ISSN 2223–5620 (Print), ISSN 2411–1554 (Online)
Електромагнітна сумісність та
безпека на залізничному транспорті, 2012, № 4

УДК 656.256:621.318.5

А. І. КУСАЙКО – студент, Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна, andrey_11111@mail.ru

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ НАДІЙНОСТІ ТА ФУНКЦІЙНОЇ БЕЗПЕКИ МІКРОПРОЦЕСОРНИХ СИСТЕМ ЕЦ

Статтю представив д. фіз.-мат. н., проф. В. І. Гаврилюк

Вступ

Сучасний стан пристроїв залізничної автоматики і телемеханіки (ЗАТ) на залізницях України характеризується фізичною та моральною зношеністю більшості основних фондів. Релейно-контактні системи ЗАТ, застарілі як фізично, так і морально, не відповідають сучасним вимогам щодо ефективного управління процесом перевезень та забезпечення конкурентоспроможності залізничного транспорту. Згідно з прийнятими державними програмами проблема переоснащення систем ЗАТ має бути вирішена з використанням мікроелектронної програмувальної техніки. Враховуючи, що переважну кількість пристроїв ЗАТ за технічною оснащеністю становлять станційні системи електричної централізації стрілок та сигналів (ЕЦ), яка досягає майже 50%, основні зусилля з модернізації цих пристроїв мають припадати саме на системи ЕЦ.

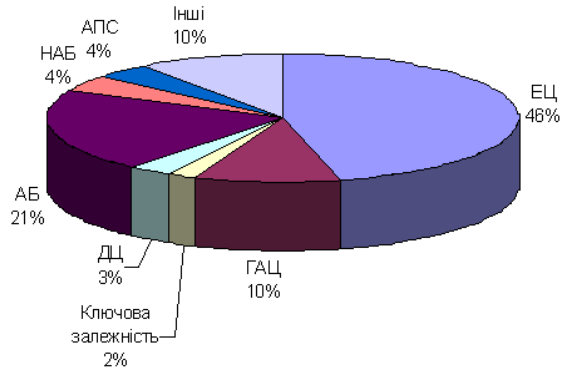

Рис.1. Внесок різних пристроїв ЗАТ в загальну технічну оснащеність.

Разом з фізичним має місце і моральне старіння релейних систем ЕЦ. При широкому впровадженні в теперішній час інформаційних технологій в процес перевезень і управління залізничним транспортом релейні системи важко інтегруються у відповідні інформаційні і обчислювальні структури. Для цієї інтеграції виявляються недостатніми функціональні і інформаційні можливості релейних систем, їх швидкодія, крім того, вимагаються додаткові перехідні пристрої і перетворювачі електричних сигналів. В цьому відношенні мікропроцесорні і релейно-процесорні централізації повністю задовольняють сучасним вимогам.

Мета роботи

Метою роботи є дослідження показників надійності та функційної безпечності мікропроцесорних систем ЕЦ.

Критерії небезпечних відмов МПЦ

Критерієм небезпечної відмови системи МПЦ є видача заборонених (більш дозволяючих) управляючих впливів на об’єкти низової автоматики, а також поява в системі можливості видачі заборонених управляючих впливів внаслідок спотворення даних системи, що відображають реальну технологічну ситуацію на станції.

Віповідно до цього небезпечними є такі відмови:

- відкриття або підтримка дозволяючого сигналу світлофора при невиконанні умов безпеки;
- переведення стрілки при невиконан- ні умов безпеки;
- формування дозволяючого коду в рейкове коло при невиконаних умовах безпеки;

- зміна напрямку при невиконаних умовах безпеки;
- вмикання більш дозволяючого сигналу;
- відсутність контролю погаслого стану світлофора;
- зниження напруги живлення ламп світлофорів без команди або дозволу ДСП;
- розмикання стрілок при невиконаній послідовності умов з перевірки руху поїзду по маршруту;
- відміни маршруту чи штучне розмикання при дозволяючому сигналі на світлофорі, що огороджує маршрут;
- відсутність сигналу сповіщення на переїзд при зайняті поїздом ділянки наближення;
- помилкова індикація стану об'єктів управління і контролю на моніторах АРМ ДСП та ШН;
- неможливість ДСП перекрити світлофор, закрити переїзд;
- неможливість ДСП виконати індивідуальне замикання чи блокування стрілок, світлофорів та інших об'єктів.

