ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 5 (1), 2025

ВИЗНАЧЕННЯ ПОКАЗНИКІВ БЕЗПЕЧНОСТІ ВІДМОВОСТІЙКОЇ СИСТЕМИ ВІДПОВІДАЛЬНОГО ПРИЗНАЧЕННЯ БЕЗ ВІДНОВЛЕННЯ МЕТОДОМ ПРОСТОРУ СТАНІВ

Л. Озірковський [ORCID: 0000-0003-0012-2908], Б. Волочій [ORCID: 0000-0001-5230-9921], Б. Гусяк, М. Змисний[ORCID: 0000-0002-3384-6139]

[1]Національний університет «Львівська політехніка», вул. С. Бандери, 12, м. Львів, 79013, Україна

Corresponding author: Леонід Озірковський (e-mail: leonid.d.ozirkovskyi@ lpnu.ua).

(Отримано 1 квітня 2025)

Системи відповідального призначення (англ. – Safety Critical System – SCS) відіграють ключову роль у критичних сферах діяльності, де необхідна висока безпечність, надійність і безперервність роботи. До таких систем належать військові, космічні, енергетичні, авіаційні, медичні та транспортні комплекси, що функціонують в екстремальних умовах і мають виконувати свої функції незалежно від зовнішніх та внутрішніх впливів. Основними характеристиками таких систем є здатність виконувати свої функції при втраті працездатності їх підсистем чи модулів, можливість адаптації до змінних умов експлуатації та високий рівень захисту від зовнішніх загроз. Об'єктом дослідження, в даній роботі, є відмовостійка система відповідального призначення з мажоритарною структурою. Така система складається з непарної кількості однотипних модулів та мажоритарного елемента. Предметом дослідження є показники безпечності відмовостійкої системи відповідального призначення. В статті представлено методику визначення показників безпечності системи відповідального призначення методом простору стану. Цей метод, на відміну від методів дерев відмов, динамічних дерев відмов, дерев подій та FMEA/FMECA-аналізу, дає змогу враховувати вплив алгоритму поведінки відмовостійкої системи на виникнення аварійних ситуацій і в результаті цього отримувати достовірні кількісні значення показників безпечності. Особливістю методу простору станів є те, що показники безпечності та показники надійності визначаються з єдиної моделі. Це дає змогу встановити вплив конфігурації структури відмовостійкої системи та алгоритму надійнісної поведінки на показники її безпечності, що є неможливим при використанні інших методів аналізу безпечності. Методика проілюстрована на конкретному прикладі системи відповідального призначеннння. Для валідації результатів дослідження використано метод аналізу дерев відмов. Розроблена методика формування показників безпечності з підпростору непрацездатних станів дає змогу отримати функції аварійності вімовостійких систем, які є часовими залежностями ймовірності появи мінімальних січень. Функції аварійності, на відміну від мінімальних січень, дають змогу врахувати вплив на показники безпечності особливості алгоритму поведінки відмовостійкої системи при порушеннях працездатності.

Ключові слова: *безпечність, показники безпечності, система відповідального призначення, відмовостійка система, метод простору станів, дерево відмов*
УДК: 629.039.58, 621.396.9

Вступ

Важливою задачею, на системотехнічному етапі проектування систем відповідального призначення, є забезпечення заданого рівня надійності та безпечності [1]. Надійність забезпечується надлишковим ресурсом в структурі та в алгоритмі поведінки системи, а безпечність

– додатковими спеціальними засобами, що вводяться в структуру системи. Особливістю системи відповідального призначення є те, що вихід її з ладу призводить до аварійної ситуації [2].

