Артем ПАНАРІН,
аспірант кафедри кібербезпеки та інтелектуальних інформаційних технологій Національного аерокосмічного університету «Харківський авіаційний інститут»,
ORCID: https://orcid.org/0000-0003-1376-8425,
e-mail: a.panarin@csn.khai.edu

DOI: https://doi.org/10.32620/pls.2025.8.67

ПРИНЦИП ДИВЕРСНОСТІ ТА БАГАТОВЕРСІЙНІ ТЕХНОЛОГІЇ ДЛЯ СИСТЕМ ЗАХИСТУ РЕАКТОРІВ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ

Анотація. *У роботі розглянуто застосування принципу диверсності та багатоверсійних технологій для підвищення функційної безпечності систем захисту реакторів атомних електростанцій (АЕС), реалізованих на програмовних платформах з використанням технологій FPGA та SoC. Актуальність дослідження зумовлена необхідністю зменшення ризиків відмов за загальною причиною (Common Cause Failure, CCF) у сучасних інформаційно-керуючих системах (ІКС) АЕС та впровадженням програмно-апаратних рішень з високим ступенем інтеграції, які можуть впливати на такі ризики. Проаналізовано вимоги міжнародних стандартів та рекомендацій МАГАТЕ щодо диверсності та багатоверсійних архітектур, а також особливості їх імплементації в українській і світовій практиці. Запропоновано розширену класифікацію видів диверсності для програмних платформ, графові та матричні моделі її представлення, метод вибору диверсних конфігурацій з урахуванням метрик диверсності та відносної вартості, а також методи програмно-апаратної диверсифікації (диверсна синхронізація, структурно-просторова диверсність, диверсифікація контролю цілісності даних). Окрему увагу приділено інтеграції модельно-базованої верифікації (Model-Based Testing, MBT) у життєвий цикл систем захисту реакторів та впровадженню отриманих результатів у платформні рішення Radiy та RadICS.*

Ключові слова: *інформаційно-керуючі системи АЕС, системи захисту реактора, функційна безпечність, диверсність, багатоверсійні технології, диверсна синхронізація, просторова диверсність, диверсність підрахунку контрольної суми, FPGA, Model-Based Testing.*

Безпека критичної енергоінфраструктури і ризики відмов за загальною причиною. Збройна агресія Російської Федерації проти України, що триває з 24 лютого 2022 року, продемонструвала критичну вразливість енергетичної інфраструктури, включно з атомними електростанціями, до комплексних загроз – від фізичних атак до кібернетичних впливів і радіаційних ризиків [1; 2]. Атаки на Запорізьку АЕС, пошкодження систем живлення та спроби дистанційного втручання в ІКС підкреслили необхідність підвищення стійкості систем захисту реакторів до одночасних відмов, викликаних як зовнішніми впливами, так і внутрішніми системними дефектами. За даними МАГАТЕ, у 2022–2025 рр. зафіксовано безліч інцидентів на українській енергетичній інфраструктурі, що призвело до тимчасової втрати керування критичними функціями безпеки і підтвердило актуальність розробки технологій, стійких до CCF (Common Cause Failure) у воєнних умовах.

Ця мотивація актуалізує перехід до проєктивних підходів, орієнтованих на превентивне забезпечення функційної безпечності через багатоверсійні технології з комбінованою диверсністю. Розробка таких рішень дозволяє не лише відповідати вимогам міжнародних стандартів, але й створювати системи, здатні зберігати працездатність у умовах множинних одночасних загроз, що є критично важливим для національної безпеки України в умовах гібридної війни. Саме тому дослідження принципів диверсності для ІКС АЕС набуло стратегічного значення як складової захисту критичної інфраструктури від комплексних викликів.

Проблема забезпечення функційної безпечності систем захисту реакторів атомних електростанцій загострюється в умовах одночасної модернізації діючих енергоблоків і переходу до цифрових інформаційно-керуючих систем на базі програмовних платформ типу FPGA та SoC. У таких системах зростає частка програмно-апаратних компонентів, для яких характерні складні, часто непрозорі ланцюжки розробки (мови опису

апаратури, інструментальні засоби синтезу, IP-ядра, бібліотеки), що створює нові джерела відмов, у тому числі за загальною причиною.