Порушення в роботі схем узгоджень і об'єктів управління і контролю:

- короткочасна втрата шунта;
- відмова і пошкодження обладнання рейкового кола;
- коротке замикання ізолюючих стиків;
- перемежовуюче коротке замикання ізолюючих стиків;
- пошкодження нитки лампи світлофора;
- втрата контролю стрілки;
- переплутування лінійних проводів в схемі управління стрілкою;
- коротке замикання і обрив проводів монтажу і кабельної мереж;
- відмови станційних пристроїв автоблокування і схеми зміни напрямку.

Концепція досягнення функційної безпечності

Концепція досягнення функційної безпечності базується на таких принципах:

1. Поодинокі відмови апаратних і програмних засобів не повинні призводити до небезпечних відмов (появи хибних сигналів включення інтерфейсних реле, що управляють польовими пристроями; та хибних одиниць в однойменних розрядах вхідних масивів даних які передаються в контролер централізації та блокування).
2. Поодинокі відмови апаратних і програмних засобів повинні виявлятися і блокуватися із заданою вірогідністю не пізніше, ніж у системі виникне друга відмова, за умови, що одночасна наявність обох відмов у системі може привести до небезпечної відмови.
3. Поодинокі відмови апаратних і програмних засобів повинні виявлятися з заданою ймовірністю при робочих і тестових впливах не пізніше, ніж виникне друга відмова.
4. Не повинно відбуватися накопичення невиявлених відмов хоча б в одному каналі модулів вводу/виводу.
5. Апаратно-програмному переході в незворотний захисний стан обчислювального каналу при виявленні відмови.
6. Використання схем управління, в яких забезпечується безпечне вмикання об'єкту, а у випадку відмови пристроїв схеми – переведення об'єкту в безпечний стан.
7. Забезпечувати захист даних в мережах зв'язку між рівнями системи засобами завадостійкого кодування.
8. Застосовувати систему і пристрої живлення технічних засобів, які дозволять забезпечити неперервне і якісне живлення.

9. Застосувати в модулях вводу/виводу схем, що працюють у динамічному режимі, трансформаторну гальванічну розв'язку кіл управління і живлення реле.

Підвищення показників надійності (безпеки та безвідмовності) МПЦ шляхом резервування

Однією з проблем мікроелектронної апаратури є її чутливість до зовнішніх електромагнітних впливів(її чутливість до електромагнітних перешкод більше в 10000 раз,ніж у електромагнітних реле). Тому застосування екранування повинно бути обов'язковим і встановлюватись в об'ємі в залежності від умов експлуатації .

Звичайно, щоб від всіх таких впливів захисти в повній мірі не вийде і апаратура може функціонувати під негативним впливом перешкод, призводячи при цьому неправильні та небезпечні дії, або взагалі може вийти з ладу. Звідси виникає потреба у резервуванні апаратури. Резервування може мати різну структуру та принцип функціонування. Кожна резервована структура має свої власні показники безпеки, безвідмовності, надійності і тому застосування тієї чи іншої конфігурації визначається необхідними рівнями цих показників для даної системи.

При побудові безпечних мікропроцесорних централізацій в теперішній час найбільше застосовують двоканальні та трьохканальні (мажоритарні) структури. Проведемо аналіз цих структур. Двоканальна (дубльована) система, яку називають "два з двох" . Система працездатна тільки у тому випадку, коли працездатні обидва канали і показники безвідмовності розраховуються за формулами:

$$P'2\vee 2'(t)=e^{-2\lambda t}, \quad (1)$$

$$Q'2\vee 2'(t)=1-e^{-2\lambda t}, \quad (2)$$

$$\lambda'2\vee 2'(t)=2\lambda, \quad (3)$$

$$T'2\vee 2'(t)=\frac{1}{2\lambda}. \quad (4)$$

Система переходить в небезпечний стан, коли не працездатні обидва канали. Тому,

$$Q_{\text{ОП}}'2\vee 2'(t)=\left(1-e^{-\lambda t}\right)^2, \quad (5)$$

$$P_{\text{б}}'2\vee 2'(t)=2e^{-\lambda t}-e^{-2\lambda t}, \quad (6)$$

$$\lambda_{\text{ОП}}'2\vee 2'(t)=\frac{2\lambda\left(1-e^{-\lambda t}\right)}{2-e^{-\lambda t}}, \quad (7)$$

$$T_{\text{ОП}}'2\vee 2'(t)=\frac{3}{2\lambda}. \quad (8)$$

На рис. 2 показаний графік відношення ймовірності безпеки двоканальної системи до одно канальної в залежності від інтенсивності відмов.

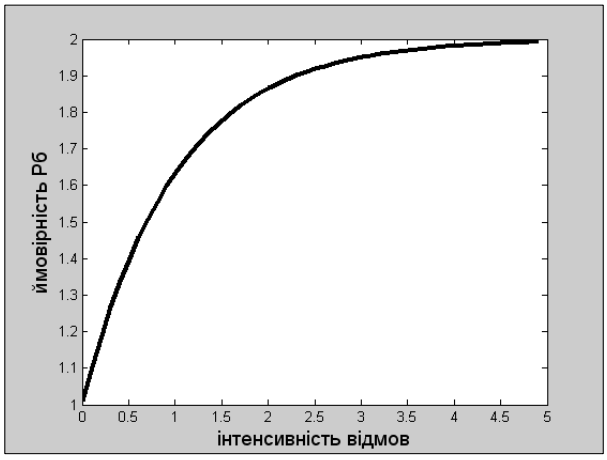

Рис. 2. Графіки співвідношення безпеки двоканальної та одноканальної систем (відношення ймовірностей безпеки $\frac{P_{\text{б}}'2\vee 2'(t)}{P_{\text{б}}'1\vee 1'(t)}$)

Для даного моменту часу t ймовірність безпечної роботи системи "два з двох" збільшується у порівнянні з ймовірністю безпечної роботи одного каналу в $\left(2-e^{-\lambda t}\right)$ разів, оскільки

$$\frac{P_{\text{б}}'2\vee 2'(t)}{P_{\text{б}}'1\vee 1'(t)}=2-e^{-\lambda t}. \quad (9)$$

Звідси можна зробити висновок, що ймовірність безпечної роботи двоканальної системи "два з двох" не може бути більшою ніж ймовірність безпечної роботи одного каналу в 2 рази. Наприклад, при t = 10T це збільшення складає 1.999955. Щоб отримати більше підвищення безпеки,

необхідно підвищувати число каналів(кратність резервування) в багатоканальній системі.

Якщо порівняти двоканальну та одноканальну системи за показником безвідмовності рис. 3, то бачимо, що один канал має перевагу над двома у цьому аспекті.

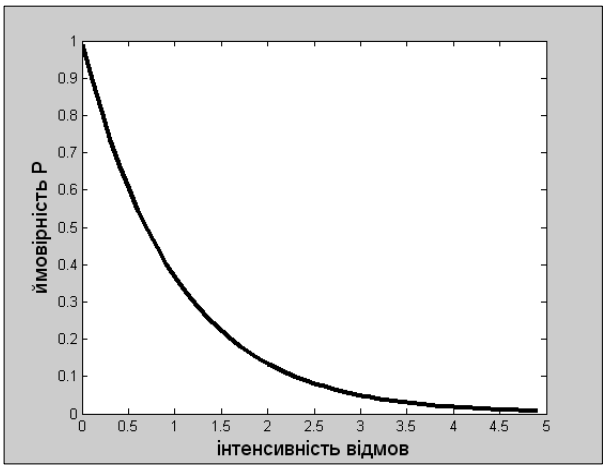

Рис.3. Графіки співвідношення безвідмовності двоканальної та одноканальної систем (відношення ймовірностей безвідмовності $\frac{P\ '2\vee 2'(t)}{P\ '1\vee 1'(t)}$)

На рис. 4 приведені характеристики системи “два з двох”.