Для оцінювання ефективності введеної надлишковості та засобів забезпечення безпечності, коли ще системи немає в «залізі», використовують цілу низку методів [3]. Для оцінки показників безпечності найчастіше використовують методи аналізу дерев відмов (FTA), динамічних дерев відмов (DFTA) та дерев подій (ETA), а також FMEA/FMECA-аналіз [4, 5]. Для оцінки показників надійності – метод структурних схем надійності (RBD), метод простору станів та дерева відмов [6]. Основними обмеженнями цих методів є те, що для оцінювання показників надійності та показників безпечності використовуються різні моделі, які не дають змоги побачити як зміни надлишкового ресурсу у відмовостійкій структурі впливають на безпечність і як додаткові засоби для підвищення безпечності впливають на надійність. Для усунення цих обмежень доцільно застосувати удосконалений метод простору станів [7], який містить як повний підпростір працездатних станів, так і повний підпростір непрацездатних станів. Метод простору станів передбачає подання поведінки системи у вигляді сукупності можливих станів, між якими відбуваються переходи з певними інтенсивностями. Він дозволяє враховувати часову динаміку зміни станів у системі в процесі виходу з ладу окремих її підсистем та модулів та враховувати поведінку системи при різних сценаріях аварійних ситуацій при кількісній оцінці як показників надійності, так і безпечності. Зокрема, для систем відповідального призначення, цей метод дає змогу визначити ймовірність перебування системи в певному стані та оцінити середній час перебування її в цьому стані. Тому, удосконалений метод простору станів [7] дає змогу з єдиної моделі визначити як показники надійності – ймовірність безвідмовної роботи – R(t)), середній час роботи до відмови – MTTF, так і показники безпечності – ймовірність настання аварійної ситуації – Q(t), частоту потрапляння в аварійну ситуацію – w(t) та функції аварійності – FA(t), які є аналогами мінімальних січень – MCS, що визначаються методом аналізу дерев відмов.

Таким чином, використання удосконаленого методу простору станів підвищить достовірність отриманих показників безпечності з урахуванням надійнісної поведінки системи, що дасть змогу правильно оцінити ризики її експлуатації ще на системотехнічному етапі проектування та передбачити заходи для мінімізації цих ризиків. А це знизить ймовірність виникнення аварійних ситуацій, які спричиняються відмовами підсистем чи окремих модулів системи відповідального призначення.

2. Постановка задачі

Ефективним підходом до підвищення надійності та безпечності систем відповідального призначення є використання відмовостійких систем з мажоритарною структурою. Вони застосовуються в критичних обчислювальних та керуючих системах авіації, транспорту, енергетики [8], коли прийняття рішення базується на принципі більшості. Такий підхід підвищує, безпечність та надійність системи, оскільки дозволяє ігнорувати несправні модулі та модулі в яких стався збій.

Об'єктом дослідження, в даній роботі, є відмовостійка система відповідального призначення з мажоритарною структурою (рис.1). Така система складається з непарної кількості однотипних модулів та мажоритарного елемента [9]. Мажоритарний елемент ще називають пристроєм голосування або схемою вибору. На вхід кожного модуля приходить однакова інформація (сигнал), яка обробляється модулями і подається на мажоритарний елемент. Якщо жоден модуль не вийшов з ладу і не відбулося жодного збою, то на вхід мажоритарного елемента приходить однакова оброблена інформація (сигнал). Мажоритарний елемент здійснює порівняння інформації і видає на вихід інформацію, якої є більшість. Тобто, для правильної роботи системи на виході мінімум двох модулів має бути однакова інформація (сигнал). Тому, така структура відмовостійкої системи називається мажоритарною структурою 2 з 3-х з фіксованим правилом голосування. Ремонту чи

заміни модулів, які вийшли з ладу не передбачено, тому така вімовостійка система є без відновлення.

Таким чином, дана відмовостійка система відповідального призначення може виконувати свою функцію при виході з ладу 1-го модуля. Також, така система є працездатною у випадку збою в одному з модулів. Тому, системи відповідального призначення з мажоритарною структурою мають апаратний захист від збоїв, що суттєво підвищує рівень їх безпечності без застосування додаткових засобів.

