 ISSN 2071-1077(print)
ISSN 2663-2411(online

doi: 10.32620/oikit.2026.108.14

УДК 004.42:629.78

Ю. С. Манжос, Є. В. Соколова

Ймовірнісні моделі апаратної надійності та цілісності даних у кіберфізичних системах

Національний аерокосмічний університет «Харківський авіаційний інститут»

У статті досліджується надійність кіберфізичних систем з акцентом на апаратні відмови та їх поширення у програмному забезпеченні і зовнішніх фізичних процесах. Проаналізовано основні джерела відмов у підсистемах обчислення, пам’яті, комунікації, живлення та сенсорики з урахуванням впливу факторів середовища функціонування, зокрема радіації, електромагнітних завад і температурних навантажень. Розглянуто механізми виникнення одно-, багатобітових збоїв, а також пакетних помилок. Проаналізовано механізми підсилення помилок через програмні алгоритми та зворотні зв’язки. Введено формальні залежності для оцінювання інтенсивності небезпечних невиявлених відмов. Показано, що підсистеми пам’яті та передачі даних є критичними для забезпечення надійності, а інтегровані апаратно-програмні методи захисту є необхідними для функціональної безпеки. Запропоновано ймовірнісні моделі відмов пам’яті, що враховують як незалежні, так і корельовані помилки, а також ефекти старіння. Введено формальні залежності для оцінювання інтенсивності небезпечних невиявлених відмов з урахуванням діагностичного покриття. Окрему увагу приділено механізмам поширення та підсилення помилок через програмні реалізації алгоритмів, зворотні зв’язки та збереження стану, що є характерною особливістю кіберфізичних систем. Обґрунтовано необхідність застосування інтегрованих апаратно-програмних методів захисту та використання моделювання для підвищення надійності й забезпечення функціональної безпеки кіберфізичних систем.

Ключові слова: кіберфізичні системи; надійність; пам’ять; відмови; функціональна безпека.

Вступ

Надійність сучасних кіберфізичних систем (Cyber-Physical Systems КФС), які інтегрують сенсорні, обчислювальні, комунікаційні та керуючі підсистеми і функціонують у тісному зв’язку з фізичними процесами в умовах реального часу [1-3], визначається не лише коректністю алгоритмів і програмного забезпечення (ПЗ), але й фізичною цілісністю апаратного забезпечення. Зокрема, критичну роль відіграють підсистеми пам’яті, обчислення та передачі даних, які формують основу інформаційних потоків у КФС [4-7].

На відміну від традиційних систем, у КФС порушення цілісності даних або часових характеристик безпосередньо впливає на фізичні процеси, що може призводити до небезпечних дій. Тому надійність КФС слід розглядати як інтегровану властивість, що формується взаємодією програмно-апаратних компонентів.

Складність полягає в тому, що апаратні відмови, особливо в пам’яті, часто проявляються як приховані спотворення даних, які накопичуються та підсилюються під час виконання алгоритмів. Це обумовлює необхідність формалізації моделей відмов і аналізу їх поширення у КФС, що широко застосовуються у критичних галузях (авіації, автомобільній електроніці, промисловості, медицині), де навіть короткочасні збої можуть призводити до втрати керованості або порушення функціональної безпеки.

Сучасні тенденції розвитку мікроелектроніки, пов’язані зі зменшенням

технологічних норм, призводять до зменшення критичного заряду, необхідного для перемикання транзисторів, що суттєво підвищує чутливість інтегральних схем до радіаційних впливів і електромагнітних збурень [8-9]. Унаслідок цього зростає частота так званих м'яких помилок (soft errors), зокрема SEU (Single Event Upset), які виникають навіть у звичайних умовах експлуатації.

Емпіричні дослідження показують, що підсистеми пам'яті є одними із основних джерел відмов у сучасних обчислювальних системах, причому значна частина помилок має латентний характер і не виявляється стандартними засобами контролю [10-12]. Це особливо небезпечно для КФС, де пошкоджені дані можуть поширюватися через алгоритми керування та зворотні зв'язки, призводячи до нелінійного підсилення помилок.

Актуальність дослідження зумовлена необхідністю врахування фізичних механізмів апаратних відмов, розроблення ймовірнісних моделей помилок, аналізу їх поширення в контурах керування та створення інтегрованих методів забезпечення надійності, бо сучасні КФС включають підсистеми пам'яті, комунікації (узгодженість між вузлами) та процесори реального часу, а саме ці підсистеми формують найбільший внесок у загальну інтенсивність відмов [8, 10, 11, 13-15], тому ефективне підвищення надійності можливе лише за рахунок цілеспрямованого їх.

На відміну від традиційних інформаційних систем, у КФС: помилки не обмежуються цифровим рівнем, поширюються на фізичні процеси, існують зворотні зв'язки, що підсилюють відмови. Це призводить до прихованого пошкодження даних SDC (Silent Data Corruption), яке не виявляється та може накопичуватися системою [12, 16, 17]. Таким чином, проблема забезпечення надійності КФС є багаторівневою.

Практична цінність роботи полягає у розробленні формалізованих моделей апаратно-обумовлених відмов та методів їх аналізування, що дозволяють підвищити надійність КФС шляхом раннього виявлення та запобігання поширенню помилок у процесах керування.

1. Аналізування останніх досліджень і публікацій

Основи теорії КФС закладені у роботах [1-3], що визначають архітектурні принципи інтеграції обчислювальних і фізичних процесів та формулюють вимоги до часової детермінованості та взаємодії компонентів. Подальший розвиток КФС, архітектур систем реального часу та вбудованих систем подано у роботах [4-6], де розглядаються питання ресурсних обмежень, енергоспоживання та надійності. Автори у [18, 19] дають моделі взаємодії програмно-апаратних (ПА) підсистем, зокрема через гібридні автомати та формальні методи.

Дослідження надійності апаратного забезпечення, зокрема впливу радіаційних факторів, представлені авторами у [8-11], де описані механізми виникнення SEU та показано, що зі збільшенням інтеграції зростає вплив корельованих багатобітових помилок (Multiple Bit Upset) та просторової кореляції помилок [20] на надійність пам'яті. У роботі [21] досліджено фізичні механізми генерації заряду в CMOS-структурах під дією радіації, а також вплив топології мікросхем на поширення помилок, що дозволяє більш точно оцінювати інтенсивність відмов.

Методи підвищення надійності пам'яті, включаючи ECC (Error Correction Codes), резервування та надлишковість, розглянуто у [11, 13, 22-24]. Сучасні підходи, орієнтовані на багатобітові помилки, включають багатовимірні коди,

LDPC та Reed–Solomon [25]. Проблема корельованих помилок у пам’яті детально досліджується у [21, 25], де визначається, що традиційні ECC-схеми втрачають ефективність при кластеризованих пошкодженнях, а також розглядаються методи фізичного рознесення бітів.

