KAPITEL 8 / *CHAPTER 8* [8]
FUZZY FTA - A SIMPLIFIED METHOD FAULT TREE ANALYSIS OF COMPLEX SYSTEMS

DOI: 10.30890/2709-2313.2025-41-07-014

Вступ.

У роботі представлено аналіз найбільш популярних механізмів забезпечення відмово стійкості складних систем, таких як соціо-кібер-фізичні системи (СКФС). Найбільш популярним є метод аналізу дерев відмов, які представляються у вигляді логічних схем взаємозв'язку станів компонентів структури, що аналізується. У класичному методі FTA стани компонентів описуються ймовірностями їх безвідмовної роботи. Однак в реальних системах отримати їх значення практично складно, а довідкові дані неточні або взагалі відсутні. Визначення стану системи, як правило, пов'язане з рядом складних перетворень цих ймовірностей. Тому в даній роботі пропонується спрощений і швидкий метод FTA, в якому стан компонентів описується нечіткими значеннями логічних станів 0 і 1. В логічних схемах вони представлені коефіцієнтами належності або ймовірностями станів в діапазоні (0,1]. Всі логічні елементи в F_FTA є двоканальними для обробки логічних станів та коефіцієнтів належності.

8.1. СКФС: концептуальне проектування: склад та архітектура

Концептуальне проектування охоплює ранні етапи створення систем. До них, відповідно до стандарту 34, належать стадії перед проектних досліджень, розробка ескізного проекту, технічне завдання та технічний проект. Завдання, які вирішуються на цих етапах, є надзвичайно важливими, суттєво впливаючих на ефективність систем, що проектуються. Помилки, допущені на цих етапах,

[8]***Authors:*** *Kosolapov Anatolii, Romanenko Arsenii*
Number of characters: *20436*
Author's sheets: *0,51*

пов'язані з дуже витратними роботами з їх усуненнями. У цьому випадку до них належить і оцінка відмово стійкості створюваних систем [2].

Важливість цього концептуального проектування зростає під час переходу до нових систем керування технологічними процесами, еволюція яких зображена в таблиці 1.1 [2].

Еволюція комп'ютерних систем характеризується зміною парадигм комп'ютеризації, що відображає зміни у вимогах користувачів [1]. Парадигма (від грецького "приклад, зразок, модель") являє собою комплекс базових наукових положень, концепцій і термінів, який визнається та підтримується науковою спільнотою, згуртовуючи більшість її представників [2]. Вона сприяє безперервності розвитку науки й творчого пошуку в ній [2]. Етапи розвитку парадигм комп'ютеризації наведено в таблиці 1.1.

Таблиця 1.1 - Етапи розвитку парадигм комп'ютеризації *(джерело [1])*

ЕТАПИ РОЗВИТКУ ПАРАДИГМ КОМП'ЮТЕРИЗАЦІЇ				
Обчислювальні системи (ОС)	**Інформаційні системи (ІС)**	**Інтелектуальні смстеми (ІІС)**	**Соціо-технічні системи (СТС)**	**Соціо-кібер-фізичні системи (СКФС)**
Щвидкодія	Достут до данних («тут і зараз»)	Інтелектуальний інтерфейс	Інтелектуальний інтерфейс	**Смарт-системи** (підприємство, дім, будівля)
Інтерфейс	Інтерфейс	Достут до данних («тут і зараз»)	Достут до данних в соц.мережах	**Інтернет-людей, Інтернет-речей, Інтернет-сервісів**
Достут до данних	Щвидкодія	Щвидкодія	Щвидкодія	**СИСТЕМИ-СИСТЕМ** («підключайся і працюй»)

Будь-яка архітектура ІС (інформаційної системи), незалежно від її парадигми, є комплексом взаємопов'язаних структур, який можна виразити наступним чином:

АІС = Мета створення системи (КТЗ, МЗ, ПЗ, ІЗ, ЛЗ, ОЗ, МетрЗ, ДЗ) [2]

В цій конструкції: КТЗ (комплекс технічних засобів) чи ТЗ (технічне забезпечення, МЗ (математичне забезпечення), ПЗ (програмне забезпечення), ІЗ (інформаційне забезпечення), ЛЗ (лінгвістичне забезпечення),ОЗ (організаційне забезпечення), МетрЗ (метрологічне забезпечення),ДЗ (документація) - комплект документів, що описують систему та всі її компоненти [2].