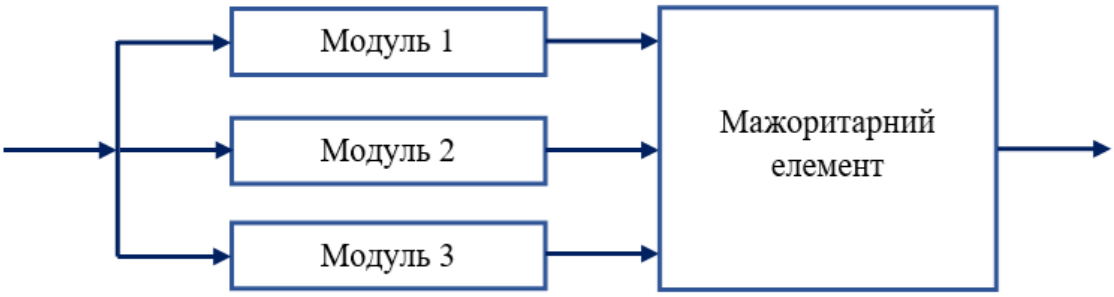

Рис.1.Структурна схема відмовостійкої системи відповідального призначення з мажоритарною структурою

Предметом дослідження є показники безпечності відмовостійкої системи спеціального призначення. Такими показниками є:

- Мінімальні січення (MCS) – комбінації відмов мінімальної кількості підсистем чи модулів, які призводять до катастрофічної відмови. Кількісно мінімальні січення оцінюються ймовірністю появи мінімального січення.
- Ймовірність настання аварійної (Q) – це ймовірність того, що в результаті відмов складових системи наступлять одна чи декілька катастрофічних відмов сукупність яких призводить до аварійної ситуації. Кількісно ймовірність настання аварійної ситуації визначається як сума (логічна) мінімальних січень.
- Частота потрапляння в аварійну ситуацію (w) – добуток ймовірності перебування системи в працездатному стані на інтенсивність переходу системи з працездатного стану в стан аварійної ситуації. Цей показник характеризує швидкість потрапляння в аварійну ситуацію і часовий проміжок за який система туди потрапить. Кількісно оцінюється ймовірністю потрапляння в аварійну ситуацію.

Всі ці показники безпечності визначаються шляхом аналізу дерева відмов в конкретний момент часу експлуатації системи і є точковою оцінкою безпечності. Крім цього, вони не враховують надійнісної поведінки системи. Однак, на системотехнічному етапі проектування систем відповідального призначення потрібно мати не точкові оцінки, а часові залежності показників безпечності, які б давали змогу оцінити тенденцію їх зміни при введенні додаткових надлишкових засобів для підвищення відмовостійкості, а саме – резервних модулів, більш надійних основних модулів, технічне обслуговування та ремонт, зміну правила голосування тощо. Тому, для визначення показників безпечності потрібно застосувати удосконалений метод простору станів, який дає змогу отримати часові характеристики на весь період експлуатації системи спеціального призначення. На основі такого методу потрібно сформувати методику визначення показників безпечності відмовостійкої системи відповідального призначення з мажоритарною структурою.

3. Побудова аналітичної моделі для визначення часових характеристик показників безпечності системи спеціального призначення

Для побудови аналітичної моделі відмовостійкої системи відповідального призначення з мажоритарною структурою без відновлення застосовано удосконалений метод простору станів [7].

Побудова моделі, згідно цього методу, передбачає формування вербальної моделі. На основі вербальної моделі шляхом логічного аналізу будується граф станів та переходів. На відміну від традиційного методу простору станів, в даному методі стани відмови не об'єднують в один, а утворюють повний підпростір непрацездатних станів. Крім цього, для кожного модуля потрібно використовувати окрему компоненту вектора станів, щоб в кожному стані, в кожен момент часу мати повну інформацію про працездатність складових системи. Такий підхід суттєво розширює підпростір працездатних станів.

Граф станів і переходів для досліджуваної системи представлено на рис. 2. Вектор станів складається з трьох компонент – V1, V2, V3, кожна з яких однозначно ідентифікує стан кожного модуля. Якщо компонента має значення 1, то модуль є справний, якщо – 0, то модуль є непрацездатним. Система є справною, якщо будь які два з 3-х модулів є працездатними. В нашому випадку стани 1, 2, 3 та 4 є працездатними, а стани 5, 6, 7 та 8 – непрацездатними. Інтенсивності переходів (λ1, λ2, λ3) із стану в стан, в даному випадку, є інтенсивностями відмов відповідних модулів.

