

УДК 656.2: 621.3: 614.8

ФУНДАМЕНТАЛЬНІ НЕДОЛІКИ БАЗОВИХ МОДЕЛЕЙ НЕБЕЗПЕЧНИХ ВІДМОВ ДЛЯ РОЗРАХУНКУ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ СИСТЕМ КЕРУВАННЯ РУХОМ ПОЇЗДІВ

Канд. техн. наук В. Ф. Кустов

FUNDAMENTAL LIMITATIONS OF BASIC DANGEROUS FAILURE MODELS FOR FUNCTIONAL SAFETY ASSESSMENT IN TRAIN CONTROL SYSTEMS

PhD (Tech.) V. F. Kustov

DOI: <https://doi.org/10.18664/1994-7852.212.2025.336537>



Анотація. У статті досліджено поширену практику застосування експоненціального закону розподілу небезпечних відмов для оцінювання ризику в системах керування рухом поїздів. Наведено основні фізичні ознаки старіння компонентів систем залізничної автоматики, що призводять до суттєвої похибки в разі використання експоненціальних моделей для розрахунків нормативних показників функціональної безпеки. Показано, що у випадку реальних систем з іншими законами розподілу відмов, особливо за довготривалої експлуатації (більше 10 років), таке спрощене обчислення призводить до багатократних прорахунків в оцінюванні функціональної безпеки і, як наслідок, недопустимого зниження безпеки руху поїздів. Як доказ функціональної безпеки пропонується використовувати інші закони розподілу небезпечних відмов або на етапі допуску в експлуатацію враховувати в розрахунках реальне підвищення інтенсивності небезпечних відмов елементів внаслідок їх старіння в жорстких умовах експлуатації систем залізничної автоматики.

Ключові слова: безпека руху поїздів, експоненціальний закон, небезпечні відмови, недооцінювання ризику безпеки, розподіл небезпечних відмов, системи керування рухом поїздів, функціональна безпека, SIL(інтегральний рівень безпеки).

Abstract. The article examines the widespread practice of using the exponential distribution law for modeling hazardous failures in risk assessment of railway traffic control systems. It outlines key physical signs of aging in components of railway automation systems, which can lead to significant errors when exponential models are applied to calculate the normative indicators of functional safety. It is demonstrated that in real systems with alternative failure distributions—particularly under long-term operation (over 10 years)—such simplified calculations result in multiple misestimations of functional safety, ultimately leading to unacceptable reductions in railway traffic safety. To justify functional safety, the article recommends the use of other hazardous failure distribution laws or, during the commissioning phase, the inclusion of actual increases in failure intensity caused by aging under harsh operating conditions typical for railway automation systems.

Keywords: train traffic safety, exponential distribution, dangerous failures, underestimation of safety risk, distribution of dangerous failures, train control systems, functional safety, SIL (Safety Integrity Level).

Вступ. Розрахунок імовірності небезпечної відмови є основним етапом у забезпеченні функціональної безпеки критичних систем, у тому числі систем

керування рухом поїздів. Найбільш розповсюдженим для розрахунку на практиці є використання експоненціального закону розподілу небезпечних відмов, але в

багатьох реальних випадках такий розподіл має іншу форму: із піком на середині життєвого циклу, або з ефектом зношування. У таких ситуаціях застосування експоненціального закону може призвести до критичного недооцінювання ризику відповідальних систем автоматизації.

Аналіз останніх досліджень і публікацій. Розробленню методів нормування і встановлення вимог щодо функціональної безпеки систем керування рухом поїздів присвячені роботи [1, 2]. Питання вдосконалення методів оцінювання функціональної безпеки систем залізничної автоматики в умовах наявності кратних небезпечних відмов у каналах резервування розглянуто в роботі [3]. Результати досліджень математичних моделей функціональної безпеки та безвідмовності відновлюваних технічних засобів за різних способів резервування наведено в роботах [4, 5]. Особливості забезпечення функціональної безпеки мікропроцесорних систем керування і контролю на залізничному транспорті висвітлено в дослідженні [6]. Теоретичні основи надійності та функціональної безпеки систем залізничної автоматики детально розглянуті в роботі [7]. Базові питання стандартизації функціональної безпеки в Україні наведено в публікаціях [8–10], а міжнародний досвід – у роботах [11, 12].

У світовій практиці найпоширенішим підходом для оцінювання функціональної безпеки є використання експоненціальної моделі розподілу часу до небезпечної відмови елементів і каналів резервування. Проте в умовах реальної експлуатації, особливо із застосуванням сучасних мікроелектронних компонентів високої якості, відмови часто мають інший характер розподілу. Через це в останніх версіях міжнародних стандартів [11, 12] наголошено на необхідності обережного використання експоненціальних моделей, хоча конкретних прикладів помилок чи недооцінювання ризику через їх

застосування не наведено. Це зумовлює потребу в критичному оцінюванні достовірності математичних моделей розподілу небезпечних відмов, які є основою для визначення рівня функціональної безпеки. Очевидно, що точність таких оцінок, безпосередньо пов'язаних із ризиком виникнення аварій і катастроф на залізничному транспорті, має як велике наукове, так і практичне значення.

Визначення мети та завдання дослідження. Метою дослідження є оцінювання достовірності різних математичних законів розподілу часу до небезпечних відмов, що застосовують для розрахунку функціональної безпеки, порівняно з базовим експоненціальним законом, який найчастіше використовуваний і регламентований чинними стандартами.

У межах дослідження передбачено виконання таких завдань:

- проаналізувати особливості застосування експоненціального закону у стандартах функціональної безпеки;
- порівняти результати розрахунку імовірностей небезпечних відмов за експоненціальним і альтернативними законами розподілу;
- визначити потенційні похибки (недооцінювання або переоцінювання) рівня функціональної безпеки з використанням неадекватної моделі розподілу;
- сформулювати рекомендації щодо доцільності застосування певних законів розподілу залежно від типу елементів, умов експлуатації та етапу життєвого циклу.