Соціо-кібер-фізичні системи (СКФС) представляють собою сучасний етап розвитку комп'ютерних технологій, що виник на основі соціо-технологічних систем (СТС). Вони об'єднують фізичні, цифрові та соціальні компоненти, використовуючи можливості Інтернет речей, хмарних обчислень і кібер-фізичних систем (КФС). СКФС з'явилися завдяки зростанню кількості пристроїв із вбудованими процесорами, їх інтеграції у великі мережі та потребі компенсувати обмеження людських когнітивних здібностей. Ці системи трансформують взаємодію людини з технологіями, охоплюючи такі сфери, як промисловість, транспорт, охорона здоров'я та "розумні" міста. Концептуальне проектування СКФС дозволяє систематизувати ці складні взаємозв'язки, створюючи основу для їх ефективної реалізації.

СКФС інтегрують фізичні, цифрові та соціальні компоненти в єдину функціональну структуру, яку показано на рисунку 1.1, де представлено схематичне зображення складу СКФС, який ілюструє взаємозв'язки між ключовими елементами системи, що забезпечують ефективну роботу в реальному часі.

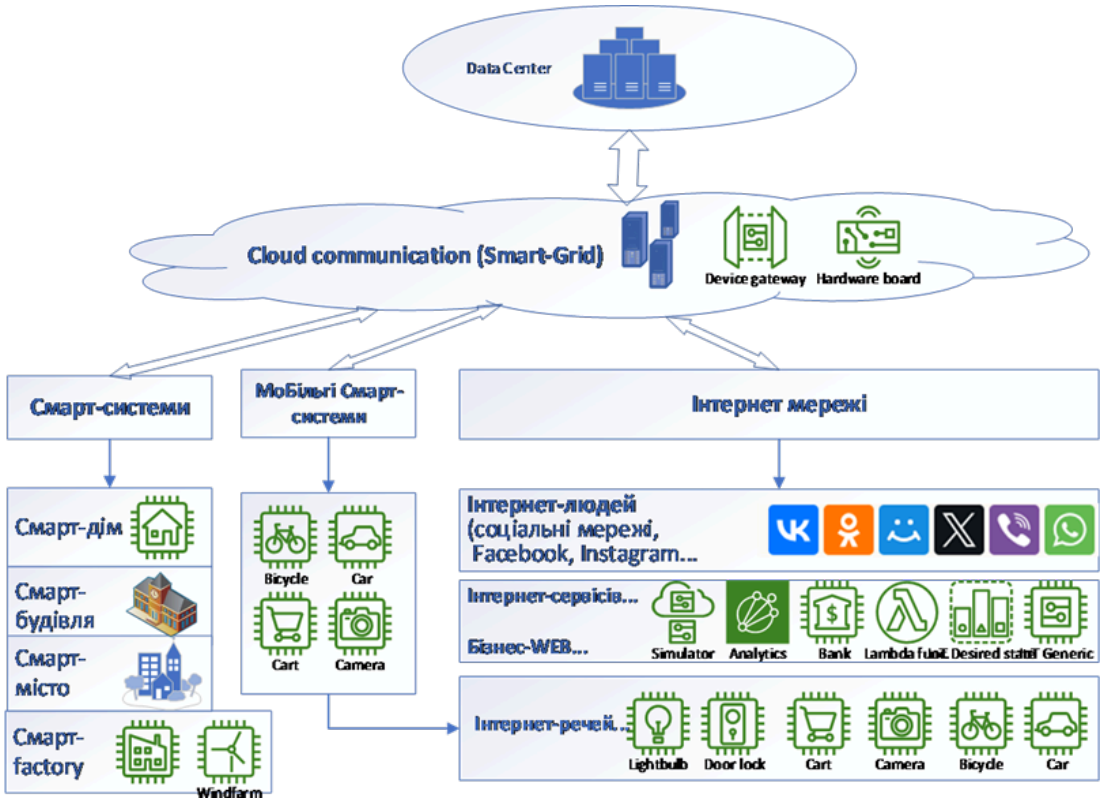

Рисунок 1.1 - Склад СКФС *(джерело [1])*

Впровадження соціо-кібер-фізичних систем (СКФС) на підприємствах ускладнює їхню структуру через зростання кількості компонентів. Це призводить до необхідності вдосконалювати різні аспекти їх побудови - технічні, інформаційні та програмні [1]. Соціо-кібер-фізичні системи докорінно трансформують структуру всієї системи, перетворюючи її на "розумну" сітку (Smart Grid) [1]. Архітектурні особливості таких систем детально відображено на рисунку 1.2.