Тому по відношенню до одного каналу в двоканальній системі “два з двох” для любого моменту часу ti прирощення ймовірності безпечної роботи дорівнює зменшення ймовірностей безвідмовної роботи. В системі “два з двох” є суттєвий недолік: безпека забезпечується за рахунок зменшення безвідмовності.

Найбільш частіше при побудові систем використовують трьохканальні мажоритарні структури(“два з трьох”). Стан всієї системи може бути працездатним (П) або небезпечним (Н). З даної висловлення витікає принцип роботи мажоритарної системи “два з трьох”: система працездатна, якщо будуть працездатними хоча б два канали з трьох; при відмові двох каналів система переходить в небезпечний стан; захисних станів не існує.

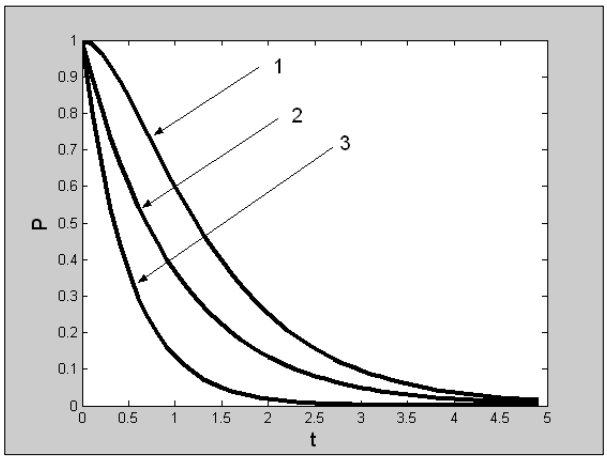

Рис. 4. Характеристики надійності системи “два з двох”:
1 – графік залежності ймовірності безпеки системи $P_б'2\vee 2'(t)$, 2 – графік залежності ймовірності безпеки одноканальної системи $P_б'1\vee 1'(t)$, 3 – графік залежності ймовірності безвідмовності системи $P'2\vee 2'(t)$

Показники безвідмовності системи “два з трьох” розраховуються за формулами:

$$P'2\vee 3'(t)=3e^{-2\lambda t}-2e^{-3\lambda t}, \qquad (10)$$

$$\lambda\ '2\vee 3'(t)=\frac{6\lambda\left(1-e^{-\lambda t}\right)}{3-2e^{-\lambda t}}, \qquad (11)$$

$$T_{\text{ОП}}'2\vee 3'(t)=\int_0^{\infty}P''2\vee 3''(t)dt-\frac{5}{6\lambda}. \qquad (12)$$

З графіку співвідношення безвідмовності систем “ два з трьох ” та “ два з двох” рис. 5 видно, що безвідмовність мажоритарної системи перевищує безвідмовність системи “ два з двох ” при всіх значеннях λ t. В області великих значень це перебільшення рівно трьом. Безпека мажоритарної системи, навпаки, завжди менше безпеки системи “ два з двох ”. Це пов’язано з тим , що в системі “ два з трьох ” всі відмови є небезпечними (захисних відмов немає). Як безпечність мажоритарної системи зменшується видно з графіку співвідношення безпеки систем “ два з трьох ” та “ два з двох” рис.6 в області малих значень λt (λt>0.2) це зменшення не суттєве. Наприклад,при λt=0.2 по відношенню до системи “два з двох” безпека мажоритарної системи зменшуєть-

ся на 5.5%, в той час безвідмовність збільшується на 36.3%.