Результати роботи можуть бути використані для удосконалення методик обґрунтування функціональної безпеки систем залізничної автоматики з урахуванням реальних характеристик відмов технічних засобів.

Метою статті є оцінювання достовірності різних законів розподілу небезпечних відмов для розрахунку функціональної безпеки порівняно з

базовим експоненціальним законом, який частіше за все використовуваний і регламентований стандартами з функціональної безпеки, а також дослідження недооцінки і переоцінки розрахунку ймовірностей небезпечних відмов у разі використання інших законів розподілу відмов відносно базового експоненціального закону.

Основна частина дослідження

1. Порівняльний аналіз щільностей ймовірностей небезпечних відмов для експоненціального, нормального та вейбулівського законів розподілу

Щільність ймовірності небезпечних відмов (щільність розподілу часу до небезпечної відмови) дає змогу визначити ймовірність виникнення такої відмови протягом будь-якого інтервалу часу експлуатації системи. Геометрично це відповідає площі під кривою функції щільності в межах заданого цього інтервалу. Крім того, на її основі визначають функцію ризику – інтенсивність небезпечних відмов у часі $\lambda(t)$.

Розуміння форми розподілу часу до небезпечної відмови є основним для врахування у функціональній безпеці таких аспектів:

- розрахунок ймовірності виникнення небезпечної відмови в будь-яку годину експлуатації (PFH – Probability of Dangerous Failure per Hour) відповідно до вимог міжнародних і європейських стандартів;

- визначення необхідного рівня функціональної безпеки (SIL1–SIL4) на основі отриманого значення PFH;

- моделювання сценаріїв небезпечних відмов, що можуть призвести до втрати безпечної функції у відповідальних системах автоматизації.

За стандартами [10-12], нормативне значення PFH визначають як середнє значення щільності ймовірності небезпечних відмов. Для експоненціального закону розподілу, який найчастіше використовуваний в інженерній практиці, PFH наближено дорівнює λ за умови малих

значень добутку λt ($\lambda t < 0,1$). У таких умовах це наближення вважають допустимим, і воно навіть дає певний запас безпеки для оцінювання ризику.

Порівняльний аналіз щільностей ймовірностей відмов дає змогу:

- ідентифікувати часові ділянки з максимальною ймовірністю виникнення небезпечної відмови (так звану «зону підвищеного ризику»);

- ухвалювати обґрунтовані рішення про періодичне технічне обслуговування, своєчасну заміну компонентів або модернізацію систем;

- виявити потенційні недоліки у використанні типового (експоненціального) підходу для моделювання відмов для систем із реальною статистикою деградації.

Для досліджень вибрано закони розподілу $f(t)$ із приблизно однаковими значеннями середнього наробітку до небезпечної відмови і відповідними параметрами (рис. 1):

- експоненціальний:

$$\lambda = 1/100\,000 \text{ 1/год};$$

- нормальний розподіл:

$$\mu = 100\,000 \text{ год}, \sigma = 20\,000 \text{ год};$$

- Вейбулла: $\beta = 2$, $\eta = 113\,000 \text{ год}$.

Аналіз форми розподілу щільностей розподілу небезпечних відмов уже на якісному рівні дає змогу дійти висновку про ймовірності появи небезпечних відмов за будь-який поточний час експлуатації чи будь-який інтервал періодичного контролю чи часу експлуатації. За рис. 1, ймовірність небезпечних відмов для експоненціального закону розподілу найбільша на ранніх етапах експлуатації і зменшується з часом, що не завжди відповідає реальним умовам. Інші закони розподілу враховують старіння і знос і мають піки ймовірностей відмов. Для кількісного оцінювання ризику прорахунку функціональної безпеки (недооцінювання/переоцінювання) проведемо більш ретельний теоретичний аналіз.

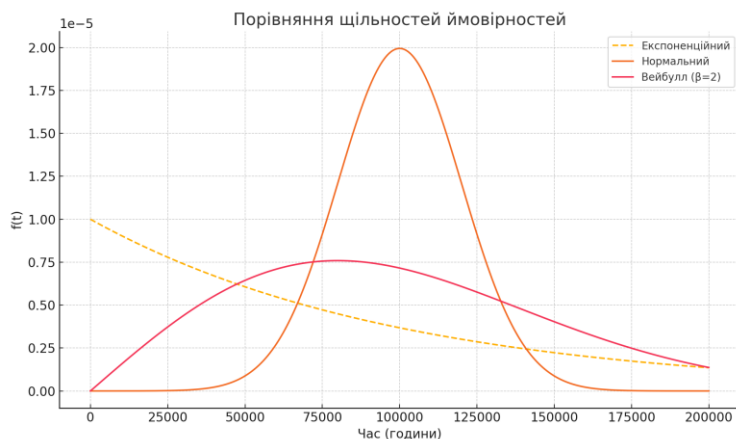


Рис. 1. Порівняння щільностей розподілу небезпечних відмов

2. Визначення коефіцієнтів недооцінювання ризику прорахунку функціональної безпеки для різних законів розподілу небезпечних відмов

Для кількісного аналізу для кожної моделі визначено ймовірність небезпечних відмов на рівних інтервалах часу та

обчислено коефіцієнт недооцінювання ризику (Ratio), яке дорівнює відношенню значень щільності небезпечних відмов «істинних» розподілів до експоненціального закону: $\text{Ratio}(t) = f_{\text{true}}(t) / f_{\text{exp}}(t)$. Відповідні графіки наведено на рис. 2.