Еволюція комп'ютерних систем зберігає базову архітектурну основу, яка, подібно до ДНК, поступово збагачується новими елементами, не втрачаючи своєї класичної сутності. Усі комп'ютерні системи базуються на цій архітектурній формулі, яка була розглянута раніше [1].

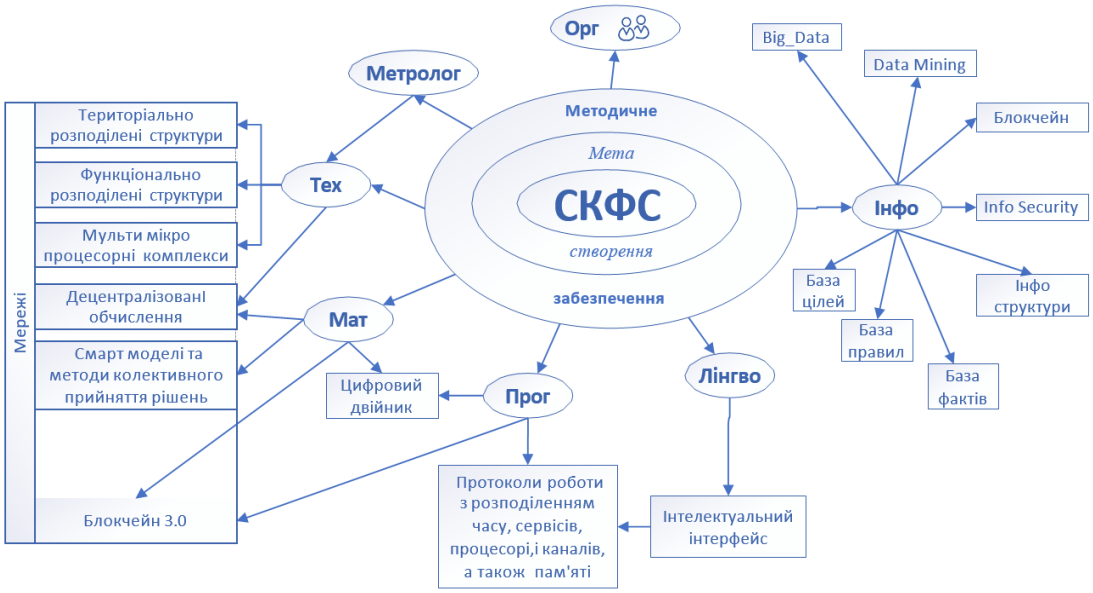

Рисунок 1.2 - Архітектурні особливості СКФС *(джерело [1])*

8.2. Огляд механізмів аналізу відмов СКФС.

Розглянемо ключові аспекти оцінки відмово стійкості комп'ютерних систем. Концепція надійності, що представлена на рисунку2.1, є комплексною системою, що охоплює не лише теоретичні засади, а й практичні компоненти, які забезпечують її реалізацію.

До таких компонентів належать загрози, що впливають на систему (збої, помилки, відмови), атрибути, які визначають її якісні характеристики, та засоби досягнення, спрямовані на підтримку безперебійної роботи. Це дозволяє

Рисунок 2.1 - Структура концепції надійності обчислювальних систем

(джерело [3])

зрозуміти, як теоретичні основи відмово стійкості застосовуються для створення надійних обчислювальних систем у реальних умовах.

Відмова (failure), у контексті обчислювальних систем, виникає, коли послуга, що надається, відхиляється від правильної, що може бути пов'язане з невідповідністю специфікації або її недостатньою точністю.

Помилка (error) - це стан системи, що може призвести до відмови, виявляючись, коли вона досягає інтерфейсу послуги та порушує її.

Збій (fault) вважається передбачуваною причиною помилки: він активний, якщо викликає помилку, і сплячий, якщо ні. Система може демонструвати різні режими відмов, які класифікуються за ступенем тяжкості та характеризуються через такі аспекти, як область відмови, керованість, узгодженість та вплив на навколишнє середовище.

Режими відмов (failure) системи визначають і класифікують за рівнем тяжкості. На рисунку 2.2 представлені види відмов, охарактеризовані через чотири аспекти: область відмови, керованість, узгодженість за наявності кількох користувачів та вплив на навколишнє середовище. Симптоми цих відмов також показані на рисунку 2.2.