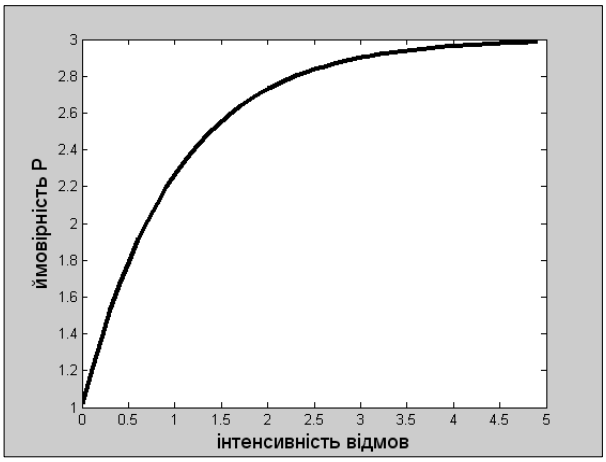

Рис.5. Графіки співвідношення безвідмовності систем “ два з трьох “ та “два з двох“ (відношення ймовірностей безвідмовності $P'2 \vee 3'(t) / P'2 \vee 2'(t)$)

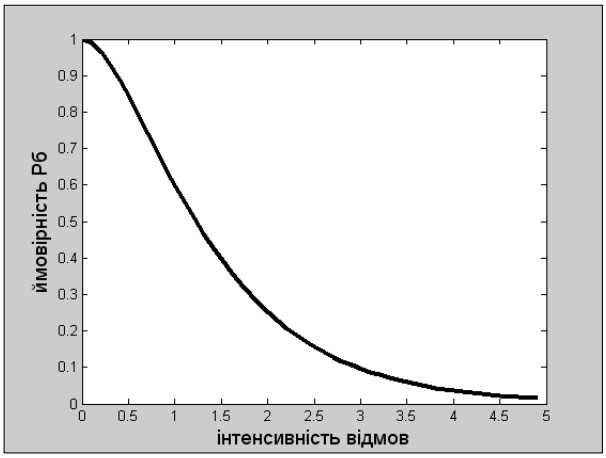

Рис.6. Графіки співвідношення безпеки систем “ два з трьох “ та “ два з двох “(відношення ймовірностей безпеки $P_б'2 \vee 3'(t) / P_б'2 \vee 2'(t)$)

В порівнянні з системою “ два з двох ” відносна зміна інтенсивності відмов системи “ два з трьох ” дорівнює зміні інтенсивності небезпечних відмов. В цілому система “ два з двох ” у порівнянні з системою “ два з трьох ” дає суттєве збільшення безвідмовності при визначеному зменшенні безпеки.

Щоб покращити показники безпеки мажоритарної структури, зберігаючи при цьому той самий рівень безвідмовності, застосуємо систему “ два з трьох ” з реконфігурацією. В цій системі при відмові одного каналу виходи цього каналу відключаються і структура “ два з трьох ” трансформується в структуру “ два з двох”. Тому

$$P'2 \vee 3P'(t) = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}, \quad (13)$$

$$\lambda_{ОП}'2 \vee 3P'(t) = \frac{3\lambda - 6\lambda e^{-\lambda t} + 3\lambda e^{-2\lambda t}}{3 - 3e^{-\lambda t} + e^{-2\lambda t}}. \quad (14)$$

$$T_{ОП}'2 \vee 3P'(t) = \frac{3}{\lambda} - \frac{3}{2\lambda} + \frac{1}{6\lambda} = \frac{11}{6\lambda} = 1{,}83\frac{1}{\lambda}. \quad (15)$$

Відношення ймовірностей безпеки системи “ два з трьох ” з реконфігурацією до одноканальної системи виражається наступним виразом:

$$\frac{P_б''2 \vee 3P''(t)}{P''1 \vee 1''(t)} = 3 - 3e^{-\lambda t} + e^{-2\lambda t}. \quad (16)$$

Таким чином, в області великих значень λ t ймовірність безпечної роботи системи “два з трьох ” з реконфігурацією в три рази перевищує величину $P''1 \vee 1''(t)$, так як небезпечна відмова виникає при одночасній відмові усіх трьох каналів. В той же час величина $P_б''2 \vee 3P''$ перевищує величину $P_б''2 \vee 2''(t)$ в 1,5 рази, так як небезпечна відмова у системі “ два з двох ” виникає при одночасній відмові двох каналів (рис. 7). Вираз співвідношення за яким будується даний графік:

$$\frac{P_б''2 \vee 3P''(t)}{P''2 \vee 2''(t)} = \frac{3 - 3e^{-\lambda t} + e^{-2\lambda t}}{2 - e^{-\lambda t}}. \quad (17)$$

З точки зору безвідмовності в області малих значень λt найкращі показники мають мажоритарна система “ два з трьох ” та система з реконфігурацією. Особливо ця перевага перед другими системами дуже велика при високій надійності одного каналу.