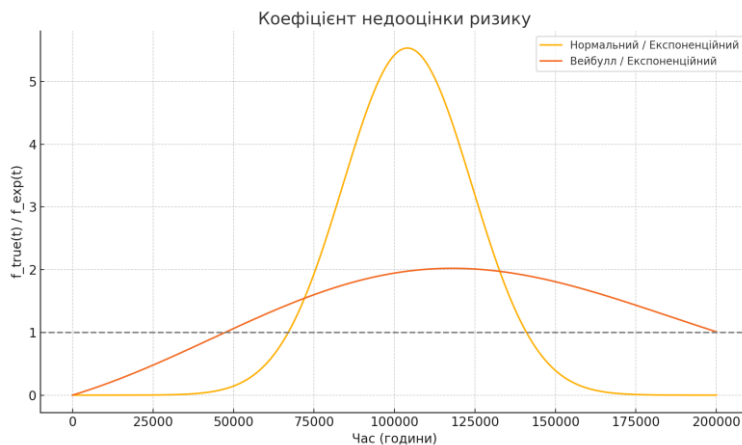


Рис. 2. Коефіцієнти недооцінювання ризику (Ratio) заміни існуючих законів розподілів небезпечних відмов на експоненціальний закон

Коефіцієнт відношення ймовірностей небезпечної відмови, отриманих за різними законами розподілу, до значень, розрахованих за експоненціальним законом (із припущенням сталої інтенсивності відмов), дає змогу кількісно оцінити ступінь

спрощення та пов'язану з ним похибку у визначенні ризику. Це дає змогу виявити кратність недооцінювання, що виникає внаслідок застосування базового експоненціального припущення.

Аналіз графіків на рис. 2 показує, що найбільше недооцінювання ризику – чотири-шість разів – спостерігають для «істинного» нормального закону розподілу в середній частині інтервалу експлуатації системи. Це означає, що практично протягом третини терміну служби виникає суттєвий прорахунок у визначенні ймовірності небезпечної відмови. Для розподілу Вейбулла така похибка є меншою, але все ж таки значною – до двох разів – у проміжку до 75 % часу експлуатації (тобто переважну частину життєвого циклу системи).

З огляду на значну кратність недооцінювання ризику (від двох до шести разів), було проведено додаткові розрахунки для ширшого діапазону параметрів і розглянуто інші реально застосовувані закони розподілу небезпечних відмов у системах автоматизації:

- експоненціальний розподіл – для компонентів зі сталою інтенсивністю відмов;
- розподіл Вейбулла – для моделювання зростаючого або спадного ризику з часом;
- гамма-розподіл – для складних сценаріїв із кількома стадіями зношування (використовуваний рідше);

- нормальний розподіл – застосовують у випадках оцінювання середнього часу безвідмовної роботи. Однак у контексті моделювання часу до небезпечних відмов він є менш реалістичним. Відповідно до центральної граничної теореми, за великої кількості незалежних факторів впливу загальний розподіл наблизатиметься до нормального. Проте, за рекомендаціями [12], використання нормального розподілу для оцінювання рівнів SIL (SIL1–SIL4) є недоцільним.

Дослідження проводили для типового терміну служби систем автоматизації — 10–20 років, із середнім часом до небезпечної відмови в межах 100 000 – 150 000 годин. Було порівняно:

- розподіли Вейбулла з параметрами $\beta = 1.5; 2.0; 3.0$ (що моделюють зростання ризику з часом);
- гамма-розподіли з параметрами $\alpha = 2; 3$ і відповідними значеннями β ;
- нормальні розподіли з різними стандартними відхиленнями $\sigma = 10\ 000; 20\ 000; 30\ 000$ год.

На рис. 3 наведено узагальнені коефіцієнти недооцінювання або переоцінювання ризику для різних законів розподілу, подані у вигляді графіків відносних значень (Ratio).

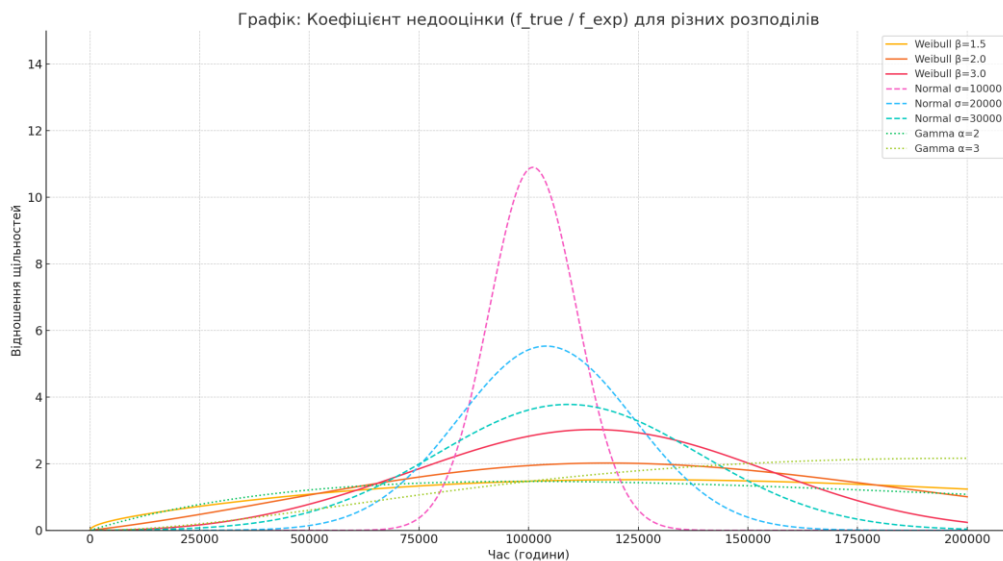


Рис. 3. Коефіцієнти недооцінювання ризику заміни різних («істинних») законів розподілів небезпечних відмов на експоненціальний закон

Для аналізу недооцінювання ймовірностей небезпечних відмов використовуємо відношення ймовірностей небезпечних відмов «істинного» закону

розподілу до експоненціального (інтервальні коефіцієнти недооцінювання). Результати досліджень наведено на рис. 4.