Автори у джерелах [14, 15] проаналізували комунікаційні аспекти КФС і показали, що суттєва деградація мережі (затримки, втрати пакетів даних) впливає на системну надійність і стабільність керування. У роботах [19, 26] досліджується взаємозв’язок між обчислювальними помилками та фізичними процесами, що є ключовим для КФС. Показано, що навіть незначні помилки можуть призводити до значних відхилень через механізми зворотного зв’язку.

Огляд сучасних підходів до забезпечення надійності показали автори у [27], а програмні методи підвищення відмовостійкості – у [28, 29], включаючи моніторинг, перевірки узгодженості та контроль потоку виконання. Проблема SDC активно досліджується у [16, 17], де автори показали, що значна частина помилок залишається невиявленою традиційними механізмами контролю. У дослідженнях [27, 28] автори запропонували інтегровані підходи до забезпечення надійності КФС, які поєднують ПА-методи на різних рівнях проєктування.

Аналізування сучасної наукової літератури показує, що: класичні моделі добре описують незалежні помилки; сучасні дослідження акцентують увагу на корельованих відмовах; роботи підкреслюють важливість динаміки КФС; новітні підходи орієнтовані на інтеграцію ПА-методів.

Попри значний обсяг досліджень, залишаються такі проблеми: недостатній облік корельованих помилок; відсутність інтегрованих ПА моделей; обмежене аналізування поширення помилок у КФС (з урахуванням зворотних зв’язків); недостатнє моделювання SDC як системного явища; відсутність моделей, що інтегровані у практичні CPS-симуляції. Ці прогалини обґрунтовують необхідність подальших досліджень.

2. Мета дослідження

Метою статті є розроблення та аналізування моделей апаратно-обумовлених відмов у КФС із урахуванням їх поширення через ПЗ та фізичні процеси. Для досягнення поставленої мети слід вирішити такі задачі: проаналізувати джерела апаратних відмов у КФС; формалізувати моделі однобітових, багатобітових та пакетних помилок; дослідити механізми поширення та підсилення відмов; побудувати модель системної надійності.

3. Основні типи апаратних відмов

КФС є новим класом систем, що інтегрують обчислення, комунікацію та керування фізичними процесами в реальному часі [1-3]. Надійність КФС визначається коректністю ПЗ і фізичною цілісністю апаратних компонентів [4] в умовах: електромагнітних завад, температурних коливань, радіаційного впливу, нестабільного живлення. Це призводить до виникнення як тимчасових, так і постійних відмов пам’яті, як це написано у роботах авторів [6-9].

Сумарна інтенсивність відмов описується:

$$\lambda_{system} = \lambda_{CPU} + \lambda_{memory} + \lambda_{bus} + \lambda_{power} + \lambda_{I/O},$$

де λ − інтенсивність відмов: системи, процесора, пам’яті, шини, джерела живлення та підсистеми вводу/виводу.

Найважливішими для надійності КФС є пам’ять і комунікаційні підсистеми

[7-10], на роботу яких впливають різноманітні помилки: (див. Табл. 1) SEU − одинична зміна біта пам’яті під дією зарядженої частинки [8]. MBU − одночасне пошкодження кількох бітів [11]. Для сучасних технологій багатобітові помилки стають домінуючими, як відзначили автори у [10]. Пакетні помилки охоплюють послідовні біти або слова та породжуються електромагнітним впливом, збоями живлення тощо.

Таблиця 1

Багатобітові та пакетні помилки

	MBU- корельовані помилки	**Burst Error – пакетні помилки**
Природа	Це тип «м'якої» помилки (soft error), яка виникає, коли одна енергетична частинка (наприклад, космічний промінь або нейтрон) влучає в чип і перевертає значення відразу в декількох сусідніх комірках пам'яті. Випадкові за часом (soft error).	Це серія помилок, які відбуваються в багатьох послідовних бітах під час передачі або зчитування даних через завади, фізичні дефекти, збої ліній. Може бути постійною через апаратний дефект: EMI, шини, живлення тощо.
Час	Час життя триває миттєво.	Час життя може тривати довго.
Особливість	Біти зазвичай пошкоджуються в межах одного фізичного слова або сусідніх логічних адрес. Зі зменшенням техпроцесу ймовірність MBU зростає, оскільки комірки розташовані щільніше.	Вони не обов'язково викликані радіацією; причиною можуть бути електромагнітні завади, фізичні дефекти (подряпини на диску) або несправність цілої лінії передачі даних (наприклад, вихід з ладу одного каналу в чипі). Послідовні біти в потоці даних.
Виправлення	Традиційні алгоритми ECC (SEC-DED) можуть виявити MBU, але часто нездатні їх виправити, оскільки вони розраховані лише на одиночні бітові збої. Захист: Спеціальні коди для суміжних бітів.	Потрібен метод interleaving, що переставляє дані і робить з одного пакету однобітних помилок кілька незалежних однобітових помилок. Захист: Коди Ріда-Соломона, перемежування.

Стандартна пам'ять може виправити 1 біт і лише виявити дві помилки. Для боротьби з корельованими та пакетними помилками використовують просунуті технології, такі як ChipKill [32], які дозволяють КФС продовжувати роботу навіть у разі повного виходу з ладу цілого чипа пам'яті.

3.1. Пакетні помилки

Основні причини цих помилок: EMI (Electromagnetic Interference) – електромагнітні завади можуть індукувати спотворення сигналу в лініях передачі або шині даних; збої живлення – короткочасні просідання напруги можуть призводити до некоректного запису або читання серій бітів; порушення цілісності сигналу – відбиття, затухання, перехресні перешкоди; збої синхронізації – порушення умов у цифрових схемах; помилки шин і DMA (Direct Memory Access) – пошкодження під час масових передач даних. Характерні властивості: помилки виникають у суміжних адресах пам’яті або послідовних бітах потоку; можуть

охоплювати як окремі слова, так і великі блоки даних; часто мають часову локалізацію (виникають протягом короткого інтервалу).

Стандартні ECC (наприклад, SECDED) неефективні для довгих пакетів, тому необхідні: рознесення бітів, багатовимірні коди, контрольні суми та блокові перевірки. Пакетні помилки критичні для швидкісних інтерфейсів і пам’яті.

3.2. Старіння

Старіння елементів мікроелектроніки є повільним деградаційним процесом, що з часом підвищує інтенсивність відмов і формує довготривалу компоненту надійності системи [12].

Основні фізичні механізми:

1. BTI (Bias Temperature Instability): викликає зміну порогової напруги транзисторів; залежить від температури та напруги та призводить до уповільнення логічних елементів.

2. HCI (Hot Carrier Injection): гарячі носії заряду пошкоджують оксид затвора, що спричиняє деградацію параметрів транзистора та впливає на швидкодію та надійність перемикання.