В області великих значень λt безвідмовність структур “ два з трьох ” та “два з трьох ” з реконфігурацією стає менше без-

відмовності одного каналу. Наприклад, у системи “ два з трьох ” це проходить при $\lambda t>0.69$.

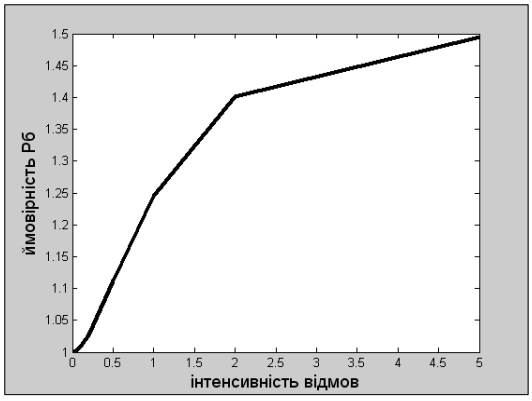

Рис.7. Графіки співвідношення безпеки систем ”2∨3Р” та “2∨2” (відношення ймовірностей безпеки $\frac{P_{б}"2\vee 3Р"(t)}{P\ "2\vee 2"(t)}$)

При $\lambda t\to\infty$ ці системи реконфігуруються в дубльовані системи і їх інтенсивність відмов наближується до величини 2λ. Проходить це тому ,що в структурі “ два з трьох ” з реконфігурацією пріоритет безпеці за рахунок безвідмовності. Цими обставинами пояснюється той факт, що одноканальна система має найбільше значення середнього напрацювання на відмову:

$$T=\frac{1}{\lambda} \qquad (18)$$

З точки зору безпеки найкращі показники має система “ два з трьох ” з реконфігурацією у порівнянні з системою “ два з трьох ” (рис. 8). В області малих значень ця система забезпечує високий рівень безпеки. В структурі “два з трьох ” з реконфігурацією успішно поєднуються високі якості безвідмовності мажоритарних структур і високі якості безпеки кон’юктивного співпадання. Система “ два з трьох ” з реконфігурацією має найбільші значення середнього напрацювання до небезпечної відмови $1{,}83\frac{1}{\lambda}$.

Системи “ два з трьох ” та “ два з трьох” з реконфігурацією дійсно мають гарні показники надійності, але якщо мова йде про ці структури як системи, які відповідають за видачу важливої інформації, то тут є деякі недоліки. Наприклад, візьмемо структуру “ два з трьох ” з реконфігурацією. Ця структура працездатна, коли два канали працездатні, а третій ні. Як поведе себе система у цьому випадку, наприклад, якщо працездатний канал видасть помилкову інформацію.

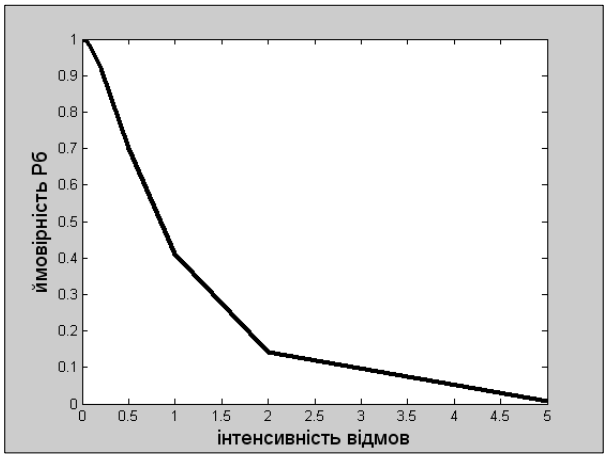

Рис. 8. Графіки співвідношення безпеки систем ”2∨3” та “2∨3Р” (відношення ймовірностей безпеки Рб”2∨3”/Рб”2∨3Р")