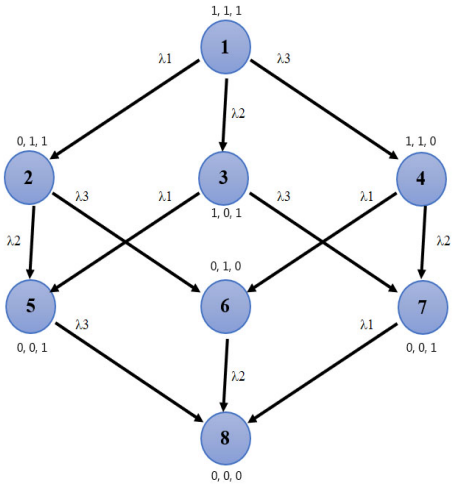

Рис. 2. Граф станів і переходів відмовостійкої системи відповідального призначення з мажоритарною структурою

На основі побудованого графу станів і переходів формується система лінійних диференційних рівнянь Колмогорова-Чепмена з постійними коефіцієнтами. Кількість рівнянь відповідає кількості станів. Кожне з рівнянь формується за таким правилом: в лівій частині записується похідна по часу від ймовірності перебування і-му стані, в правій частині алгебраїчна сума добутків інтенсивностей, що виходять з і-го стану зі знаком мінус помножена на ймовірність перебування в і-му стані та інтенсивностей, що входять в і-й стан зі знаком плюс з інших станів помножені на ймовірності перебування в цих станах. Отримана система рівнянь для графу станів та переходів (рис.2) представлена нижче.

Система рівнянь (1) є аналітичною моделлю надійнісної поведінки відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х без відновлення. Розв'язок системи рівнянь (1) здійснено методом Рунге-Кутти-Мерсона з адаптивним кроком і отримано розподіл ймовірностей *(P1(t), P2(t), P3(t), P4(t), P5(t), P6(t), P7(t), P8(t))* перебування системи в кожному з станів. З цих ймовірностей можна сформувати вирази для обчислення показників безпечності та показників надійності.

$$\frac{dP1(t)}{dt} = -(\lambda 1 + \lambda 2 + \lambda 3) \cdot P1(t)$$

$$\frac{dP2(t)}{dt} = \lambda 1 \cdot P1(t) - (\lambda 2 + \lambda 3) \cdot P2(t)$$

$$\frac{dP3(t)}{dt} = \lambda 1 \cdot P1(t) - (\lambda 1 + \lambda 3) \cdot P3(t)$$
$$\frac{dP4(t)}{dt} = \lambda 1 \cdot P1(t) - (\lambda 1 + \lambda 2) \cdot P42(t) \quad (1)$$
$$\frac{dP5(t)}{dt} = \lambda 2 \cdot P2(t) + \lambda 1 \cdot P3(t) - \lambda 3 \cdot P5(t)$$
$$\frac{dP6(t)}{dt} = \lambda 3 \cdot P2(t) + \lambda 1 \cdot P4(t) - \lambda 2 \cdot P6(t)$$
$$\frac{dP7(t)}{dt} = \lambda 3 \cdot P3(t) + \lambda 2 \cdot P4(t) - \lambda 1 \cdot P7(t)$$
$$\frac{dP8(t)}{dt} = \lambda 3 \cdot P5(t) + \lambda 2 \cdot P6(t) + \lambda 1 \cdot P7(t)$$

Показники надійності формуються з ймовірностей перебування системи в працездатних станах – *P1(t), P2(t), P3(t), P4(t)*, а показники безпечності – з ймовірностей перебування системи в непрацездатних станах – *P5(t), P6(t), P7(t), P8(t)*.

4. Методика формування показників безпечності з підпростору непрацездатних станів

Методику формування показників безпечності з підпростору непрацездатних станів розроблено на базі підходу, представленого в [7]. В результаті застосування даної методики проектант отримує функції аварійності, які є аналогами мінімальних січень, які отримуються методом аналізу дерев відмов. На відміну від мінімальних січень, які є точковими оцінками в конкретний момент інтервалу експлуатації системи, функції аварійності показують як змінюється мінімальне січення на усьому інтервалі експлуатації системи в залежності не тільки від показників надійності підсистем (особливостей відмовостійкої структури), але й від алгоритму поведінки системи.