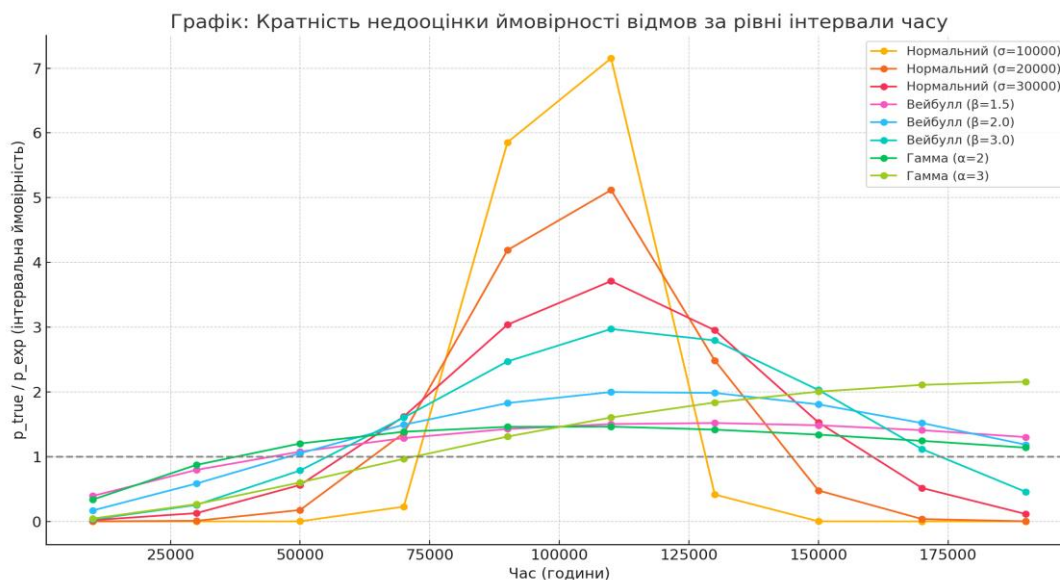


Рис. 4. Залежність недооцінювання ймовірностей небезпечних відмов для різних законів розподілу

3. Аналіз похибок оцінювання функціональної безпеки з використанням експоненціального закону

Результати дослідження показали таке:

- нормальний розподіл: за ширших розподілів ($\sigma > 20\,000$ год) недооцінювання ризику за експоненціальною моделлю поширюється на довший інтервал експлуатації. Водночас максимальне недооцінювання ризику спостерігають у випадку вузьких нормальних розподілів із малим стандартним відхиленням (до п'яти-семи разів);

- розподіл Вейбулла, який є найбільш придатним для опису процесів деградації в системах залізничної автоматики, — недооцінювання імовірності небезпечної відмови за експоненціальним законом

проявляється вже після першої третини життєвого циклу;

- гамма-розподіл з $\alpha = 3$, що моделює багатозначне зношування, демонструє зсув піку ризику до завершальної фази експлуатації, унаслідок чого критичне недооцінювання ризику виникає саме в передаварійній зоні;

- середня похибка в розрахунку функціональної безпеки протягом 20-річного життєвого циклу з помилковим використанням експоненціального закону замість розподілу Вейбулла або гамма-розподілу може перевищувати нормативний рівень майже на порядок.

У табл. 1 подано характерні приклади похибок оцінювання ризику, що виникають з некоректним застосуванням експоненціального закону розподілу небезпечних відмов.

Таблиця 1

Оцінювання ризику з хибним застосуванням експоненціального закону розподілу небезпечних відмов

Реальний розподіл	Поведінка ризику	Помилка з заміною на експоненціальний
Нормальний	Пік у середині	Недооцінювання в чотири-шість разів у центрі
Вейбулла ($\beta > 1$)	Старіння	Недооцінювання в середині і наприкінці ресурсу
Вейбулла ($\beta < 1$)	«Дитячі хвороби»	Переоцінювання на початку
Експоненціальний	Сталий ризик	-

Отже, навіть використовуючи моделі, які формально дозволені чинними стандартами з функціональної безпеки, надзвичайно важливим є обґрунтований вибір адекватного закону розподілу. Експоненціальний закон є лише окремим випадком розподілу Вейбулла за умови $\beta = 1$, тому будь-яке спрощення моделі до припущення постійної інтенсивності без належної валідації є методологічно помилковим.

Проведене моделювання показало, що найбільшу похибку серед усіх розглянутих випадків дає не виправдана заміна нормального розподілу експоненціальним. У таких випадках імовірність небезпечної відмови може бути недооцінена майже на порядок, особливо зі зменшенням стандартного відхилення, що призводить до втрати достовірності розрахунків.

Окремо було проаналізовано сценарій із дуже малим стандартним відхиленням ($\sigma = 1000$ год), який відповідає високій повторюваності терміну служби – типовий для чітко контрольованих і масово протестованих систем. У цьому випадку ймовірність відмови різко концентрується поблизу середнього значення, що ще раз підтверджує невідповідність експоненціальної моделі реальним характеристикам.

На рис. 5 подано графік порівняння щільностей імовірностей відмов f_{true} (нормальний розподіл) і f_{exp} (експоненціальний розподіл) для вузького нормального випадку. На рис. 6 наведено графік інтервального відношення $p_{\text{true}} / p_{\text{exp}}$ (оцінювання кратності недооцінювання) для нормального розподілу зі $\sigma = 1000$ год.