Відмови за загальною причиною CCF можуть бути зумовлені спільними помилками вимог і проєктування, дефектами засобів розробки, систематичними похибками конфігурації ПЛІС або апаратно-залежними вразливостями, і здатні призвести до одночасної втрати працездатності кількох незалежних на перший погляд каналів захисту. Такі відмови дещо обмежують ефективність традиційного мажоритарного резервування «k з n», на якому історично базувалися системи захисту реактора, і прямо відзначаються у рекомендаціях NUREG/CR 7007 та стандартах IEC 61513, IEC 61508 як особливий клас ризиків, що потребує спеціальних заходів.

Принцип диверсності для зменшення ризиків CCF. У цих умовах принцип диверсності розглядається міжнародними та національними регуляторами як один з базових підходів до побудови багатоверсійних систем, стійких до CCF, за рахунок свідомого використання версійної надмірності на рівні архітектури, апаратури, програмно-алгоритмічних рішень і експлуатаційних процедур. Для систем захисту реакторів це обумовило перехід від простого дублювання і трьохкратного резервування до структур, у яких канали відрізняються за реалізацією функцій, застосованими технологіями та життєвими циклами розробки, що відповідає вимогам IEC 60880, IEC 62138 та рекомендаціям МАГАТЕ SSG 39 щодо диверсності систем безпеки АЕС.

Рекомендації NUREG/CR-7007 «Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems», розроблені Комісією з ядерного регулювання США (NRC), стали ключовим орієнтиром для систематизації видів диверсності у критичних системах безпеки АЕС [3; 4; 5]. Вона класифікується за шістьма основними категоріями: Design (архітектурна), Equipment (апаратна), Function (функціональна), Human (людський фактор), Signal (сигнальна), Software (програмна), пропонуючи модель взаємозв’язків цих типів диверсності з критичними галузями застосування (космос, авіація, залізниця, автомобільна промисловість, енергетика та АЕС).

Розширений класифікатор диверсності. та інші класифікації стали основою для розробки розширеної чотирьохрівневої моделі диверсності, адаптованої для програмних платформ ІКС АЕС, яка включає понад 60 підвидів: архітектурний рівень (різні топології каналів захисту, гібридні архітектури FPGA/SoC), апаратний (гетерогенні ПЛІС, різні тактові домени, структурно-просторова диверсність LUT/DSP-блоків), програмно-алгоритмічний (диверсифікація HDL-коду VHDL/Verilog, алгоритмів CRC, протоколів передачі), експлуатаційний (різні життєві цикли розробки, процедури верифікації).

На базі розширеного класифікатора побудовано матричну модель диверсності, де рядки відповідають рівням класифікації, а стовпці – конкретним підвидам диверсності з числовими метриками ефективності диверсності та відносної вартості, отриманими шляхом експертного оцінювання. Матриця дозволяє формалізовано оцінювати комбінації диверсності для систем захисту реактора, обчислюючи інтегральні показники, що забезпечує обґрунтований вибір стратегій «максимальна диверсність», «мінімальні витрати» або компромісні конфігурації.

Такий підхід до класифікації та моделювання диверсності дозволяє систематично аналізувати можливі шляхи усунення спільних вразливостей на етапі проєктування, що є особливо актуальним для ІКС АЕС в умовах підвищених воєнних ризиків.

Диверсна синхронізація є окремим і важливим методом реалізації програмної диверсності, який направлений на уникнення одночасних помилок через часові зсуви таймінгів у багатоверсійних інформаційно-керуючих системах [6]. Ідея методу полягає у застосуванні різних часових зсувів у тактових сигналах окремих каналів системи, що запобігає одночасному спрацьовуванню помилкових сигналів у всіх каналах. Такий підхід усуває небезпеку одночасної втрати працездатності через синхронні таймінгові відмови, які можуть виникати при одночасному спрацюванні логічних елементів в різних каналах, що в свою чергу призводить до пікових навантажень енергоспоживання, рознесення та пом'якшення яких суттєво підвищує стабільність і живучість систем захисту шляхом зниження одночасного стресу на апаратні компоненти та запобігання каскадним відмовам, що є важливою умовою забезпечення безпеки ядерних реакторів у складних експлуатаційних та воєнних умовах.

Метод диверсної синхронізації полягає у використанні незалежних часових кортежів для кожного каналу, де тактові сигнали різняться за фазою та іноді за тривалістю імпульсів, що забезпечує часову роздільність обробки інформації. Зсуви таймінгів формують асинхронне рознесення такту, яке мінімізує перетин критичних операцій і збільшує відмовостійкість системи у цілому.