Взаємозв'язок між збоями (fault), помилками (error) та відмовами (failure) визначається процесами активації (activation), поширення (propagation) та причинності (causation). Збій стає активним, роблячи помилку, коли він

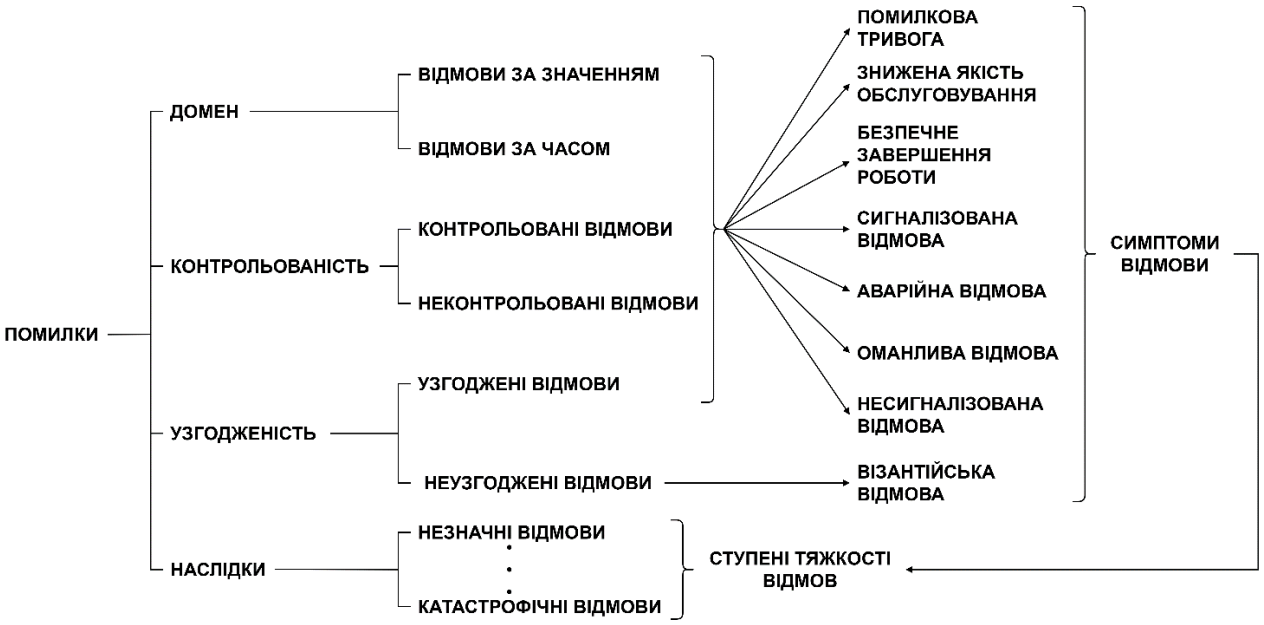

Рисунок 2.2 - Види відмов та їх симптоми *(джерело [3])*

переходить зі сплячого стану під впливом обчислювального процесу або зовнішніх умов, або виникає як зовнішній збій. Помилка поширюється в середині компонента через обчислення (внутрішнє поширення) або між компонентами, коли досягає інтерфейсу послуги, викликаючи некоректну роботу та передачу помилки далі (зовнішнє поширення).

Ланцюжок причинності ілюструється на рисунку 2.3, де стрілки відображають послідовний вплив збоїв, помилок і відмов, підкреслюючи, що перед відмовою може виникнути кілька помилок.

Рисунок 2.3 - Ланцюжок взаємозв'язку збоїв, помилок та відмов

Надійність (dependability) поєднує наступні ключіві атрибути:

доступність (availability) - готовність до правильної роботи;

безвідмовність (reliability) - безперервність коректної служби;

безпека (safety) - відсутність катастрофічних наслідків для користувачів та середовища;

конфіденційність (confidentiality) - захист від несанкціонованого розкриття даних;

цілісність (integrity) - відсутність некоректних змін стану системи;

ремонтопридатність (maintainability) - здатність до ремонту та модифікацій [3].

Крім основних атрибутів надійності (dependability) існують додаткові, вторинні атрибути. До них належать стійкість (robustness) - надійність щодо зовнішніх збоїв (faults), підзвітність (accountability) - забезпечення доступності та цілісності (integrity) даних про особу, яка виконала операцію, автентичність (authenticity) - цілісність змісту та джерела повідомлення, а також беззаперечність (non-repudiability) - підтвердження доступності й цілісності ідентичності відправника або одержувача повідомлення. Ці атрибути особливо важливі для безпеки та різняться залежно від типу інформації [3].