Розроблена методика містить 6-ти етапів, в результаті виконання яких, проектант отримує функції аварійності з графу станів та переходів. Розроблена методика проілюстрована на прикладі відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х без відновлення.

1. ***Формування логічної умови відмови системи.*** З компонент вектора станів необхідно сформувати умову відмови відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х без відновлення. Система буде непрацездатною, якщо 2 з 3-модулів вийдуть з ладу. Таки чином, в нашому випадку, аварійна ситуація наступить в результаті настання одного з 3-х варіантів комбінацій несправних модулів: відмовили 1-й і 2-й модулі; відмовили 1-й і 3-й модулі та відмовили 2-й і 3-й модулі. Якщо модуль несправний, то відповідна компонента вектора станів дорівнює 0. Тому, умова відмови системи (логічна функція непрацездатності) буде мати вигляд:

   (V1=0 AND V2=0) OR (V1=0 AND V3=0) OR (V2=0 AND V3=0)

2. ***Мінімізація логічної функції умови відмови за правилами алгебри логіки.*** Для формування масок аварійних ситуацій логічний вираз умови відмови повинен бути представлений як диз'юнкція елементарних кон'юнкцій. Оскільки, в загальному випадку, вираз умови відмови системи містить надлишкові операнди, то його необхідно мінімізувати за правилами агебри логіки. В нашому випадку функція непрацездатності вже є диз'юнкцією елементарних кон'юнкцій, а тому додаткової мінімізації вона не потребує.

3. ***Формування масок аварійних ситуацій.*** З мінімізованої умови відмови потрібно сформувати маски аварійних ситуацій. Кількість масок дорівнює кількості елементарних кон'юнкцій. В нашому випадку є 3 елементарних кон'юнкції, тому маємо маски 3-х аварійних ситуацій:

$$(V1=0 \text{ AND } V2=0);\ (V1=0 \text{ AND } V3=0);\ (V2=0 \text{ AND } V3=0).$$

4. ***Вибір станів, з підпростору непрацездатних станів, які відповідають конкретній аварійній ситуації.*** За допомогою маски аварійної ситуації вибирають стани в яких відповідні компоненти вектора станів дорівнюють нулю як і операнди елементарних кон'юнкцій в масці аварійної ситуації. До *Аварійної ситуації 1*, у відповідності до маски *(V1=0 AND V2=0)* відносяться станани 5 та 8, оскільки в цих станах 1-а і 2-а компоненти вектора станів дорівнюють нулю (рис.2). До *Аварійної ситуації 2*, у відповідності до маски *(V1=0 AND V3=0)* відносяться стани 6 та 8, оскільки в цих станах 1-а і 3-я компоненти вектора станів дорівнюють нулю (рис.2). До *Аварійної ситуації 3*, у відповідності до маски *(V2=0 AND V3=0)* відносяться стани 7 та 8, оскільки в цих станах 2-а і 3-я компоненти вектора станів дорівнюють нулю.
5. ***Формування виразів для визначення часових залежностей функцій аварійності.*** Вираз функції аварійності є сумою ймовірностей перебування у станах, які вибрані за допомогою масок аварійних ситуацій. В нашому випадку буде 3 функції аварійності: *FA1(t), FA2(t), FA3(t)*, які представлено виразами (2).

$$\begin{aligned} FA1(t) &= P5(t) + P8(t) \\ FA2(t) &= P6(t) + P8(t) \\ FA3(t) &= P7(t) + P8(t) \end{aligned} \tag{2}$$

Графіки залежностей функцій аварійності (точкові, штрихові та штрих-пунктирні лінії) від періоду експлуатації відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х представлено на рис. 3.

6. ***Формування виразу для обчислення ймовірності потрапляння системи в аварійну ситуацію.*** Ймовірність потрапляння системи в аварійну ситуацію Q(t) обчислюється як сума функцій аварійних ситуацій:

$$Q(t) = 1 - \big(1 - FA1(t)\big) * \big(1 - FA2(t)\big) * \big(1 - FA3(t)\big) \tag{3}$$

Графік залежності ймовірності потрапляння в аварійну ситуацію (суцільна крива) від періоду експлуатації відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х представлено на рис. 3.