Так, система буде знаходитись у працездатному, але яку інформацію вона видасть на виході, яка команда буде прийнята і як вона вплине на подальший процес функціонування апаратури ЕЦ. Звідси виникає проблема надійності роботи централізації із-за недостовірної інформації. Багато відмов на станції виникає з приводу невірних та помилкових даних. Рішенням цієї проблеми є застосування структури “три з трьох”. Така система працює за наступним принципом : всі три канали працездатні (і дають однакову інформацію) – стан структури працездатний (на виході системи достовірна інформація); якщо один або два канали непрацездатні система переходить в захисний стан (інформація класифікується як недостовірна); якщо всі канали непрацездатні стан системи класифікується як небезпечна відмова.

Порівняно зі структурами “ два з трьох ” та “ два з трьох ” з реконфігурацією система “три з трьох” має менший показник по безвідмовності (рис. 9) та однаковий по безпеці, це зумовлено тим, що система в більшості випадків переходить в захисний стан.

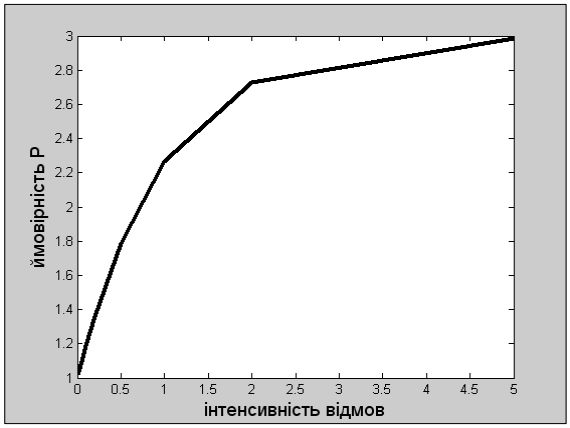

Рис. 9. Графіки співвідношення безвідмовності систем 2∨3Р” та “3∨3”

Такий принцип роботи пояснюється призначенням даної структури, як інформаційної. Тому важливість прийняття правильного рішення (або отримання достовірної інформації) є більш пріоритетним, а звідси і менші показники по безвідмовності. Перевага тут полягає у чіткому розмежуванні стану системи з виключенням всіх ситуацій, які могли б вплинути на подальшу роботу всієї структури. Показники безвідмовності та безпеки розраховуються за формулами:

$$P"3 \vee 3"(t) = e^{-3\lambda t}, \qquad (19)$$

$$P_б"3 \vee 3" = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}. \qquad (20)$$

На рис. 10 і рис. 11 наведені графіки залежностей ймовірностей безпеки та безвідмовності від інтенсивності відмов всіх систем. З рис. 10 видно, що при малих значеннях інтенсивності відмов показники безвідмовності приблизно однакові, і тільки зі збільшенням λt кожна структура веде себе по-різному. І це необхідно враховувати при проведенні періодичних профілактичних перевірок. Проаналізувавши графік, зображений на рис.11, можна зробити 100% висновок, що найбільш безпечною системою є “ два з трьох ” з реконфігурацією. Але застосування тієї чи іншої структури залежить від умов експлуатації , нормативних вимог безпеки, призначення системи за функціонуванням, економічності застосування та ін.

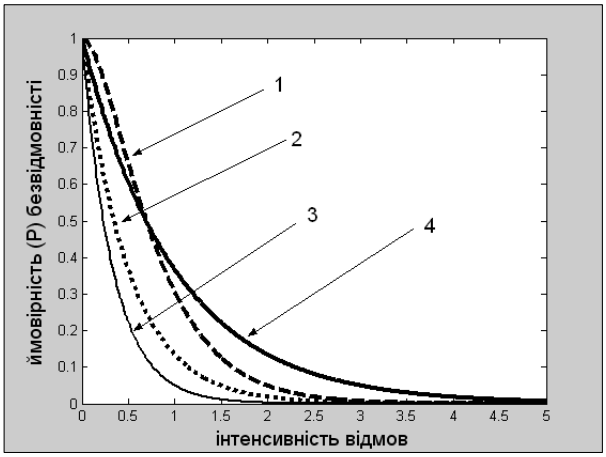

Рис.10. Графіки залежностей ймовірностей безвідмовності від інтенсивності відмов:
1 – система “ два з трьох “ та “ два з трьох “ з реконфігурацією; 2 – система “ два з два “; 3 – система “ три з трьох “; 4 – система “ один з одного“