Надійність (dependability) обчислювальних систем досягається через поєднання чотирьох ключових засобів, кожен із яких включає свої методи та підходи [3]; :

1) Запобігання несправностям (Fault Prevention), спрямоване на виключення виникнення збоїв (faults) на етапах проектування та виробництва за допомогою технік контролю якості, таких як структуроване програмування та модульність для ПЗ, а також суворі правила проектування та захист від зовнішніх впливів для обладнання;

2) Відмово стійкість (Fault Tolerance) забезпечує безперервну доставку коректної послуги незважаючи на активні збої, реалізуючи через виявлення помилок (error detection) та відновлення системи (recovery), включаючи обробку помилок (rollback, compensation, rollforward) та управління збоями (діагностика, ізоляція, реконфігурація];

3) Усунення несправностей (Fault Removal) проводиться як на стадії розробки (через верифікацію, діагностику та корекцію), так і в процесі експлуатації (коригуюче та попереджувальне обслуговування), щоб скоротити кількість або тяжкість збоїв;

4) Прогнозування несправностей (Fault Forecasting) оцінює поточний стан, майбутню частоту та наслідки збоїв з використанням якісних (наприклад, аналіз

режимів відмов) та кількісних (імовірнісних) методів, таких як моделювання та тестування.

Ці засоби взаємодоповнюють один одного, забезпечуючи комплексний підхід до досягнення надійності системи.

Розглянемо основні механізми оцінки відмово стійкості обчислювальних систем, які дозволяють кількісно та якісно аналізувати їх надійність і стійкість до збоїв. Ці механізми та їх порівняльні характеристики зведені в таблицю 2.2.

В таблиці 2.2 проаналізовані та представлені такі методи, як аналіз дерева несправностей (FTA), аналіз видів та наслідків відмов (FMEA), ексафлопний симулятор Монте-Карло (MCESim), блокова діаграма надійності (RBD) та аналіз першопричин (RCA), що формують основу для виявлення, прогнозування та управління потенційними відмовами в системах.

Більш детально зупинемось на методі аналізу дерев несправностей (Fault Tree Analysis, FTA). Він є важливим інструментом в інженерній практиці, що використовується для аналізу надійності систем і виявлення причин відмов. Цей метод застосовується у різних галузях, таких як авіація, автомобілебудування та ядерна енергетика. FTA дозволяє моделювати процес виникнення системного збою шляхом побудови орієнтованого ациклічного графа, який показує, як низькорівневі несправності поширюються системою, призводячи до відмови на верхньому рівні. Метод допомагає приймати обґрунтовані рішення під час проектування та обслуговування систем [4].

Аналіз дерева несправностей (FTA) заснований на використанні різних символів для моделювання логічних зв'язків між подіями системи, рисунок 2.3 (a-b). Структура дерева несправностей включає такі типи подій, зображені на рисунку 2.3 (a), на схемі присутні:

- базові події (basic events), позначені колом, є вихідними збоями, які не вимагають подальшого уточнення та ініціюють відмову системи;
- верхньорівнева подія (top event), позначена прямокутником, моделює повну відмову системи, а проміжні події (intermediate event), пов'язані з відмовами підсистем або компонентів, оснащені логічними вентилями.

Таблиця 2.2 - Порівняння механізмів аналізу відмово стійкості *(з джерел [4, 5, 6, 7, 8])*

Механізми	Мета та галузь застосування	Тип аналізу	Складність реалізації	Точність	Масштабованість
FTA	Надійність техніки, прийняття рішень	Якісний та кількісний	Від поміркованого до високого	Залежить від вхідних даних та припущень	Помірно, але покращується за допомогою таких методів, як діаграми бінарних рішень
FMEA	Управління ризиками, поліпшення якості	Аналіз причин і наслідків, числове оцінювання ризиків	Від поміркованого до високого	Залежить від вхідних даних та експертизи команди	Помірно, але покращується за допомогою цифрових інструментів
MCESim	Симуляції відмов у високопродуктивних обчислювальних системах	Симуляція поведінки, оцінка продуктивності	Висока, складна архітектура симулятора	Залежить від точності моделювання відмов та системи	Висока, призначена для симуляції екзафлопсних систем
RBD	Оцінка надійності та доступності складних систем	Графічне зображення, метрики надійності та доступності, аналіз шляхів успіху та причин невдач	Від поміркованого до високого	Залежить від якості вхідних даних і моделей	Висока, з використанням піддіаграм і симуляцій Монте-Карло
RCA	Управління відмовами у виробництві	Аналіз причин, збір і обробка даних	Від поміркованого до високого, залежить від інструментів і даних	Залежить від якості даних і експертизи команди	Помірна, з використанням шаблонів і інструментів

Авторська таблиця.