3. Електроміграція (Electromigration) обумовлена переміщенням атомів у провідниках під дією струму; призводить до утворення розривів або коротких замикань; критична для міжз’єднань (interconnects).

Характерні особливості старіння: має накопичувальний характер;залежить від: температури (модель Арреніуса), напруги, режиму роботи; призводить до: stuck-at відмов, зростання затримок, втрати збереження даних.

Інтенсивність відмов через старіння $\lambda_{aging}(t)$ збільшується з часом та з температурою: $\lambda_{aging}(T) = \lambda_{aging0} \exp(-E_a/(kT))$, де λ_{aging} (T) [1/час] – інтенсивність відмов через старіння при температурі T; λ_{aging0} [1/час] – передекспоненціальний множник, що означає інтенсивність відмов при «умовно нескінченній температурі» (нормувальний коефіцієнт) та залежить від: технології (CMOS, FinFET), якості виробництва і матеріалів та визначається експериментально; E_a [Дж або електрон-вольти eV] – енергія активації, що відповідає енергії, яка необхідна для запуску деградаційного процесу, наприклад: BTI (Bias Temperature Instability), HCI (Hot Carrier Injection), електроміграція, що мають типові значення: 0.3–0.7 [eV] для BTI; 0.7–1.1 [eV] для електроміграції; k – константа Больцмана, що визначає зв’язок між температурою і енергією частинок і має значення $k = 1.38 \times 10^{-23}$ [Дж/К] або 8.617×10^{-5} [eV/К]; T [Кельвіни K] – абсолютна температура середовища зі збільшенням якої знаменник kT зростає, інтенсивність відмов зростає експоненційно тому підвищення температури призводить до швидкого старіння та збільшення відмов, а кожні +10–15 °C подвоюють або навіть потроюють інтенсивність відмов, ось чому потрібна терморегуляція.

Як видно на рисунку 1, інтенсивність відмов залежить від поточної температури і енергії активації деградації і збільшується приблизно в 100 разів при збільшенні температури на 100 градусів.

На рисунку 2 відображена відносна інтенсивність відмов, що утворює експоненційну залежність. При зміні температури від -100 С до 100 С відносна інтенсивність відмов змінюється на 10 порядків.

Модель Арреніуса добре описує експоненційну залежність надійності від температури, що є критичною для проєктування КФС: довготривале старіння та термічно активовані процеси, але НЕ враховує: радіаційні ефекти, які призвдять

ISSN 2071-1077(print)
ISSN 2663-2411(online

до однобітових спотворень даних, випадкові помилки та корельовані збої а даних. Старіння формує довготривалу складову ризику SDC.

