектів та формування профілів відносних і абсолютних дефектів з урахуванням ефектів самомаскування і блокування системи.

Застосування зазначених результатів забезпечує:

- підвищення повноти та обґрунтованості оцінювання функційної безпечності інформаційно-керуючих систем на програмованій логіці;

- зменшення ризику неповного врахування критичних відмов і небезпечних станів;
- підвищення достовірності прийняття інженерних рішень при проєктуванні, верифікації та супроводі систем, що експлуатуються у відповідальних та потенційно небезпечних умовах.

Результати досліджень були впроваджені при розробленні та постачанні платформних рішень для інформаційно-керуючих систем енергоблоків Рівненської, Хмельницької та Південноукраїнської атомних електростанцій України, зокрема, в системах аварійного захисту та суміжних системах, реалізованих на програмовних платформах ПАТ "НВП "Радій".

Голова комісії Олександр СІОРА

Члени комісії Віктор ГОЛОВІР

Юрій БЄЛИЙ

ДОДАТОК В.
ТАБЛИЦІ ОПИТУВАННЯ ЕКСПЕРТІВ

Assumptions, limitations	**Modes**	**Effects**	**Probability**	**Severity**
Expert assessment	Not all components are defined for safety assessment	Safety overestimation		
	The number of components used for safety assessment is given too high	Safety underestimation		
	Not all failure modes are considered	Safety overestimation		
	Excess failure modes are considered	Safety underestimation		
	Failure criticality (probability, severity) is underestimated	Safety overestimation		
	Failure criticality (probability, severity) is overestimated	Safety underestimation		
	Failure mistakenly treated as detected	Safety overestimation		
	Failure mistakenly treated as undetected	Safety underestimation		
Single / multiple faults	Failure multiplicity is underestimated	Safety overestimation		
	Failure multiplicity is overestimated	Safety underestimation		
	Multiple faults of different components at one level are not considered	Safety overestimation		
	Multiple faults of different components at different levels are not considered	Safety overestimation		
	Multiple faults of different versions are not considered	Safety overestimation		
System levels	Not all levels are considered	Safety overestimation		
	Excess levels are considered	Safety underestimation		
	Interaction between levels is not considered	Safety overestimation		
	Excess interaction between levels is considered	Safety underestimation		
Types of faults	Not all software faults are considered	Safety overestimation		
	More than required software	Safety underestimation		

	faults are considered	
	Not all hardware faults (physical and project) are considered	Safety overestimation
	More than required hardware faults (physical and project) are considered	Safety underestimation
	Hardware and software faults are not considered with respect to possible attacks	Safety overestimation