Логічні зв'язки між подіями визначаються типами вентилів, які представлені на рисунку 2.3 (b):

- AND-вентилі вказують, що подія відбудеться лише за одночасного виникнення всіх пов'язаних із нею базових чи проміжних подій;
- OR-вентиль показує, що подія відбудеться, якщо настане хоча б одна із пов'язаних подій;
- k/N-вентилі (або VOT) позначають, що подія відбудеться, якщо настане щонайменше k з N пов'язаних подій.

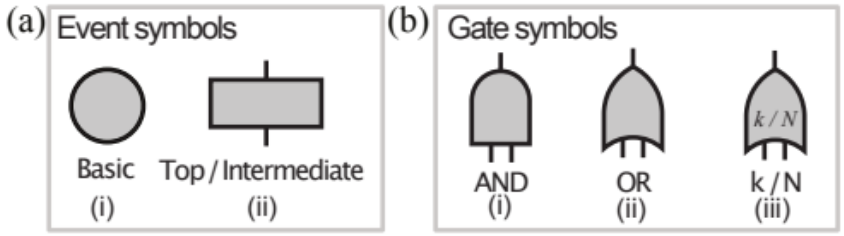

Рисунок 2.3 - Елементи аналізу дерева неисправностей (події та вентилі)

(джерело [4])

Даний механізм включає два основні типи аналізу: якісний та кількісний. Якісний аналіз ґрунтується на структурі дерева несправностей та спрямований на виявлення критичних компонентів системи. Він визначає мінімальні набори відмов (minimal cut sets), які призводять до системної відмови, а невеликі набори вказують на вразливість системи [4].

Кількісний аналіз, своєю чергою, зосереджено розрахунку метрик надійності системи. До них відносяться:

- безвідмовність (reliability) - ймовірність відсутності відмови системи за певний період;
- доступність (availability) - частка часу, протягом якого система залишається працездатною;
- середній час до відмови (Mean Time To Failure, MTTF) - середній інтервал до першої відмови [4].

Для виконання таких розрахунків базові події дерева несправностей повинні

бути забезпечені ймовірностями відмов, представленими у вигляді функцій щільності ймовірності, або у вигляді постійних ймовірностей [4].

Кількісний аналіз дерева FTA є достатньо складним і потребує певних обчислювальних ресурсів. Для цього аналізу використовується показники надійності початкових блоків в структурі, які достатньо складно обрахувати або знайти в літературних джерелах. Тому для кількісних метрик визначення характеристики відмовостійкості будемо використовувати нечітке моделювання подій в методі FTA. Сутність цього підходу пов'язана з введенням нечітких моделей відвомостійкості та відповідних логічних структур для опису складних систем керування. Цей удосконаленний метод будемо називати **Fuzzy fault tolerant analysis (F-FTA).**

8.3. Нечіткий аналіз відмово стійкості систем F- FTA

8.3.1 Теоретичні передумови побудови F- FTA

Відомі логіко-імовірнісні схеми (ЛІС) дозволяють оцінити коефіцієнт готовності пристрою на основі коефіцієнтів готовності його компонентів та логічних зв'язків між ними. Така схема представлена нижче, на рисунку 3.1.

Отримання кінцевого результату пов'язано з певним обсягом математичних обчислень з допомогою ймовірностей подій. Ці ймовірності часто відсутні або є неточними для компонентів системи. Тому з метою спрощення та прискорення оцінки працездатності складних комп'ютерних систем та мереж пропонується методика отримання інформації про стан пристроїв на основі нечітких значень станів елементів системи та їх логічних зв'язків.

Розглянемо основні положення запропонованої методики.

1. Усі виділені компоненти системи, що впливають на її працездатність, мають два стани: 1 - елемент або весь пристрій - працездатні; 0 - система непрацездатна, або в стані відмови.