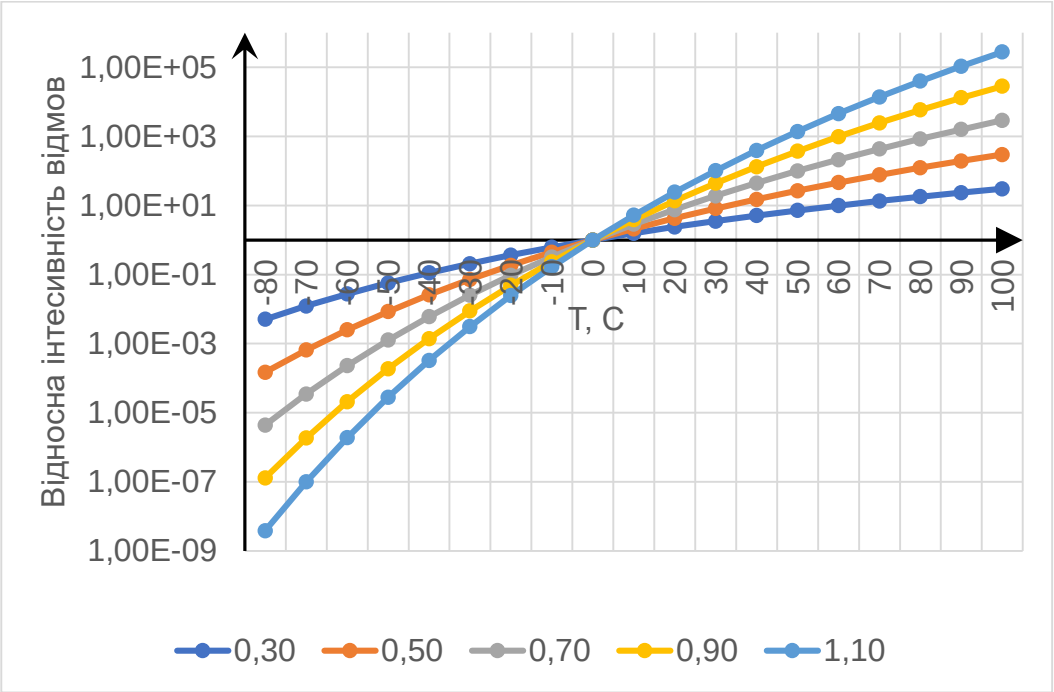

Рис. 1. Відношення поточних інтенсивностей до інтенсивності відмов при T=0 C

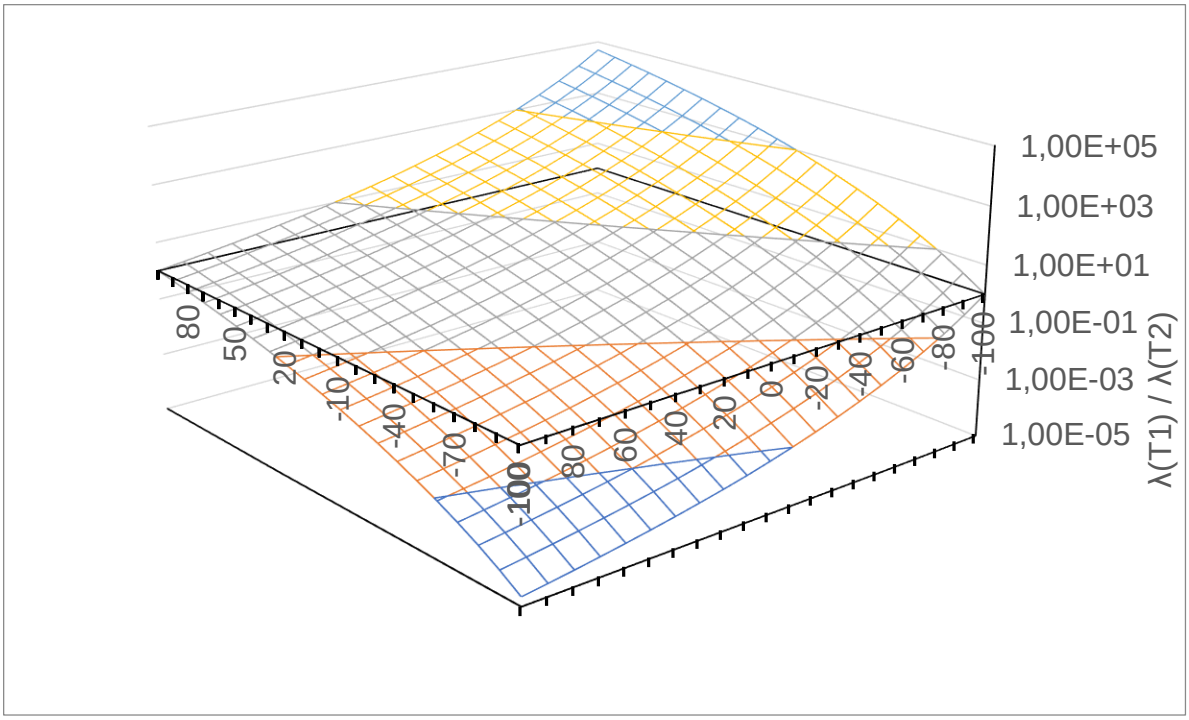

Рис. 2. Відношення $\lambda_{aging}(T_1)/ \lambda_{aging}(T_2)$ для E_a=0.3 eV

3.3. Комунікаційні відмови

Комунікаційна підсистема КФС забезпечує обмін даними та узгодженість стану між розподіленими компонентами системи (сенсорами, контролерами та

виконавчими механізмами). На відміну від локальних збоїв, комунікаційні помилки мають властивість реплікуватися між вузлами, що призводить до системної неузгодженості та виникнення прихованих спотворень даних (SDC) на рівні мережі [14, 15]. Особливої ваги набуває аналіз SDC у мережевих протоколах, оскільки такі помилки можуть залишатися невиявленими протягом багатьох циклів керування [16]. Особливості комунікаційних відмов для КФС: помилки можуть накопичуватися у зворотних зв'язках; затримки можуть призводити до нестабільності систем керування; некоректні дані можуть викликати розбіжність станів вузлів.

3.3.1. Біноміальна модель незалежних бітових помилок)

Модель описує канал із незалежними шумовими спотвореннями. Звичайно $p_b \in [10^{-12}, 10^{-3}]$ – ймовірність помилки одного біта (безрозмірна величина), n– довжина пакета (у бітах, типово 10^2 … 10^6). Ймовірність того, що пакет містить хоча б одну помилку: $P_{packet} = 1 - (1 - p_b)^n$. Обмеження застосування моделі: не враховує кореляцію помилок; не описує пакетні ефекти; не придатна для реальних КФС-мереж (CAN, Ethernet, SpaceWire); коректна лише для ідеалізованих каналів або попередніх оцінок.

3.3.2. Модель Гілберта–Елліотта (Gilbert–Elliott)

Ця модель описує канал як дискретний марковський процес із двома станами: Good (G) – низький рівень помилок, Bad (B) – високий рівень помилок.

Параметри моделі:

$p_G \in [10^{-12}, 10^{-6}]$ – ймовірність помилки у стані G;

$p_B \in [10^{-3}, 10^{-1}]$ – ймовірність помилки у стані B;

$P_{GB} \in [10^{-6}, 10^{-2}]$ – ймовірність переходу із стану G до стану B;

$P_{BG} \in [10^{-3}, 10^{-1}]$ – ймовірність переходу із стану B до стану G.

Стаціонарні ймовірності станів: $\pi_G = P_{BG}/(P_{BG} + P_{GB})$, $\pi_B = P_{GB}/(P_{BG} + P_{GB})$.

Фізичний зміст: стан G – нормальна робота каналу; стан B – вплив перешкод (EMI, збої живлення, перевантаження мережі).

Переваги: описує пакетні помилки; враховує кореляцію; придатна для CPS.

Обмеження: двостанове наближення може бути недостатнім; не враховує топологію мережі.

3.3.3. Модель втрат пакетів

Втрати пакетів моделюються як пуассонівський процес:

$$P_{loss}(k) = (\lambda_{loss}\, T)^k \exp(-\lambda_{loss}\, T)/\, k!,$$

де λ_{loss} – інтенсивність втрат [1/с] (типово $[10^{-6}, 10^{-1}]$), T – час спостереження [с]. Ймовірність хоча б однієї втрати: $P_{loss} = 1 – \exp(-\lambda_{loss}\, T\}$

Фізичний зміст: описує випадкові втрати через перевантаження буферів, колізії, відмови каналів.

Обмеження не враховує пакетні втрати та залежності між пакетами.

3.3.4. Модель затримки передачі

Загальна затримка: $D = D_{proc} + D_{queue} + D_{trans} + D_{prop}$, де: D_{proc} – оброблення 1-1000 [мкс], D_{queue} – затримка в черзі 0–100 [мс], D_{trans} – тривалість передачі залежить від полоси частот, D_{prop} – поширення 1 [нс] - 1 [мс].

3.3.5. Джиттер (варіація затримки)

Джиттер визначається як дисперсія затримки: J = Var(D), або $J = E[(D - E[D])^2]$, де E математичне очікування. Типові значення: Ethernet: 10^{-9} – 10^{-6} [сек²], wireless: 10^{-6} – 10^{-2} [сек²]. Фізичний зміст: викликає: фазові зсуви, втрату синхронізації, нестійкість регуляторів.

3.3.6. Вплив на системи керування

Затримка у зворотному зв'язку $x_{k+1} = A\,x_k + B\,u_{k-d}$, де d – затримка (дискретні такти), може спричиняти нестійкість і змінювати фазові характеристики.

Втрати вимірювань y_k = виміряне значення, з ймовірністю 1 - p_{loss} та y_k =0 або ∅ з ймовірністю p_{loss} призводить до деградації оцінки стану

Стохастична модель $x_{k+1} = A\,x_k + B\,u_k + \omega_k$, де ω_k – шум, що включає комунікаційні помилки.

3.3.7. Загальна інтенсивність комунікаційних відмов

$\lambda_{comm} = \lambda_{bit} + \lambda_{packet} + \lambda_{loss} + \lambda_{delay}$

де λ_{bit} – інтенсивність бітових помилок [1/с],

λ_{packet} – інтенсивність пакетних помилок[1/с],

λ_{loss} – інтенсивність втрати пакетів даних [1/с],

λ_{delay} – інтенсивність критичних затримок даних [1/с].

Приклад 1: $\lambda_{bit}=10^{-6}$ [$с^{-1}$] $\lambda_{packet}=5\cdot10^{-5}$ [$с^{-1}$] $\lambda_{loss}=2\cdot10^{-4}$ [$с^{-1}$] $\lambda_{delay}=1\cdot10^{-4}$ [$с^{-1}$], тоді: $\lambda_{comm}=10^{-6}+5\cdot10^{-5}+2\cdot10^{-4}+10^{-4}=3.51\cdot10^{-4}$ [$с^{-1}$].