5. Валідація отриманих результатів

Для валідації результатів дослідження використано метод аналізу дерев відмов. Для цього побудовано дерево відмов для відмовостійкої системи з мажоритарною структурою (рис.1). Для побудови дерева та розрахунку мінімальних січень використано програмне забезпечення TopEventFTA [10]. Дерево відмов представлено на рис. 4, а результати розрахунків представлено табл.1.

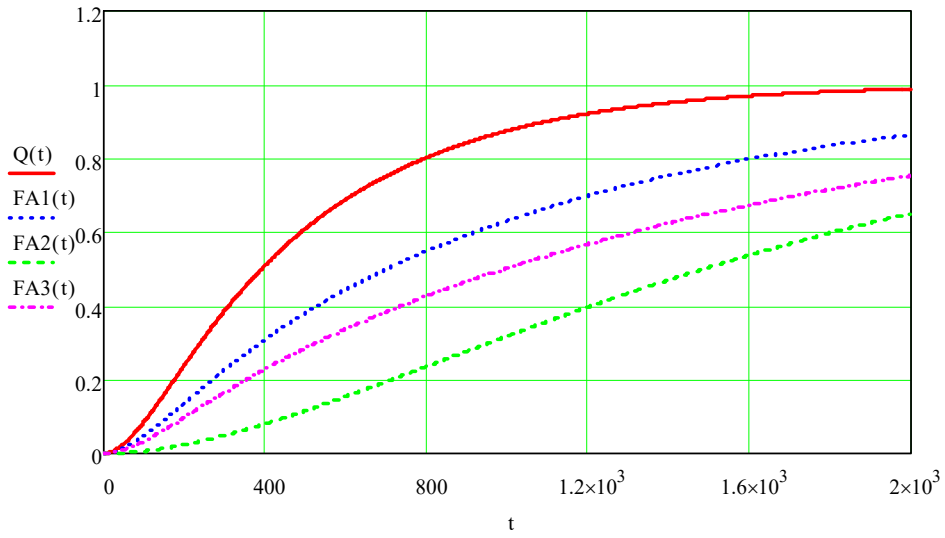

Рис. 3. Функції аварійності (FA1(t), FA2(t), FA3(t)) та ймовірність потрапляння в аварійну ситуацію (Q(t)) відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х