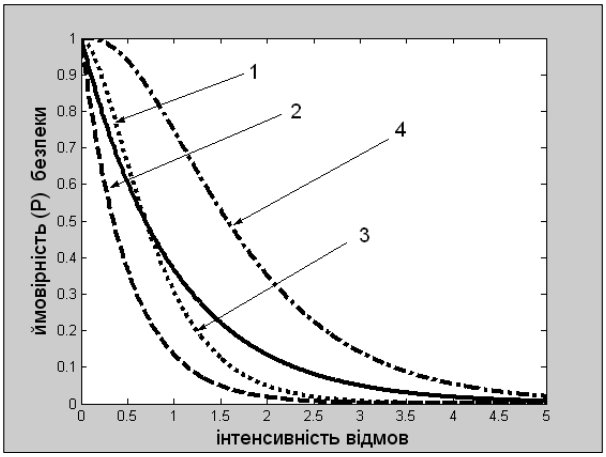

Рис. 11. Графіки залежностей ймовірностей безпеки від інтенсивності відмов:
1 – система “ один з одного “ ; 2 - система “ два з двох “; 3 - система “ два з трьох “; 4 -система “ два з трьох “ з реконфігурацією

Висновок

Відповідно до поставленої мети було розроблено критерії небезпечних відмов мікропроцесорної централізації стрілок і сигналів. Сформульовано концепцію досягнення функційної безпечності системи МПЦ. Детально розглянуто способи резервування, як захист апаратури від негативного впливу перешкод. Резервування може мати різну структуру та принцип функціонування. Кожна резервована структура має свої власні показники безпеки, безвідмовності, надійності і тому застосування тієї чи іншої конфігурації визначається необхідними рівнями цих показників для даної системи.

Бібліографічний список

1. Кустов, В.Ф. Основи теорії надійності та функціональної безпечності систем залізничної автоматики [Текст]: навчальний посібник для вузів / В. Ф. Кустов. – Харків: УкрДАЗТ, 2008. – 218 с.
2. Мойсеєнко, В. И. Основы системного похода к безопасности железнодорожного транспорта [Текст] / В. И. Мойсеєнко // Збірник наукових праць Донецького інституту залізничного транспорту. – 2006. Вип. 7. – С. 5-14.
3. Бочков, К. А. Методы обеспечения безопасности в микропроцессорных системах железнодорожной автоматики и телемеханики [Текст]: учебное пособие для студентов транспортных специальностей высших учебных заведений / К. А. Бочков, С. Н. Харлап. – Гомель: БелГУТ, 2001. – 84 с.
4. Сапожников, В. В. Сертификация и доказательство безопасности систем железнодорожной автоматики [Текст] / В. В. Сапожников, Вл. В. Сапожников, В. И. Талалаев. – М.: Транспорт, 1997. – 288 с.
5. Основные принципы обеспечения безопасности и безотказности микропроцессорных систем железнодорожной автоматики и телемеханики [Текст] / Памятка ОСЖД Р-858 от 09.11.2006 г. – Варшава,2006.–24с.

Ключові слова: надійність та безпечність, резервування, безпека МПЦ, поодинокі відмови МПЦ, критерії небезпечних відмов.

Ключевые слова: надёжность и безопасность, резервирование, безопасность МПЦ, одиночне отказы МПЦ, критерии опасных отказов.

Keywords: reliability and bezop-clarity, redundancy, security MOC MOC single fault, the criteria for dangerous failures.

Надійшла до редколегії 25.10.2012