Очікувана кількість відмов≈0.000351 [відмов/с] ≈ 1відмова за кожні 47 хв

Домінує втрата пакетів та затримки, а не бітові помилки.

Приклад 2 (високонадійна система): $\lambda_{bit}=10^{-9}$, $\lambda_{packet}=10^{-6}$, $\lambda_{loss}=10^{-6}$, $\lambda_{delay}=10^{-6}$, $\lambda_{comm}=3.001\cdot10^{-6}$, тобто приблизно 1 відмова кожні ~92 години.

3.3.8. Модель поширення помилок у мережі

Комунікаційні помилки можуть: реплікуватися між вузлами, синхронізуватися (shared state), викликати глобальні відмови. Ймовірність поширення: $P_{prop}^{net} = 1 - (1 - p)^N$ де N – кількість вузлів. Комунікаційні відмови можуть призводити до некоректних, але допустимих значень та відсутності сигналізації помилки, що формує SDC на рівні мережі. Модель враховує: стохастику помилок, затримки, втрати; не враховує: складні протоколи (TCP, CAN, TSN); адаптивні механізми повторної передачі; кіберзагрози.

Ймовірність поширення помилок між вузлами: $P_{prop}^{net} = 1 - (1 - p)^N$, де p – ймовірність помилки в одному вузлі, N – кількість вузлів.

Фізичний зміст: при великому N: P_{prop}^{net} наближається до одиниці, навіть малі помилки масштабуються до системного рівня.

Приклад: велика мережа CPS з p=0.01, N=50, $P_{propnet} = 1-(0.99)^{50}$ $P_{propnet} =1-0.605=0.395$, відповідає ~40% ризику поширення помилки.

Комунікаційні відмови можуть не викликати явної помилки та передавати "правдоподібні, але неправильні" значення, що формують SDC на рівні мережі КФС. Таким чином:

1. Біноміальна модель є базовою, але недостатньою.
2. Модель Гілберта–Елліотта є ключовою для КФС.
3. Джиттер є критичним параметром для систем керування.

4. Комунікаційні відмови мають мультифакторну природу.

5. Масштабування мережі підсилює ризик системних відмов.

Пакетні помилки, ефекти старіння та комунікаційні відмови є взаємодоповнюючими джерелами ризику у КФС. Їх поєднання формує складну багаторівневу картину відмов, яка не може бути адекватно описана лише простими моделями незалежних помилок, що обґрунтовує необхідність використання інтегрованих ймовірнісних та системних моделей надійності.

3.4. Моделі відмов пам’яті

3.4.1. Модель одиничних збоїв

Призначення моделі: модель використовується для оцінювання частоти одиничних збоїв SEU у пам’яті за умов випадкових незалежних подій, характерних для впливу радіації або шумів.

Обмеження застосування: передбачає незалежність бітових збоїв; не враховує просторову кореляцію; не описує багатобітові ефекти MBU; точність моделі зменшується для сучасних технологій виготовлення мікросхем.

Причини деградації моделі:

1. Зменшення критичного заряду призводить до того, що один зовнішній удар спотворює одразу кілька бітів.

2. Висока щільність розміщення бітових комірок призводить до одночасного спотворення кількох бітів.

3. Через зовнішній вплив електричний заряд бітових комірок поширюється між вузлами.

4. 3D-ефекти призводить до вертикальної кореляції між комірками пам’яті

Через це порушується незалежність бітових комірок і SEU перетворюється на ідеальний випадок.

Параметри: λ_{bit} − інтенсивність збоїв одного біта; N − загальна кількість бітів пам’яті; T − час. Очікувана кількість збоїв: $\Lambda = N \lambda_{bit} T$. Тоді ймовірність спотворень k бітів визначається так: $P_k = \Lambda^k \exp(-\Lambda)/k!$. Ймовірність хоча б одного збою: $P_{SEU} = 1 – \exp(-\Lambda)$.

Модель SEU є базовою для первинної оцінки надійності, однак у сучасних КФС її необхідно доповнювати моделями корельованих відмов.

3.4.2. Модель корельованих подій

Призначення моделі: багатобітові збої MBU, що виникають через фізичну близькість комірок пам’яті та вплив єдиної події.

Параметри: λ_{event} − інтенсивність подій [1/год або 1/сек], тобто частота зовнішніх фізичних впливів (частинки, EMI тощо); λ_{SEU} – інтенсивність однобітових спотворень (використовують модель одиничних збоїв); m – кількість бітів, уражених однією подією (безрозмірна величина); p_m − ймовірність ураження точно m бітів однією подією.

Обмеження застосування: потребує експериментального визначення функції f(m); залежить від топології пам’яті та технологічного процесу; складна для аналітичного застосування без статистичних даних.

Визначимо інтенсивність багатобітових помилок як $\lambda_{MBU} = \lambda_{event} \cdot p_m$, тому ефективна інтенсивність буде $\lambda_{bit,eff} = \lambda_{SEU} + m \lambda_{MBU}$ збоїв на біт за секунду.

Для опису просторової кореляції: $P(m) = f(m)$, де $f(m)$ залежить від топології пам’яті [9] та визначає, наскільки небезпечні MBU для ECC, якщо $P(m>t)$ велике,

то ECC неефективний. Функція розподілу f(m) = P(m) відповідає розподілу кластера пошкоджених бітів. Типові приклади:

1. Геометричний розподіл (експоненційний спад): $P_m = (1- \alpha)\ \alpha^{m-1}$ характерний для слабкої кореляції. Параметри: $\alpha \in [0,1)$ − ймовірність поширення події на ще один біт; m − кількість бітів, уражених однією MBU-подією. Моделює слабко корельовані події: більшість подій уражає 1–2 біти, довгі кластери рідкісні. Чим більше α, тим більша ймовірність появи великих кластерів. Середня кількість уражених бітів: E[m]=1/(1−α). Використовується, коли події переважно локальні та не сильно залежать від топології пам'яті.

2. Пуассонівський розподіл: $P(m)=\mu^m \exp(-\mu)/m!$ використовується, якщо кількість уражених бітів випадкова без сильної локалізації. Параметри: μ − середня кількість уражених бітів на одну подію; m − кількість уражених бітів. Модель підходить, коли кількість уражених бітів випадкова, без сильної локалізації. Часто використовується для апаратних симуляцій, де кожен удар радіації може пошкодити різну кількість бітів незалежно. Середнє та дисперсія збігаються: E[m]=Var[m]=μ.

3. Степеневий закон (важкі хвости): $P(m) \sim m^{-\beta}$, де m≥1 описує рідкі, але великі кластери. Параметри: β>1 − показник степеня, який визначає "тяжкість хвоста"; m − кількість уражених бітів. Використовується для рідкісних, але великих кластерів. Ймовірність великих багатобітових помилок не зникає швидко, тому важливо для оцінки ризику перевищення можливостей методів і засобів захисту пам'яті. Середнє значення та дисперсія залежать від β: для β≤2 дисперсія нескінченна, що відображає високі коливання. Багатобітові помилки є домінуючими у сучасних технологіях, тому їх урахування є критичним для оцінки ефективності методів і засобів захисту пам'яті.