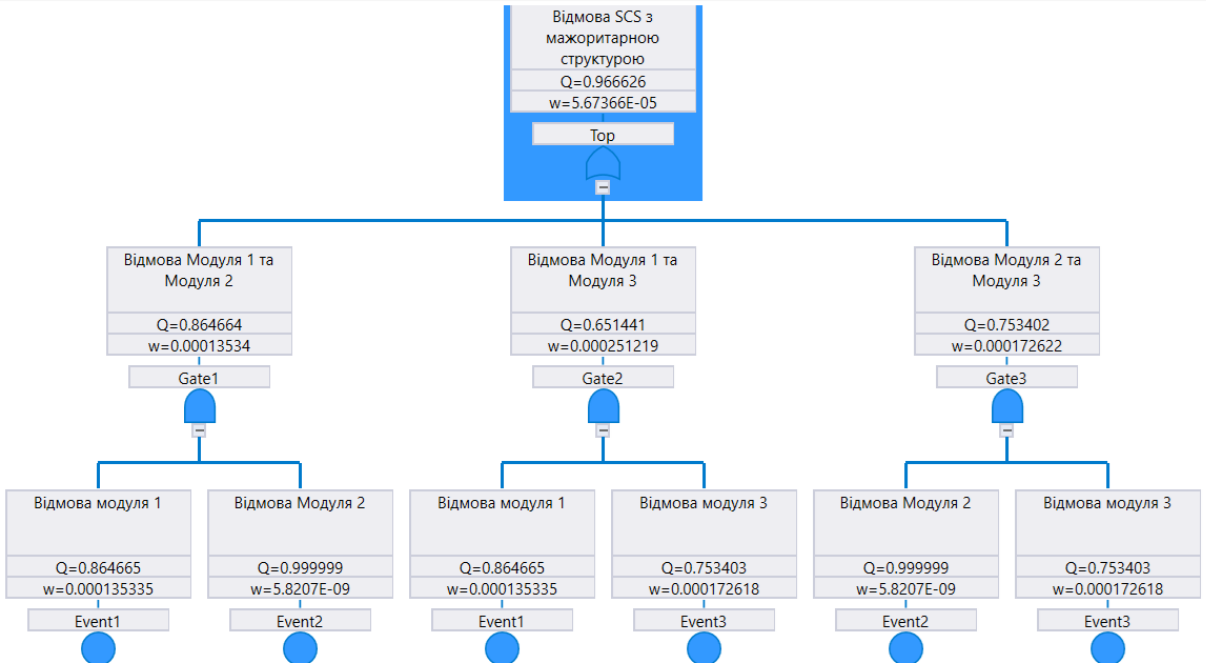

Рис. 4. Дерево відмов відмовостійкої системи відповідального призначення з мажоритарною структурою 2 з 3-х

Таблиця 1

Результати розрахунку ймовірностей існування мінімальних січень (MCS) та функцій аварійності (FTA) у визначені моменти періоду експлуатації

t, год	10	100	500	800	1000	1200	1500	1800	2000
MSC1	0,000672	0,0479062	0,381588	0,548635	0,631544	0,698649	0776848	0,834698	0,864664
FA1(t)	0,000672	0,0479062	0,381588	0,548635	0,631544	0,698649	0776848	0,834698	0,864664
MCS2	0,000069	0,0340339	0,286394	0,427205	0,502986	0,568162	0,650044	0,716344	0,753402
FA2(t)	0,000069	0,0340339	0,286394	0,427205	0,502986	0,568162	0,650044	0,716344	0,753402
MCS3	0,000471	0,00643358	0,116196	0,236423	0,318219	0,397124	0,505014	0,597935	0,651441
FA3(t)	0,000471	0,00643358	0,116196	0,236423	0,318219	0,397124	0,505014	0,597935	0,651441
Qfta	0,001204	0,0818962	0,558803	0,741464	0,816861	0,869865	0,921907	0,953119	0,986626
Q	0,001204	0,0818962	0,558803	0,741464	0,816861	0,869865	0,921907	0,953119	0,986626

З отриманих результатів видно, що значення ймовірностей появи мінімальних січень (MCS), отриманих методом аналізу дерев (FTA), та значення функцій аварійності (FA(t)), отриманих методом простору станів, співпадають в аналогічні моменти часу. Це підтверджує достовірність результатів, отриманих за допомогою запропонованої методики.

Висновки

1. На системотехніному етапі проектування відмовостійких систем відповідального призначення проектанту потрібно мати змогу отримати достовірні значення показників безпечності з урахуванням як особливостей відмовостійкої структури системи, так і з урахуванням її поведінки при порушеннях працездатності. Отримати такі показники безпечності можна шляхом використання удосконаленого методу простору станів. На основі цього методу було розроблено методику визначення показників безпечності, шляхом аналізу підпростору непрацездатних станів.

2. Розроблена методика формування показників безпечності з підпростору непрацездатних станів дає змогу отримати функції аварійності вімовостійких систем, які є часовими залежностями ймовірностей появи мінімальних січень.

3. Функції аварійності, на відміну від мінімальних січень, дають змогу врахувати вплив на показники безпечності особливості алгоритму поведінки відмовостійкої системи при порушеннях працездатності.

4. Валідація результатів, отриманих за допомогою запропонованої методики, підтверджує їх достовірність.

Список використаних літературних джерел

[1]. Karmakar, G., Wakankar, A., Kabra, A., Pandya, P. (2023), Development of Safety-Critical Systems, Springer pulished, https://doi.org/10.1007/97

[2]. Knight, J.C. (2002) "Safety critical systems: challenges and directions", ICSE '02: Proceedings of the 24th International Conference on Software Engineering Pages 547 – 550, https://doi.org/10.1145/581339.581406

[3]. Maurya, A., Kumar, D. (2020) "Reliability of safety-critical systems: A state-of-the-art review", Quality and Reliablity Engineering Intetnattonal, vol. 36, pp. 2547–2568. https://doi.org/10.1002/qre.2715

[4]. Zhang, M., Cui, C., Liu, S., and Yi, X. (2021) "Reliability technology using FTA, FMECA, FHA and FRACAS: A review," IEEE International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC), Weihai, China, 2021, pp. 282-291, doi: 10.1109/SDPC52933.2021.9563512.