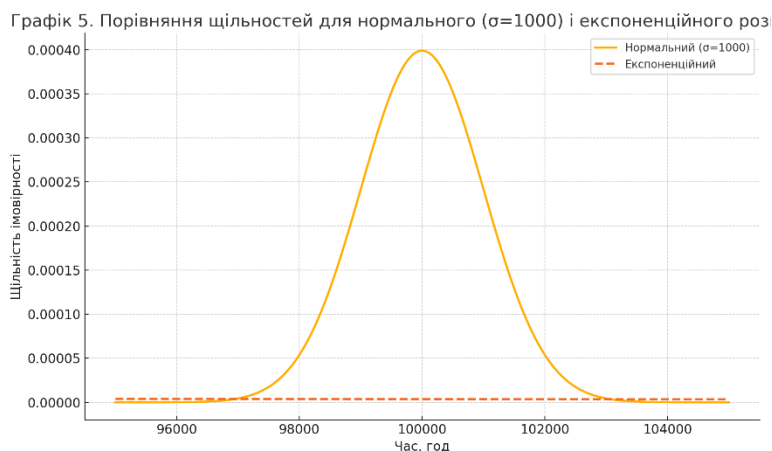


Рис. 5. Недооцінювання експоненціального розподілу у випадку нормального закону зі $\sigma = 1000$

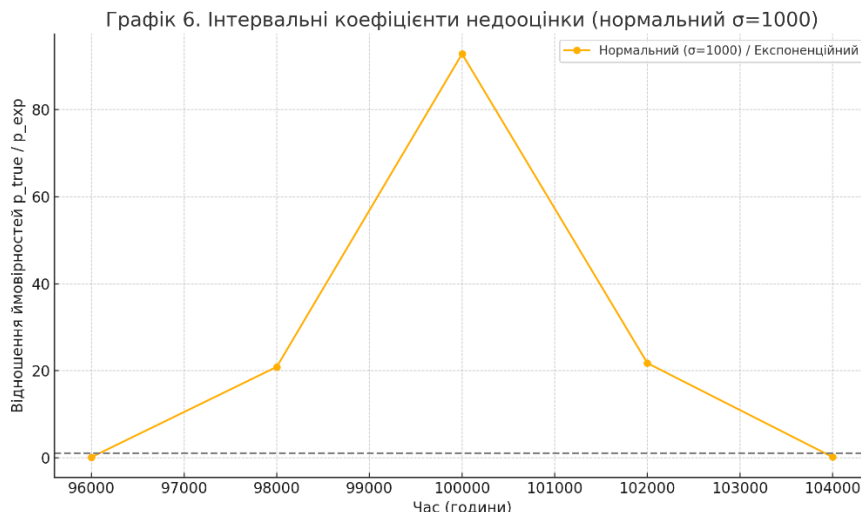


Рис. 6. Інтервальні коефіцієнти недооцінювання імовірностей небезпечних відмов (нормальний закон розподілу з параметром $\sigma = 1000$)

4. Аналіз законів розподілу небезпечних відмов у залізничній автоматичності

Для систем залізничної автоматики рекомендовано використовувати такі закони розподілу небезпечних відмов:

- експоненціальний;
- Вейбулла;
- гамма-розподіл;
- нормальний.

4.1. Експоненціальний розподіл

Цей розподіл характерний для випадків із постійною інтенсивністю небезпечних відмов. Імовірність відмови в одиницю часу (PFH) залишається сталою протягом усього терміну експлуатації, тобто ризик не змінюється з часом. За стандартами [10, 11], експоненціальний закон рекомендовано застосовувати для елементів без вираженого зношування, зокрема електронних компонентів, що працюють у межах заявленого ресурсу.

У стандарті EN 50129 прямо зазначено, що PFH для електронної апаратури може бути визначено за експоненціальним розподілом, якщо немає достовірних даних щодо старіння. Аналогічно, у ДСТУ EN 50129 [9] випадкові (random) відмови в електронних компонентах також передбачено моделювати експоненціально. Отже, у

практиці функціональної безпеки залізничної автоматики експоненціальну модель трактують як допустиму і консервативну за відсутності підтвердженого впливу старіння або деградації.

У стандарті EN 50126 / ДСТУ EN 50126 [9] вказано, що для систем, у яких переважають випадкові відмови, дозволено використовувати постійну інтенсивність, тобто експоненціальний розподіл. У разі наявності явних ознак старіння (наприклад через знос або термічну деградацію) дозволено застосування розподілу Вейбулла, але використання експоненціального підходу при цьому не заборонено.

Щодо практики, то спрощеність експоненціального моделювання і його відповідність мінімальним вимогам стандартів призводить до його поширення в сертифікаційних процедурах для систем залізничної автоматики [8–10].

Міжнародний стандарт ІЕС 61508 також дає змогу використовувати експоненціальний розподіл для оцінювання PFH, якщо відсутня верифікована інформація про зношення компонентів (частина 6, додаток В). У розділі В.3.2 цієї частини стандарту експоненціальна модель наведена як базова для прикладів оцінювання PFH та PFDavg [11].

Очікують, що результати цього дослідження можуть бути враховані під час доопрацювання проєкту нової редакції prEN IEC 61508-6:2025, публікацію якої заплановано на 2026 рік.

У разі ж виявлення ознак фізичного зношування або отримання експлуатаційних даних, що свідчать про зміну інтенсивності відмов із часом, необхідно переходити до більш адекватної моделі – розподілу Вейбулла.

4.2. Розподіл Вейбулла

Розподіл Вейбулла є універсальною та гнучкою моделлю, яка дає змогу враховувати зростання або зменшення ризику з часом:

$\beta < 1$ — висока ймовірність початкових відмов («дитячі хвороби»);

$\beta = 1$ — експоненціальна поведінка (постійна інтенсивність);

$\beta > 1$ — зростаюча інтенсивність відмов (ефекти старіння та зношення).

Цей розподіл є особливо цінним для моделювання складних систем, у яких

протягом життєвого циклу відбуваються фізичні зміни, що впливають на надійність. Системи залізничної автоматики, які працюють у складних умовах і схильні до зношення, найбільш адекватно описує саме закон Вейбулла.

Фізичні прояви старіння (wear-out) електронних компонентів — це, зокрема, зміни електричних і теплових характеристик, зниження електричної міцності ізоляцій, деградація паяння, електроміграція тощо. Усе це призводить до підвищення ймовірності небезпечних відмов на пізніх етапах експлуатації. Ці ефекти часто не виявлені під час періодичних функціональних тестів, але критично впливають на динаміку $\lambda(t)$ і коректність визначення рівня функціональної безпеки (SIL).

У табл. 2 наведено приклади фізичних ознак старіння основних компонентів систем залізничної автоматики, які мають бути враховані під час вибору закону розподілу небезпечних відмов.