3.4.3. Модель пакетних помилок

Призначення моделі: модель описує послідовні (кластерні) пошкодження даних, що виникають через збої шин, EMI або порушення цілісності сигналу.

Параметри: *l* − довжина пакета (кількість послідовних бітів/слів); q − параметр геометричного розподілу (ймовірність завершення пакета); t − коригувальна здатність ECC (макс. кількість помилок, що може бути виправлена); E[L] − математичне сподівання довжини пакета.

Обмеження застосування: передбачає геометричний розподіл довжини пакета; не враховує складні залежності між пакетами; параметр q потребує калібрування.

Геометричний розподіл $P(L = l) = (1 - q)^{l-1}q$ означає, що кожен наступний біт пошкоджується з імовірністю 1−q , а пакет завершується з імовірністю *q.* Таким чином, малому значенню q відповідають довгі пакети, а великому q відповідають короткі пакети. Середня довжина пакета визначається як: E[L] = 1/q. Ймовірність перевищення порога відновлення ECC буде: $P(L > t) = (1 - q)^t$. У реальних системах пакети є залежними через:

1. Кореляцію помилок у часі: один пакет підвищує ймовірність наступного (наприклад, через перегрів).

2. Просторову залежність: сусідні банки пам'яті мають пов'язані відмови.

3. Самозбуджувані процеси: події породжують нові події.

Тому необхідно емпірично калібрувати параметр q=1/E[L], а також оцінити частоти довжин пакетів методом максимальної правдоподібності: $\hat{q} = 1 / \bar{L}$.

Пакетні помилки можуть перевищувати можливості класичних ECC, тому необхідно використовувати багатовимірні коди та перестановки бітів.

3.4.4. Узагальнена модель

Призначення моделі: інтегрує всі основні механізми відмов для комплексної оцінки надійності пам’яті

$$\lambda_{total} = \lambda_{SEU} + \lambda_{MBU} + \lambda_{burst} + \lambda_{aging}, \lambda_{UD} = \lambda_{total}(1 - C)$$

Параметри узагальненої моделі:

1. Інтенсивності [1/час]: λ_{SEU} – одиничних помилок; λ_{MBU} – корельованих помилок; λ_{burst} – пакетних помилок; λ_{aging} – помилок через старіння; λ_{UD} – небезпечних невиявлених помилок;

2. C – діагностичне покриття, безрозмірна величина $C \in [0,1]$.

Обмеження застосування: передбачає незалежність механізмів; не враховує складні взаємодії між видами відмов; потребує точного оцінювання параметрів. Модель дозволяє оцінити залишковий ризик та ефективність механізмів захисту, що є ключовим для систем із вимогами функціональної безпеки.

Поєднання трьох моделей: базової моделі SEU, ключової для сучасних технологій моделі корельованих багатобітових помилок та критичної для комунікацій моделі пакетних помилок забезпечує більш адекватний опис реальних умов функціонування пам’яті в КФС. Найбільш критичним фактором є кореляція помилок, яка істотно знижує ефективність традиційних методів захисту. Це обґрунтовує необхідність переходу до багаторівневих підходів забезпечення надійності, що поєднують апаратні та програмні механізми.

3.5. Поширення помилок та підсилення відмов

Апаратні відмови у КФС рідко залишаються локальними, і, на відміну від класичних обчислювальних систем, вони мають здатність поширюватися через ПЗ та фізичні процеси, формуючи складні багаторівневі ланцюги відмов, як це описано авторами у [2, 3, 11]. Особливо небезпечні ситуації, коли первинна помилка не призводить до негайної відмови, а трансформується у приховане спотворення стану, яке підсилюється алгоритмічно та фізично.

3.5.1. Механізми підсилення помилок

ПЗ відіграє ключову роль у трансформації локальних апаратних збоїв у системні відмови, тому розглянемо основні механізми підсилення помилок:

1. Ітеративні алгоритми (накопичення помилок): у багатьох КФС використовуються рекурсивні або ітеративні алгоритми (фільтрація, оцінювання стану, інтегрування). Якщо помилка потрапляє у внутрішній стан, вона накопичується з часом, наприклад:

$$x_{k+1} = \alpha\, x_k + \beta\, y_k.$$

Якщо значення x_k спотворене, то похибка переходить у x_{k+1}, накопичується експоненційно при $\alpha \approx 1$ і може призвести до розходження алгоритму. Тому навіть одинична помилка може породити довготривалу динамічну деградацію.

2. Зворотні зв’язки: КФС характеризуються наявністю замкнених контурів керування. Помилка в обчисленні керуючого сигналу: впливає на фізичний процес,змінює сенсорні вимірювання, повторно потрапляє в алгоритм. Це створює позитивний зворотний зв’язок помилки, що може: дестабілізувати

систему, викликати автоколивання, спричинити аварійний режим.

3. Повторне використання стану: у КФС стан зберігається у пам’яті та використовується повторно, тому пошкодження таблиць калібрування, параметрів регуляторів, накопичених оцінок призводить до довготривалого спотворення поведінки, латентних відмов та активації помилки лише за певних умов.

4. Розподілені обчислення: у мережевих КФС вузли обмінюються станами, синхронізують дані, виконують колективні алгоритми. Тому помилка в одному вузлі може реплікуватися через мережу, впливати на інші вузли та призводити до системної неузгодженості, як показано у [14, 15].

3.5.2. Ланцюг поширення відмов

Поширення помилки у КФС відповідає ланцюгу: пошкодження пам’яті → некоректне обчислювальне рішення → некоректні дані для виконавчого механізму → зміна фізичного стану КФС → спотворення сенсорних даних → зворотне потрапляння помилки у програму, що є фундаментальною відмінністю КФС від традиційних IT-систем, як показано у роботах [2, 3].

3.5.3. Ймовірність небезпечної події

Не кожна апаратна помилка призводить до аварії. Для виникнення небезпечної ситуації необхідні дві умови: виникнення помилки та її активація в критичному контексті.

Формально: $P_{hazard} = P_{fault} \cdot P_{activation}$, де P_{hazard} – ймовірність невиявленого некоректного стану КФС, P_{fault} – ймовірність виникнення помилки, $P_{activation}$ – ймовірність того, що помилка вплине на критичний фрагмент системи. Тому навіть часті помилки можуть бути безпечними, якщо не активуються, але рідкісні помилки можуть бути критичними при високому $P_{activation}$.

3.5.4. Формальна модель системної відмови

Для кількісного аналізування вводиться модель інтенсивності системних відмов: $\lambda_{system} = \lambda_H \cdot P_{prop} \cdot P_{fail}$ де: P_{prop} − поширення, P_{fail} − перехід у відмову, λ_H – інтенсивність апаратних відмов [1/год].