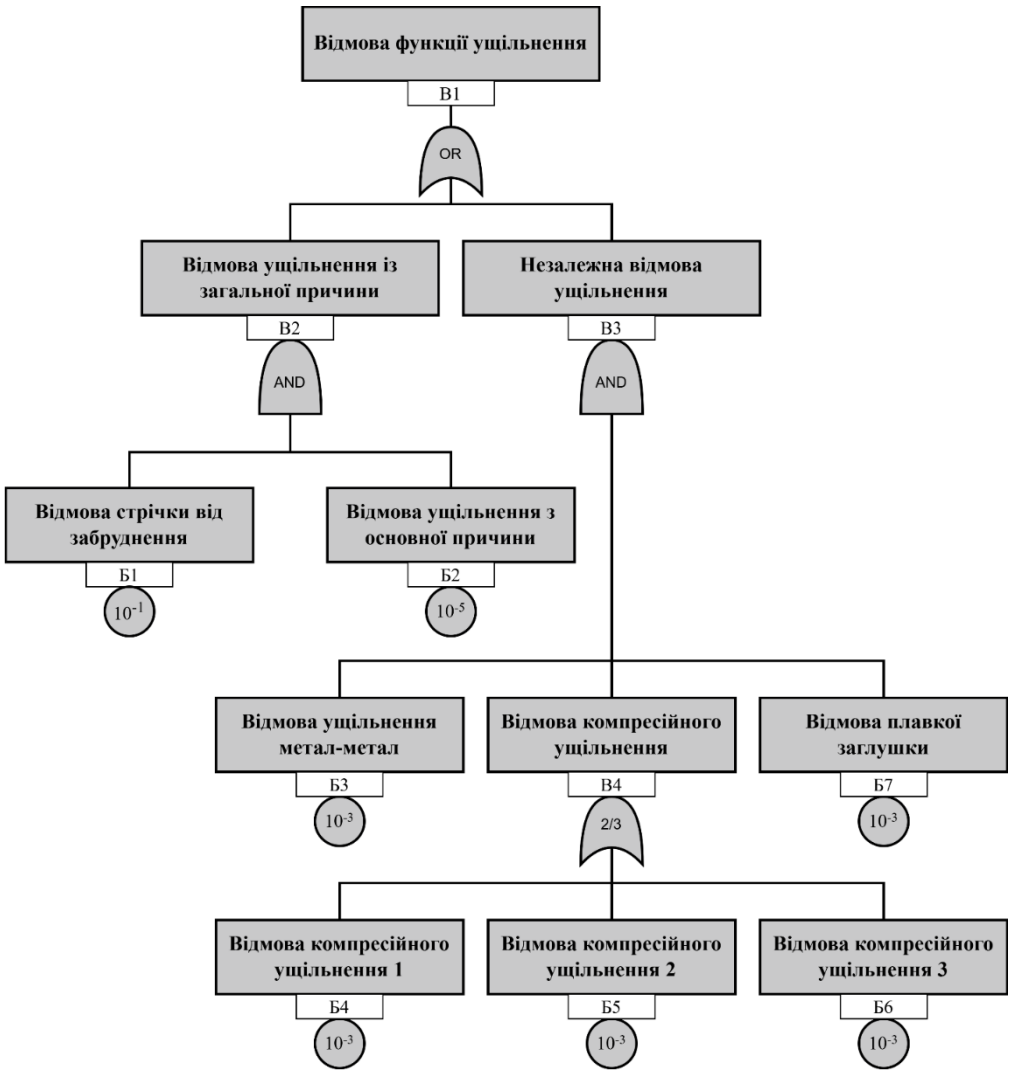

Рисунок 3.1 - Логіко-ймовірнісна схема аналізу відмово стійкості *(джерело [4])*

2. Експертним шляхом визначаються вихідні нечіткі стани елементів системи. Наприклад, "далеко" (малий,0.2) - "середньо" (середній,0.5) - "близько" (великий,0.9) до отриманого значення стану системи 0 або 1. Кожному з цих значень призначається значення коефіцієнта належності в діапазоні [0; 1]. Наприклад, для зазначених термів це можуть бути коефіцієнти (0.25 або 0.75). Для кожного елемента системи ці значення можуть відрізнятися з урахуванням їхньої функціональної завантаженості.

3. На наступному етапі будується логічна схема **з двоканальних елементів** "і", "або", "ні".

4. Кожен логічний елемент має два входи: для завдання коефіцієнта

належності і двійкового коду стану вихідного компонента (0 або 1). Обробка коефіцієнтів належності здійснюється за правилами логічних операцій над нечіткими множинами для сигналів 1 .

1. На рисунку 3.2 показані правила виконання основних операцій у задачах оцінки працездатності систем за методом F-FTA (Fuzzy Fault Tree Analysis). Якщо розглядати схему, побудовану з ненадійних елементів,

2. тобто в станах "0", то необхідно міняти логічну структуру і правила формування кінцевого ненадійного стану. Але це вже інша задача, яка потребує іншого дослідження.