Таблиця 2

Основні фізичні ознаки старіння компонентів систем залізничної автоматики

Компонент	Фізичні ознаки старіння (wear-out)
1	2
Мікропроцесори / Контролери	Деградація діелектриків, збої пам'яті, тимчасові збої (SEU), які можуть призвести до спотворення даних, збоїв у виконанні програми, помилкових спрацювань, спричинених частинкою високої енергії, наприклад нейтроном або іоном, яка влучає в мікросхему та викликає зміну збереженого біта (наприклад з 1 на 0), порушення шин I/O, що включає збільшення опору ліній, що погіршує сигнал; зміну логічних рівнів, через що пристрій перестає розпізнавати команди або реагує помилково; інтерференцію або електромагнітний шум, що викликає помилкові сигнали; втрату цілісності сигналу через мікротріщини, пошкодження доріжок чи корозію контактів; відмову драйверів I/O у мікросхемі, що робить шину повністю нефункціональною (система може виглядати працездатною, але не реагувати на сигнали або видавати некоректні команди); зниження тактової частоти, що може спричинити недопустимі затримки або помилки в синхронізації, що критично для залізничних систем реального часу, старіння комплектувальних елементів
Промислові ЕОМ	Накопичення пилу, деградація живлення, перегрів, зниження стабільності інтерфейсів, старіння комплектувальних елементів

Продовження табл. 2

1	2
Монітори / НМІ	Вигорання матриці, деградація підсвітки, зниження контрасту, несправність сенсорів, старіння комплектувальних елементів
Батареї, джерела живлення	Втрата ємності, зростання внутрішнього опору, деградація елементів живлення
Мікросхеми	Зміна порогів напруг, деградація структури кремнію, електроміграція
Транзистори	Електроміграція в структурах, зростання струмів витоку, зміна порогу відкривання, деградація оксидного шару
Тиристори	Зниження стійкості до перенапруг, деградація PN-переходів, зростання часу перемикавання
Оптрони	Зниження яскравості випромінювання світлодіода, зменшення чутливості фотоприймача, деградація оптичного каналу
Резистори	Зміна номіналу, нестабільність опору за високих температур, деградація контактів, мікротріщини
Конденсатори (неелектролітичні)	Зміна ємності через деградацію діелектрика (наприклад керамічного або плівкового), тріщини, втрати на витік, погіршення стабільності за температурних циклів
Конденсатори (електролітичні)	Втрата ємності, зростання ESR (еквівалентного послідовного опору), висихання електроліту, роздування або протікання
Дроселі / котушки індуктивності	Нагрів і деградація ізоляції, зменшення індуктивності, механічна вібрація обмоток, насичення магнітного сердечника
Трансформатори	Пересихання або деградація ізоляції, локальний перегрів, зниження ефективності магнітопроводу
Реле (електромагнітні)	Зношення або підгоряння контактів, деградація пружинного механізму, зростання часу спрацювання, втрата контактного тиску
TVS-діоди (супресори)	Погіршення швидкодії, підвищення залишкової напруги, деградація р-п переходів, зниження ефективності за повторних імпульсів, утворення мікротріщин у корпусі або виводах
Розрядники	Зношення електродів, втрата герметичності, зростання напруги пробою, погіршення реакції на імпульсні перенапруги, втрата відновлюваності після багаторазового спрацювання
Варистори	Зміна характеристики напруга-струм, зростання залишкової напруги, зменшення енергії поглинання, деградація зернистої структури, втрата чутливості до імпульсів
Електричні з'єднання	Окиснення, корозія, зростання контактного опору
Роз'єми	Окиснення контактів, механічне зношення, нестабільне з'єднання, чутливість до вібрацій
Кабелі	Мікротріщини в ізоляції, підвищення опору, волога, УФ-старіння, корозія провідників

Аналіз даних таблиці підтверджує реальність старіння і зносу у процесі експлуатації систем керування рухом поїздів, а також актуальність використання

реальних розподілів небезпечних відмов для SIL-розрахунків функціональної безпеки систем залізничної автоматики.

4.3. Гамма-розподіл у контексті оцінювання функціональної безпеки

Гамма-розподіл застосовують як альтернативу експоненціальному та вейбулівському розподілам для моделювання часу до небезпечних відмов у системах, де спостерігають:

- ненульову початкову затримку у виникненні відмов;
- багатоетапну деградацію компонентів;
- посилене старіння після певного періоду експлуатації.

Такий розподіл є доцільним для складних систем, що мають інерційний період на початку життєвого циклу або поступовий перехід між стадіями зносу. Це може бути характерно, зокрема, для окремих типів контролерів, датчиків і перетворювачів, які застосовувані в залізничній автоматизації. Попри обмежене поширення в інженерній практиці, гамма-розподіл є універсальнішим за експоненціальний, оскільки дає змогу моделювати змінну інтенсивність відмов з урахуванням початкового «затишшя» і подальшого зростання ризику.

4.4. Нормальний розподіл

Для нормального розподілу характерна симетрична, дзвоноподібна функція щільності ймовірності з максимумом у середньому значенні μ . Найвища ймовірність відмови припадає на середню частину ресурсу, що відповідає технічним системам із симетричним зносом.

Попри його застосування в ряді статистичних задач, нормальний розподіл не є адекватним для моделювання часу до небезпечної відмови в системах функціональної безпеки з таких причин:

- симетрія розподілу: нормальний закон припускає, що ймовірність «ранньої» і «пізньої» відмов однакова. Проте реальні системи зазвичай демонструють асиметричну поведінку з поступовим зростанням ризику через старіння, деградацію та накопичення дефектів;

- визначеність у від'ємній області часу: нормальний розподіл математично визначений і для $t < 0$, що суперечить фізичній суті часу до відмови. Наприклад, за середнього наробітку 100 000 год існує (хоч і дуже мала) ймовірність відмови до початку роботи, що є неприйнятним у розрахунках безпеки;

- неможливість моделювання фаз життєвого циклу: нормальний розподіл не розрізняє періоди: початкового етапу («дитячі хвороби»), випадкових відмов, відмов через старіння.