Фізичний зміст параметрів λ_H визначається технологією (радіація, старіння, температура); P_{prop} залежить від: ECC, перевірок узгодженості, моніторингу потоку керування; P_{fail} визначається архітектурою керування, наявністю безпечних режимів (fail-safe) та динамікою фізичного процесу.

Механізми захисту можуть діяти на двох рівнях: зменшення P_{prop}: ECC, CRC, runtime-перевірки; зменшення P_{fail}: безпечне керування, обмеження сигналів, аварійні режими. Це дає можливість архітектурної оптимізації надійності.

Поширення помилок у КФС є динамічним процесом, а не статичною подією. ПЗ може виступати як: фільтр помилок або їхній підсилювач. Найбільш небезпечними є: SDC, латентні помилки та корельовані відмови. Класичні моделі надійності (без урахування динаміки) є недостатніми, тому потрібні багаторівневі моделі відмов, що охоплюють апаратуру, програмний код та фізичні процеси, якими керує КФС

4. Наукова новизна отриманих результатів

На основі аналізу літератури [1-32] встановлено обмеження існуючих підходів, пов’язані з роздільним розглядом апаратних і програмних відмов та припущенням незалежності помилок. У роботі сформульовано такі наукові результати:

1. Вперше запропоновано узагальнену ймовірнісну модель відмов пам’яті КФС, що враховує помилки пам’яті та ефекти старіння, включаючи просторово-часову кореляцію, критичну для сучасних технологій.

2. Розвинено підхід до аналізу надійності шляхом формалізації поширення відмов через ПЗ і фізичні процеси: $\lambda_{system} = \lambda_H \; P_{prop} \; P_{fail}$, що дозволяє кількісно оцінювати внесок різних рівнів системи.

3. Вперше формалізовано механізми підсилення помилок у КФС, зумовлені ітеративними алгоритмами, зворотними зв’язками та збереженням стану, показано можливість довготривалих відхилень від одиничних збоїв.

4. Удосконалено модель оцінювання небезпечних станів: $P_{hazard} = P_{fault} \; P_{activation}$, що враховує латентні помилки.

5. Доведено обмеженість класичних методів і засобів контролю цілісності при багатобітових та пакетних помилках і необхідність врахування їх кореляції.

Таким чином, у роботі вперше запропоновано узагальнену модель апаратно-обумовлених відмов у КФС, яка враховує корельовані помилки пам’яті, механізми їх поширення через ПЗ та підсилення у контурах керування, а також реалізована у вигляді SiL-орієнтованого підходу для експериментального дослідження.

Висновки

У роботі проаналізовано надійність КФС з урахуванням апаратних відмов і їх поширення через ПЗ та фізичні процеси. Встановлено, що надійність має системний характер, а пам’ять є критичним елементом. Показано домінування багатобітових помилок і нелінійні ефекти їх поширення через ПЗ. Запропоновані ймовірнісні моделі забезпечують формалізацію аналізу, при цьому кореляція помилок є ключовим фактором. Обґрунтовано ефективність багаторівневих підходів та недостатність традиційних методів і засобів захисту пам’яті без перестановки бітів. Отримані результати можуть бути використані для підвищення надійності КФС на етапах проєктування, тестування та експлуатації, а також для забезпечення вимог функціональної безпеки.

Перспективи подальших досліджень

Подальші дослідження спрямовані на розроблення адаптивних ECC для корельованих помилок, інтеграцію моделей відмов у SiL, створення runtime-моніторингу SDC та застосування формальних методів аналізу. Важливими є також дослідження відповідності ISO 26262 і DO-178C, розвиток cross-layer підходів і використання ML для прогнозування відмов. Ці напрями формують основу для адаптивних і самодіагностичних КФС.

References

1. Lee E. A. Cyber-Physical Systems - Are Computing Foundations Adequate?: Position Paper for NSF Workshop On Cyber-Physical Systems: Research

Motivation, Techniques and Roadmap (October 16-17, 2006, Austin, TX) / Edward A. Lee; Department of EECS, UC Berkeley. – Berkeley: University of California, 2006. – 9 p.

2. Rajkumar R. R. Cyber-Physical Systems: The Next Computing Revolution / R. R. Rajkumar, I. Lee, L. Sha, J. Stankovic // Proceedings of the 47th Design Automation Conference (DAC 2010), Anaheim, California, USA, July 13-18, 2010. – 2010. – P. 731–736. – DOI: 10.1145/1837274.1837461.

3. Alur R. Principles of cyber-physical systems / R. Alur. – Cambridge : MIT Press, 2015. – 450 p. DOI: 10.1145/1837274.1837461.

4. Buttazzo G. Hard real-time computing systems: predictable scheduling algorithms and applications / G. Buttazzo. – 3rd ed. – Springer, 2011. – 514 p. – DOI: 10.1007/978-1-4614-0676-1.

5. Kopetz H. Real-time systems: design principles for distributed embedded applications / H. Kopetz. – 2nd ed. – Springer, 2011. – 396 p. DOI: 10.1007/978-1-4419-8237-7.

6. Burns A. Real-time systems and programming languages / A. Burns, A. Wellings. – 4th ed. – Addison-Wesley, 2009. – 528 p. DOI: 10.1007/978-1-4419-8237-7.

7. Patterson D. Computer organization and Design MIPS Edition / D. Patterson, J. Hennessy. – 6th ed. – Morgan Kaufmann, 2020. – 832 p.

8. Baumann R. C. Soft errors in advanced semiconductor devices-Part I: The three radiation sources / R. C. Baumann // IEEE Transactions on Device and Materials Reliability. – 2001. – Vol. 1, No. 3. – P. 17–22. DOI: 10.1109/7298.946464.

9. Dodd P. E. Basic mechanisms and modeling of single-event upset / P. E. Dodd, L. W. Massengill // IEEE Transactions on Nuclear Science. – 2003. – Vol. 50. – P. 583–602. DOI: 10.1109/TNS.2003.813197.

10. Ziegler J. F. Effect of cosmic rays on computer memories / J. F. Ziegler, W. A. Lanford // Science. – 1979. – Vol. 206. – P. 776–788. DOI: 10.1126/science.206.4420.776.

11. Schroeder B. DRAM errors in the wild / B. Schroeder, E. Pinheiro, W.-D. Weber // Communications of the ACM. – 2011. – Vol. 54. – P. 100–107. DOI: 10.1145/1953122.1953140.

12. Sridharan V. Memory errors in modern systems / V. Sridharan [et al.] // SIGMETRICS. – 2015. DOI: https://doi.org/10.1145/2745844.2745863.