[5]. Baklouti, N. Nguyen, F. Mhenni, J. -Y. Choley and A. Mlika, (2020) "Dynamic Fault Tree Generation for Safety-Critical Systems Within a Systems Engineering Approach," in IEEE Systems Journal, vol. 14, no. 1, pp. 1512-1522, March 2020, doi: 10.1109/JSYST.2019.2930184.

[6]. Nand Kumar Jyotish, Lalit Kumar Singh, Chiranjeev Kumar, (2023) "Reliability Assessment of Safety-Critical Systems of Nuclear Power Plant using Ordinary Differential Equations and Reachability Graph", Nuclear Engineering and Design,Volume 412, 2023, 112469, https://doi.org/10.1016/j.nucengdes.2023.112469.

[7]. Ozirkovskyy, L., Volochiy, B., Shkiliuk, O., Zmysnyi, M., & Kazan, P. (2022). "Functional safety analysis of safety-critical system using state transition diagram", Radioelectronic and Computer Systems, 0(2), 145-158. doi:https://doi.org/10.32620/reks.2022.2.12

[8]. Ruchkov, E., Kharchenko, V., Kovalenko, A., Babeshko, I., & Poroshenko, A. (2020) "Reliability assessment of 2oo3 and 1oo2 redundant structures taking into account the means of information processing and communications. Advanced Information Systems", 4(4), 77–83. https://doi.org/10.20998/2522-9052.2020.4.11

[9]. Summatta, C., Khamsen, W., Pilikeaw, A., and Deeon, S. (2016) "Design and analysis of 2-out-of-3 voters sensing in electrical power drive system", 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 2016, pp. 1-4, doi: 10.1109/ECTICon.2016.7561336.

[10]. TopEvent FTA - Fault Tree Analysis Software [https://www.fault-tree-analysis.com]

DEFINING THE SAFETY INDICATORS OF A UNRECOVERY FAULT-TOLERANT SAFETY CRITICAL SYSTEM BY THE STATE SPACE METHOD

Leonid Ozirkovskyy, BohdanVolochiy, Bohdan Husiak, Mykhailo Zmysnyi

Lviv Polytechnic National University, 12 S. Bandera St., Lviv, 79013, Ukraine

Safety Critical Systems (SCS) play a key role in critical areas of activity where high safety, reliability and continuity of operations are required. Such systems include military, space, energy, aviation, medical and transportation complexes that operate in extreme conditions and must perform their functions regardless of external and internal influences. The main characteristics of such systems are the ability to perform their functions in case of loss of operability of their subsystems or modules, the ability to adapt to changing operating conditions and a high level of protection against external threats. The object of study in this paper is a unrecovery fault-tolerant safety critical system with a majority structure. Such a system consists of an odd number of modules of the same type and a majority element (vote system). The subject of the study is the safety indicators of a fault-tolerant system of responsible assignment. The article presents a methodology for determining the safety indicators of a safety critical system using the state space method. This method, in contrast to the methods of fault trees, dynamic fault trees, event trees, and FMEA/FMECA analysis, allows taking into account the influence of the fault-tolerant system behavior algorithm on the occurrence of emergencies and, as a result, obtaining reliable quantitative values of safety indicators. The peculiarity of the state space method is that safety and reliability indicators are determined from a single model. This makes it possible to determine the impact of the configuration of the structure of a fault-tolerant system on its safety indicators, which is impossible when using other methods of safety analysis. The methodology is illustrated on a specific example of a unrecovery fault-tolerant safety critical system. The method of fault tree analysis is used to validate the results of the study. The developed methodology for generating safety indicators from the subspace of inoperable states makes it possible to obtain accident functions of vibration-resistant systems, which are time dependencies of the probability of occurrence of minimum severity. In contrast to the minimum severity functions, the accident functions allow taking into account the impact on safety indicators of the peculiarities of the fault-tolerant system behavior algorithm in case of performance disruptions.

Keywords: *safety, safety indicators, safety critical system, fault-tolerant system, state space method, fault tree analysis*