Метрики ефективності диверсної синхронізації враховують час розділення тактових імпульсів та потенційну частоту спільних порушень, дозволяючи кількісно оцінювати внесок методу у загальну стійкість системи. Результати експериментального моделювання на FPGA-платформах показали зниження ймовірності одночасних таймінгових помилок на 20-35% порівняно зі стандартною синхронізацією без зсувів при варіації фазових зсувів.

Структурно просторова диверсність апаратної реалізації багатоверсійних систем захисту реакторів передбачає цілеспрямоване рознесення логіки каналів у просторі FPGA матриці та

використання альтернативних варіантів розміщення і трасування сигналів. Для кожного каналу формуються окремі конфігурації, у яких критичні вузли розташовуються в різних ділянках кристалу, з відмінною топологією з'єднань і різними наборами використаних апаратних ресурсів [7; 8]. Це знижує ймовірність одночасного ушкодження кількох каналів локальними дефектами кристалу, радіаційними подіями або локальними перевантаженнями по живленню, а також послаблює вплив можливих систематичних помилок інструментальних засобів синтезу та розміщення. У поєднанні з вимогами стандартів IEC 61226 та IEC 61508 така структурно просторова диверсність розглядається як один з ефективних механізмів підвищення фізичної незалежності каналів безпеки.

Диверсність програмно апаратних засобів і процедур підрахунку контрольної суми орієнтована на підвищення надійності контролю цілісності даних у каналах захисту та комунікаційних інтерфейсах [9; 10]. У різних каналах застосовуються відмінні за природою апаратно програмні реалізації: різні сімейства мікроконтролерів або FPGA, апаратні інтерфейси передачі даних, різні стеки бібліотек і драйверів, альтернативні шляхи формування та обробки повідомлень. Одночасно використовуються різнорідні алгоритми контрольних сум (CRC 16, CRC 32, поліноміальні LFSR зі зміщеними поліномами й ініціалізаціями), а також відмінні режими та формати обчислення (апаратні CRC модулі проти програмних реалізацій, різні порядки байтів, вставка додаткових службових полів). Така диверсифікація зменшує ризик спільних логічних помилок у реалізації алгоритмів, підвищує ймовірність виявлення прихованих спотворень даних і зменшує вірогідність того, що одна й та сама помилка залишиться непоміченою в усіх каналах одночасно, що є критично важливим для запобігання відмовам за загальною причиною у системах захисту реакторів.

Під час розробки проєктів для систем захисту реакторів, модельно-базоване тестування (Model-Based Testing, MBT) використовується для формалізованої перевірки логіки спрацювання та часових обмежень критичних функцій. Підхід передбачає побудову моделі поведінки (стани, переходи, інваріанти безпеки, часові умови), на основі якої автоматично формуються тестові сценарії для штатних, перехідних і аварійних режимів, у тому числі зі сценаріями відмов за загальною причиною [11; 12]. Таке представлення забезпечує простежуваність від вимог до тестів і дозволяє кількісно контролювати покриття властивостей безпеки відповідно до підходів, закріплених у міжнародних стандартах для ІКС АЕС.

Практична процедура включає послідовність етапів: специфікація вимог безпеки у вигляді перевірюваних властивостей; побудова графа станів/переходів із часовими обмеженнями; автоматична генерація тестів із критеріями покриття (стани, переходи, граничні таймінги, негативні сценарії); виконання тестів на моделі та на цільовому обладнанні з реєстрацією журналів; аналіз покриття і регресійний перезапуск після змін.

Ключові метрики охоплюють: покриття станів/переходів, покриття граничних часових умов (мінімальні/максимальні затримки, таймаути), покриття сценаріїв CCF і їх комбінацій, частку виявлених відхилень до етапу натурних випробувань. Для систем, важливих для безпеки, доцільно фіксувати порогові значення покриття та зберігати артефакти (моделі, згенеровані тести, звіти покриття) як доказову базу для аудитів і регуляторної оцінки, що відповідає практикам оперативного інформування та звітності, які застосовує МАГАТЕ у своїх оновленнях щодо ядерної безпеки в Україні.

Таким чином, принцип диверсності, який враховує можливості сучасних програмовних технологій, дозволяє розширити поле можливих рішень стосовно вибору видів версійної надмірності для запобігання відмовам за загальною причиною.

Бібліографічні посилання

1. Ставченко С. Ядерний тероризм: особливості в умовах російсько-української війни. ББК 60.5 З 41. 2024. Р. 56.