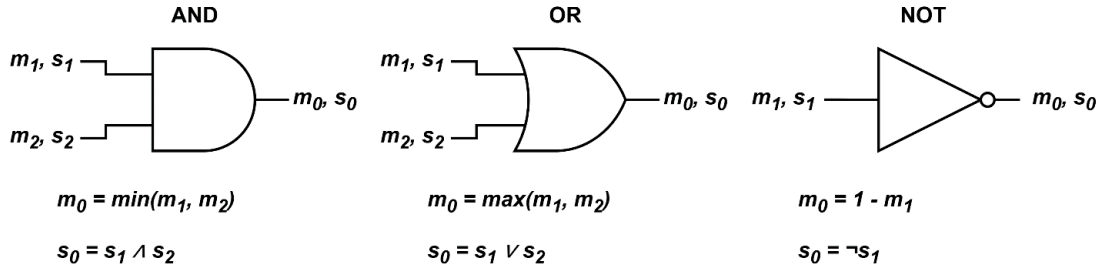

Рисунок 3.2 - Базові логічні елементи схем F-FTA

8.3.2 Приклад використання методу F-FTA

Розглянемо результат аналізу схем функціонування систем, який представлено на рисунку 3.3.

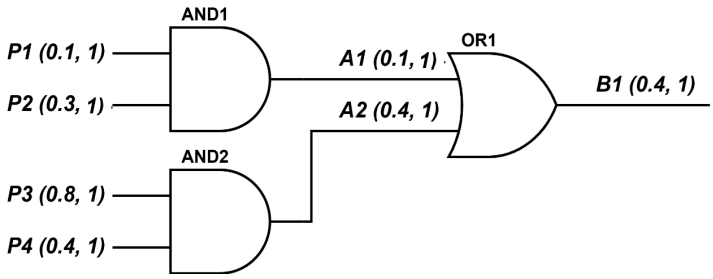

Рисунок 3.3 - Приклад нечіткого аналізу схеми

На вході системи - чотири датчики P1, P2, P3 і P4. Характеристики цих датчиків наступні:

- P1 - датчик, який видає лише 10% достовірної інформації;
- P2 – більш надійний датчик у 30% випадків;
- P3 - надійне джерело сигналу з достовірністю 80%;

- P4 - менш надійне джерело сигналу з імовірністю безотказної роботи лише 40%.

Оброблені за схемами І1 та І2, ми отримуємо два сигнали А1 і А2, які надходять на схему "АБО".

При цьому сигнал А1 можна вважати надійним на 10%, а сигнал А2 - надійним на 40%. У результаті ми отримуємо оцінку всієї схеми В1 як надійну з достовірністю 40%.

Як видно з цього прикладу, коефіцієнти належності для конкретного нечіткого стану елемента системи інженер-проектувальник може обирати більш прийнятну для нього метрику для коефіцієнта належності: імовірність, ступінь належності стану, відсотки випадків належності, коефіцієнти достовірності та інші, суб'єктивно обрані в процесі аналізу, одиниці вимірювання.

Відзначимо деякі властивості запропонованого опису дерева станів (відмов) логічної схеми пристроїв (функцій).

а) для абсолютно надійних елементів системи, тобто коли всі 1 незалежно від коефіцієнтів належності, результат також буде 1 з обчисленим коефіцієнтом для схеми;

б) якщо всі вихідні стани 0, то й результат буде 0 з певним новим коефіцієнтом належності;

в) при комбінації значень надійності елементів схеми результат буде характеристикою кінцевого стану системи;

г) під час аналізу можливі два варіанти інтерпретації кінцевого стану пристрою: 1 або 0. Усе залежить від формулювання завдання (питання, "склянка з чаєм наполовину порожня чи наполовину повна?").

Всновки та рекомендації

Удосконалений метод F-FTA (Fuzzy Fault Tree Analysis) дозволяє оцінювати відмово стійкість складних систем за допомогою нечітких значень станів компонентів, спрощуючи аналіз при неточних або відсутніх ймовірностях станів компонентів 1 або 0. Вони описуються їх коефіцієнтами належності, що обробляються за правилами нечітких множин.

Метод зручний для аналізу складних систем, дозволяючи інженерам швидко отримувати результати щодо відмово стійкості систем, що проектуються.

Рекомендується використовувати розроблений метод F-FTA на етапах концептуального проектування та розробки соціо-кібер-фізичних систем для оцінки їхньої відмово стійкості. Це дозволить виявляти потенційні вразливості системи на ранніх стадіях, зменшуючи витрати на усунення помилок під час експлуатації. Метод особливо корисний для систем, де точні ймовірності відмов компонентів важко визначити.