13. Mukherjee S. S. Architecture design for soft errors / S. S. Mukherjee. – Morgan Kaufmann, 2008. – 536 p.

14. Hespanha J. P. A survey of recent results in networked control systems / J. P. Hespanha, P. Naghshtabrizi, Y. Xu // Proceedings of the IEEE. – 2007. – Vol. 95. – P. 138–162. – DOI: 10.1109/JPROC.2006.887288.

15. Zhang W. Stability of networked control systems / W. Zhang, M. Branicky, S. Phillips // IEEE Control Systems Magazine. – 2001. – Vol. 21. – P. 84–99. – DOI: 10.1109/37.898794.

16. Silent Data Corruptions: The Stealthy Saboteurs of Digital Integrity / G. Papadimitriou, D. Gizopoulos, H. D. Dixit, S. Sankar // 2023 IEEE 29th International Symposium on On-Line Testing and Robust System Design (IOLTS). – 2023. – DOI: 10.1109/IOLTS59296.2023.10224870.

17. Silent Data Corruption: Advancing Detection, Diagnosis, and Mitigation Strategies / P. Domanski [et al.] // IEEE Xplore. – 2024. DOI: 10.1109/IOLTS60522.2024.10623345.

18. Alur R. Formal verification of hybrid systems / R. Alur // Proceedings of EMSOFT. – 2011. – P. 273–278. DOI: 10.1145/2038642.2038684.

19. Derler P. Modeling cyber-physical systems / P. Derler, E. A. Lee, A. S. Vincentelli // Proceedings of the IEEE. – 2012. DOI: 10.1109/JPROC.2011.2165279.

20. Multi-Bit Upsets Vulnerability Analysis of Modern Microprocessors / A. Chatzidimitriou [et al.] // IEEE International Symposium on Workload Characterization (IISWC). – Orlando, 2019. – DOI: 10.1109/IISWC47752.2019.9042036.

21. Overview on Radiation Damage Effects and Protection Techniques in Microelectronic Devices / Y. Ren [et al.] // Journal of Sensors. – 2024. – DOI: 10.1155/2024/3616902.

22. Hamming R. W. Error detecting and error correcting codes / R. W. Hamming // Bell System Technical Journal. – 1950. – Vol. 29. – P. 147–160. – DOI: 10.1002/j.1538-7305.1950.tb00463.x.

23. Peterson W. Error-correcting codes / W. Peterson, E. Weldon. – 2nd ed. – MIT Press, 1972. – 560 p.

24. Richardson T. Modern coding theory / T. Richardson, R. Urbanke. – Cambridge University Press, 2008. – 520 p.

25. Marinella M. J. Radiation Effects in Advanced and Emerging Nonvolatile Memories / M. J. Marinella // IEEE. – 2021. DOI: 10.1109/TDMR.2021.3071234.

26. Krichen M. Formal Methods for Cyber-Physical Systems / M. Krichen // Reliability in Cyber-Physical Systems: The Human Factor Perspective. – Springer, 2026. – DOI: 10.1007/978-3-032-09917-4_18.

27. Rehman S. Reliable software for unreliable hardware / S. Rehman, M. Shafique, J. Henkel // IEEE Design & Test. – 2016. – Vol. 33. – P. 16–25. DOI: 10.1109/MDAT.2016.2515625.

28. Rehman S. Architectural-space exploration of approximate multipliers / S. Rehman, W. El-Harouni, M. Shafique // Proceedings of the 35th International Conference. – 2016. – DOI: 10.1145/2966986.2967005.

29. Koren I. Software Fault Tolerance / I. Koren, C. M. Krishna // Fault-Tolerant Systems. – 2021. – DOI: 10.1016/B978-0-12-818105-8.00015-2.

30. Kafle P. Reliability Analysis Techniques in Distribution System: A Comprehensive Review / P. Kafle, M. Bhandari, L. Rana // International Journal of Engineering and Manufacturing. – 2022. – Vol. 12, No. 2. – P. 11–24. – DOI: 10.5815/ijem.2022.02.02.

31. Rehman S. Cross-Layer Reliability Analysis, Modeling, and Optimization / S. Rehman, M. Shafique, J. Henkel // Reliable Software for Unreliable Hardware. – 2016. – DOI: 10.1007/978-3-319-25772-3_3.

32. Zhang D. Exploring and Optimizing Chipkill-Correct for Persistent Memory Based on High-Density NVRAMs / D. Zhang, V. Sridharan, X. Jian // 2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). – 2018. – DOI: 10.1109/MICRO.2018.00063.

Надійшла до редакції 9.04.2026, розглянута на редколегії 20.04.2026

ISSN 2071-1077(print)
ISSN 2663-2411(online

Probabilistic Models of Hardre Reliability and Data Integrity in Cyber-Physical Systems

The article investigates the reliability of cyber-physical systems (CPS), focusing on hardware failures and their propagation into software and physical processes. The main sources of failures in computation, memory, communication, power supply, and sensing subsystems are analyzed, accounting for the influence of external factors such as radiation, electromagnetic interference, and thermal stress. The mechanisms of single-event upsets (SEU), multi-bit upsets (MBU), and burst errors are examined. The study analyzes error-amplification mechanisms in software algorithms and feedback loops. Formal dependencies for estimating the rate of dangerous undetected failures are introduced. It is shown that memory and data transmission subsystems are critical to ensuring CPS reliability, and that integrated hardware-software protection methods are essential for functional safety. Probabilistic memory failure models are proposed that account for both independent and correlated errors, as well as aging effects. Formal dependencies for evaluating the intensity of dangerous undetected failures, taking diagnostic coverage into account, are established. Special attention is paid to the mechanisms of error propagation and amplification through software implementations of algorithms, feedback loops, and state retention, which are characteristic features of cyber-physical systems. The necessity of applying integrated hardware-software protection methods and utilizing simulation to improve reliability and ensure the functional safety of cyber-physical systems is substantiated.

Keywords: cyber-physical systems; reliability; memory; failures; functional safety.

Відомості про авторів:

Манжос Юрій Семенович – канд. техн. наук, доц., доц. каф. інженерії програмного забезпечення, Національний аерокосмічний університет «Харківський авіаційний інститут», м. Харків, Україна, email: y.manzhos@khai.edu, ORCID: 0000-0002-4910-7285.

Соколова Євгенія Віталіївна – канд. техн. наук, доц., доц. каф. інженерії програмного забезпечення, Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна, e-mail: y.sokolova@khai.edu, ORCID: 0000-0002-1497-4987.

About the authors:

Yuriy MANZHOS – Ph.D. in Information Technologies, Associate Professor at the Department of Software Engineering and Business, National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, Ukraine, e-mail: y.manzhos@khai.edu, ORCID: 0000-0002-4910-7285.

Yevheniia SOKOLOVA – Ph.D. in Information Technologies, Associate Professor at the Department of Software Engineering and Business, National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, Ukraine, e-mail: y.sokolova@khai.edu, ORCID: 0000-0002-1497-4987.