2. Щигельська Г., Боднар В. Загрози надзвичайних ситуацій на атомних електростанціях в умовах нового етапу російсько-української війни. Збірник тез ІІ Міжнародної наукової конференції „Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки ". 2022. Р. 99–101.

3. Illiashenko O., Kharchenko V., Kor A.-L., Panarin A., Sklyar V. Hardware diversity and modified NUREG/CR-7007 based assessment of NPP I&C safety. 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)(2017). IEEE, 2017. Also available online, URL: https://ieeexplore.ieee.org/abstract/document/8095218/ P. 907–911.

4. Duzhyi V., Kharchenko V., Panarin A., Rusin D. Diversity metric evaluation considering extended NUREG-7007 diversity classification. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)(2018). IEEE, 2018. Also available online, URL: https://ieeexplore.ieee.org/abstract/document/8409092/ P. 21–25.

5. Kharchenko V., Babeshko E., Leontiiev K., Duzhy V. Diversity for safety and security of NPP I&C: post NUREG/CR 7007 stage. 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2017(2017). Also available online, URL: https://elibrary.ru/item.asp?id=35747452 P. 1528–1536.

6. Davari M., Gao W., Aghazadeh A., Blaabjerg F., Lewis F. L. An optimal synchronization control method of PLL utilizing adaptive dynamic programming to synchronize inverter-based resources with unbalanced, low-inertia, and very weak grids. IEEE Transactions on Automation Science and Engineering. Vol. 22, 2024. P. 24–42.

7. Sklyar V., Siora O., Herasimenko O., Panarin A. Development and Verification of Dependable Multiversion Systems on the basis of IP-Cores. Technical Approach to Dependability.–Wroclaw, Oficyna Wydawnicza Politechnki Wroclawskiej. 2010. P. 133–145.

8. Nangia R., Shukla N. K. Resource utilization optimization with design alternatives in FPGA based arithmetic logic unit architectures. Procedia computer science. Vol. 132, 2018. P. 843–848.

9. Abdulnabi M. S., Ahmed H. Design of efficient cyclic redundancy check-32 using FPGA. 2018 International conference on computer, control, electrical, and electronics engineering (ICCCEEE)(2018). IEEE, 2018. Also available online, URL: https://ieeexplore.ieee.org/abstract/document/8515877/ P. 1–5.

10. Zitlaw C., Sayeed A., Lim S. L. CRC Integration for Enhanced SPI Communication Reliability in Digital Systems. 2024 Multimedia University Engineering Conference (MECON)(2024). IEEE, 2024. Also available online, URL: https://ieeexplore.ieee.org/abstract/document/10776358/ P. 1–5.

11. Панарин А. С. Имитационное моделирование soft-процессоров на базе концепции Model-Based Testing. Радіоелектронні і комп'ютерні системи. 2012, 5. С. 100–106.

12. Скляр В. В., Харченко В. С., Панарин А. С. Тестирование и разработка диверсных программируемых логических контроллеров на базе ПЛИС с использованием среды функционального программирования. Радіоелектронні і комп'ютерні системи. 2014, 1. С. 29–41.

A. Panarin

Principle of diversity and multi-version technologies for nuclear reactor protection systems.

Abstract. The paper considers the application of the principle of diversity and multi-version technologies to improve the functional safety of nuclear reactor protection systems implemented on FPGA/SoC-based platforms. The relevance of the study stems from the growing role of common cause failures (CCF) in modern NPP instrumentation and control (I&C) systems and the deployment of highly integrated programmable hardware-software solutions. The work analyses the requirements of international standards and IAEA recommendations regarding diversity and multi-version architectures, as well as the specifics of their implementation in Ukrainian and international practice. An extended classification of diversity types for programmable platforms, graph and matrix models of diversity representation, and a method for selecting diversity configurations based on diversity and relative cost metrics are proposed. Methods for implementing hardware-software diversity (diverse synchronization, structural-spatial diversity, diversified integrity control) are discussed. Particular attention is paid to integrating model-based testing (MBT) into the life cycle of reactor protection systems and to implementing the proposed solutions in Radiy and RadICS platform-based systems.

Keywords: NPP I&C systems, reactor protection systems, functional safety, diversity, multi-version technologies, FPGA, model-based testing.

Зразок для цитування:

Панарін А. Принцип диверсності та багатоверсійні технології для систем захисту реакторів атомних електростанцій. Пропілеї права та безпеки, 2025. №8. С. 260-263. DOI: https://doi.org/10.32620/pls.2025.8.67.