На відміну від нього, вейбулівський розподіл дає змогу змінювати параметр форми β для відображення кожної з цих фаз.

Отже, нормальний розподіл може бути прийнятним лише для статистичного аналізу результатів лабораторного тестування однорідних вибірок або аналізу розподілу середніх значень наробітку між окремими зразками (наприклад 100 однакових пристроїв). Для оцінювання PFH або ймовірності відмови в конкретний момент часу нормальний розподіл не придатний.

4.5. Логнормальний розподіл

Логнормальний розподіл має зростаючу інтенсивність відмов $\lambda(t)$ після певного моменту часу. Як і розподіл Вейбулла, він відображує процес старіння, але не входить до переліку рекомендованих у стандартах IEC 61508 чи EN 50129 для моделювання функціональної безпеки. Його застосування можливе в дослідницьких задачах або в умовах наявності емпіричних даних, що підтверджують логнормальний характер розподілу.

4.6. Узагальнена характеристика розподілів небезпечних відмов

Особливості розподілів небезпечних відмов наведено в табл. 3.

На рис. 7 наведено графіки миттєвої інтенсивності відмов $\lambda(t)$ для різних розподілів:

- Вейбулла ($\beta = 2$) – демонструє типовий сценарій старіння з монотонним зростанням $\lambda(t)$;

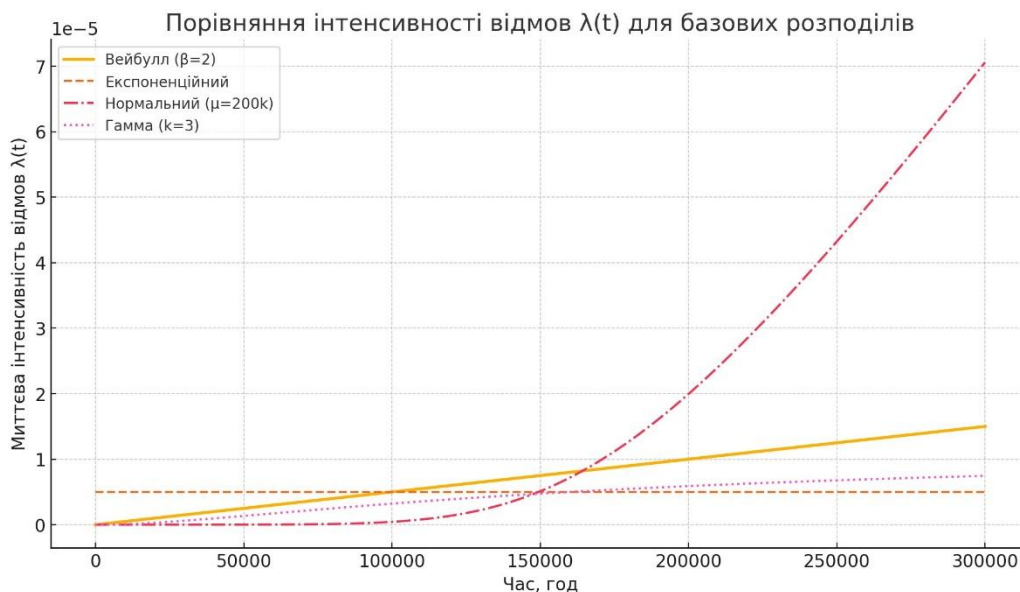
- експоненціальний — лінія з постійним значенням $\lambda(t)$, без урахування змін у часі;
- нормальний — максимум інтенсивності в середній частині терміну служби;

- гамма-розподіл — гнучка форма, яка дає змогу врахувати затримку та зростання ризику.

Таблиця 3

Особливості розподілів небезпечних відмов

Розподіл	Поведінка $\lambda(t)$	Особливості застосування
Експоненціальний	$\lambda(t) = \text{const}$	Не враховує старіння; рекомендований за відсутності даних
Вейбулла	$\lambda(t)$ змінюється залежно від β	$\beta < 1$ — «дитячі хвороби»; $\beta > 1$ — старіння
Гамма-розподіл	$\lambda(t)$ зростає за умови $k > 1$	Моделює багатостадійну деградацію, враховує інерцію
Нормальний	$\lambda(t)$ має максимум біля μ	Симетричний; не враховує фаз життєвого циклу, непридатний для PFH
Логнормальний	$\lambda(t)$ зростає асиметрично	Не рекомендований стандартами, але може враховувати старіння

Рис. 7. Графік миттєвої інтенсивності відмов $\lambda(t)$ для різних розподілів

Усі ці графіки побудовано для приблизно однакового середнього часу до відмови (~200 000 год). Цього досягають налаштуванням параметрів кожного розподілу так, щоб їхнє математичне

сподівання T_{cp} (mean time to failure, MTTF) було подібним:

- експоненціальний розподіл:
 $T_{cp} (MTTF) = 1/\lambda \approx 200\,000$ год;

- вейбулівський розподіл: $\eta = 200\,000$ за умови $\beta = 2$ середній наробіток $T_{cp} (MTTF) = \eta \cdot \Gamma(1 + 1/\beta) \approx 177\,000$ год;
- гамма-розподіл: $T_{cp} (MTTF) k = 3$, $\lambda = 1/80\,000$; $k/\lambda = 3 \times 80\,000 = 240\,000$ год;
- нормальний: $\mu = 200\,000$, σ – змінюється.

Попри те, що точні значення МТТФ трохи відрізняються (у межах $\pm 20\%$ цільового значення), така параметризація дає змогу валідно порівнювати $\lambda(t)$ для візуалізації ефекту старіння та потенційного недооцінювання PFH. Водночас саме характер змін $\lambda(t)$ демонструє суттєву відмінність у ризику, що підкреслює обмеженість експоненціального розподілу як універсального нормативного підходу до оцінювання безпеки в реальних системах керування рухом поїздів.

Висновки

1. Графіки коефіцієнтів $Ratio(t)$ та інтервальних відношень імовірностей небезпечних відмов є ефективними інструментами для виявлення критичних інтервалів ризику, зокрема у випадках недооцінювання або переоцінювання функціональної безпеки залежно від вибраного закону розподілу.

2. Протягом більшості життєвого циклу систем залізничної автоматики спостерігають суттєве недооцінювання ймовірностей небезпечних відмов з використанням експоненціального закону:

- п'ять-сім разів — для нормального розподілу;
- 1,5–3,5 рази — для інших «істинних» (неекспоненціальних) моделей.

3. У випадку дуже вузького нормального розподілу ($\sigma = 1000$ год), що моделює високостабільні, масово протестовані

системи, недооцінювання ризику може сягати 80 разів у піковій зоні. Проте через фізичну неприйнятність нормального закону для часу до відмов його не слід застосовувати для нормативного оцінювання PFH.

4. У першій чверті життєвого циклу експоненціальна модель може демонструвати переоцінювання ризику, що створює ілюзію додаткового запасу безпеки. Однак ця ситуація триває лише 20–25 % терміну експлуатації, після чого ризик стрімко зростає, і експоненціальний підхід починає критично недооцінювати ризик.

5. Якщо реальний розподіл має змінну (зростаючу) інтенсивність відмов $\lambda(t)$, як у випадку старіння, використання сталої λ призводить до суттєвих помилок у визначенні нормативних показників функціональної безпеки PFH та PFD.

6. Для систем, де максимальна ймовірність відмови припадає на середню частину ресурсу (нормальний, вейбулівський із $\beta \approx 2$), застосування експоненціального розподілу веде до критичного недооцінювання ризику.

7. Експоненціальний розподіл, хоча і зручний для обчислювання, слід застосовувати лише після перевірки відповідності реальному розподілу відмов. Його беззастережне використання без валідації може призвести до хибних рішень у контексті SIL-аналізу та сертифікації.

8. У разі неможливості використання реальних розподілів відмов для визначення функціональної безпеки рекомендовано з урахуванням проведеного дослідження вводити коефіцієнт запасу (підвищеної жорсткості вимог) для рівнів SIL1-SIL4 на старіння і знос пристроїв автоматизації.

Список використаних джерел

1. Sergii Panchenko, Anatolij Bojnik, Viktor Kustov, Vasyl Sotnyk. Ensuring railroad's digital automation systems resistance to dangerous states. *ICTE in Transportation and Logistics*. 2019. IC Tol 2019. LNITI. P. 120-128. 2020. https://doi.org/10.1007/978-3-030-39688-6_17.

2. Кустов В. Ф. Разработка требований функциональной безопасности для устройств железнодорожной автоматики. *Вестник Белорусского государственного университета железнодорожного транспорта. Наука и транспорт*. 2020. Вып. 2(41). С. 28-30. <http://lib.kart.edu.ua/handle/123456789/21030>.
3. Удосконалення якості оцінки функціональної безпеки систем залізничної автоматики за наявності кратних небезпечних відмов у каналах резервування / О. А. Бунчуков, В. Ф. Кустов, С. В. Панченко, В. О. Сотник. *Інформаційно-керуючі системи на залізничному транспорті*. 2023. 28(2). С. 55-62. <https://doi.org/10.18664/ikszt.v28i2.283281>.
4. Кустов В. Ф. Математические модели функциональной безопасности микропроцессорных систем железнодорожной автоматики. *Зб. наук. праць УкрДАЗТ*. Харків: УкрДАЗТ, 2010. Вип. 116. С. 65-71.
5. Кустов В. Ф. Математичні моделі функційної безпечності та безвідмовності відновлюваних технічних засобів у разі використання мажоритарного резервування «2» із «3». *Збірник наук. праць Донецького інституту залізничного транспорту*. 2010. № 3. С. 5-14. <http://lib.kart.edu.ua/handle/123456789/20832>.
6. ДСТУ 4178-2003. Комплекси технічних засобів систем керування та регулювання руху поїздів. Функційна безпечність і надійність. Вимоги та методи випробовування. Київ: Держспоживстандарт України, 2003. 32 с.
7. ДСТУ EN 50126-1:2015 ук. Залізничний транспорт. Специфікація та демонстрація надійності, доступності, безпеки і ремонтпридатності (РАМН). Ч. 1. Основні вимоги та загальний процес (EN 50126-1:1999, IDT).
8. ДСТУ EN 50129:2015 ук. Залізничний транспорт. Системи зв'язку сигналізації та оброблення даних. Електронні сигналізаційні системи безпеки (EN 50129:2003, IDT).
9. IEC 61508-2:2000. Functional safety of electrical/electronic/programmable electronic safety-related systems.
10. CENELEC - EN 50129. Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. 2018.
11. Кустов В. Ф. Особенности обеспечения функциональной безопасности микропроцессорных систем управления и контроля на железнодорожном транспорте. *Залізничний транспорт України*. 2015. № 1. С.22- 30.
12. Кустов В. Ф. Основы теории надійності та функційної безпечності систем залізничної автоматики: навч. посіб. Харків: УкрДАЗТ, 2008. 217 с. URL: <http://lib.kart.edu.ua/handle/123456789/8481>.

Кустов Віктор Федорович, кандидат технічних наук, доцент кафедри автоматики та комп'ютерного телекерування рухом поїздів, Український державний університет залізничного транспорту.
ORCID iD: 0000-0002-9773-5470. Тел.: +38(057) 730-10-32. E-mail: kustov.vf@kart.edu.ua.

Kustov Viktor, PhD (Tech). Associate professor, department of automation and computer telecontrol of trains, Ukrainian State University of Railway Transport. ORCID iD: 0000-0002-9773-5470. Tel.: +38(057) 730-10-32. E-mail: kustov.vf@kart.edu.ua.

Статтю прийнято 30.06.2025 р.