ОЦІНКА ЙМОВІРНОСТІ НЕБЕЗПЕЧНИХ ВІДМОВ В СИСТЕМАХ УПРАВЛІННЯ БЕЗПЕКОЮ МАШИН І МЕХАНІЗМІВ

Каштанов С. Ф., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Анотація. Визначені основні особливості застосування за стандартом IEC 62061 так званого спрощеного підходу щодо виконання процедури оцінки ймовірності виникнення небезпечних відмов пов'язаних з безпекою електричних, електронних та програмованих електронних систем управління (ПБЕСУ) машин і механізмів.

Ключові слова: система управління, безпека, машини, механізми.

Abstract. Identification of the main features of the application of the simplified approach (according to IEC 62061) to determine the likelihood of dangerous failures of electrical, electronic and programmable electronic safety management systems of machines and mechanisms.

Keywords: control system, safety, machines, mechanisms.

Вступ. Імплементація європейського та національного законодавств в сфері промислової безпеки передбачає узгодження питань технічного регулювання та приведення існуючої в Україні нормативної бази з безпеки промислового обладнання та продукції у відповідність до існуючих європейських та міжнародних стандартів, що регламентують вимоги безпеки при їх проектуванні, виробництві та експлуатації, включаючи і вимоги безпеки при проектуванні пов'язаних з безпекою систем управління.

Аналіз стану питання. Основними нормативними документами, що регламентують вимоги безпеки з розробки, проектування та експлуатації машин і механізмів є Directive 2006/42/EC і діючі у цій сфері технічні регламенти та стандарти EN ISO 12100-1/2, EN 954-1 (ДСТУ EN 954-1: 2003), EN ISO 13849-1 (ДСТУ EN ISO 13849-1-2016) та IEC 62061 [1-6].

Як бачимо, на основі стандарту ISO 13849-1 на даний час вже розроблений національний стандарт ДСТУ EN ISO 13849-1:2016 «Безпечність машин. Деталі систем управління, пов'язані з забезпеченням безпеки. Частина 1. Загальні принципи проектування». Нажаль цього не можна сказати про стандарт IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems» - «Безпека машин. Функціональна безпека, що пов'язана з безпекою електричних, електронних та програмованих електронних систем управління» [6], який на даний час є основним стандартом щодо проектування пов'язаних з безпекою електричних, електронних або програмованих електронних систем управління (ПБЕСУ), на відміну від стандарту ISO 13849-1, який регламентує вимоги безпеки щодо проектування лише електромеханічних систем управління.

Хоча стандарт IEC 62061 і був розроблений як альтернатива стандарту EN ISO 13849-1, але тільки комплексне використання цих двох стандартів, а саме IEC 62061 та EN ISO 13849-1, і дозволяє створювати високоефективні, з точки

зору безпеки, системи управління промислового обладнання. Безумовно, що визначення основних особливостей функціонування та застосування стандарту IEC 62061 і його імплементація у національне законодавство у сфері промислової безпеки є на даний час першочерговою задачею, яку необхідно як найшвидше вирішувати.

Одним з основних завдань при проектуванні пов'язаних з безпекою електричних, електронних або програмованих електронних систем управління (ПБЕСУ) є виконання процедури оцінки ймовірності виникнення небезпечних відмов цих систем.

Мета роботи: визначення основних особливостей застосування за стандартом IEC 62061 так званого спрощеного підходу щодо виконання процедури оцінки ймовірності виникнення небезпечних відмов пов’язаних з безпекою електричних, електронних та програмованих електронних систем управління (ПБЕСУ) машин і механізмів.

Методики, матеріали і результати досліджень.

Розглянемо основні особливості викладеного у стандарті IEC 62061 [6] спрощеного підходу щодо оцінки імовірності небезпечних випадкових відмов апаратних засобів для базових архітектур підсистем, що використовуються у ПБЕСУ, а також відповідні формули, які можуть бути використані для підсистем, виконаних з елементів як низької, так і високої складності.

По суті, ці формули є спрощеними виразами теорії аналізу надійності та призначені для виконання розрахунків, пов'язаних з безпекою. Всі формули, що приведені нижче, є справедливими при виконанні наступної умови: $1 >> \lambda \cdot T_1$, де: λ – загальна інтенсивність відмов; T_1 – найменше значення з інтервалу значень між контрольними перевірками або терміну служби для підсистем, що працюють в режимі з високою частотою запитів.

Якщо для електромеханічних пристроїв інтенсивність відмов визначається за допомогою величини B_{10} , яка характеризує кількість робочих циклів, коли кількість компонентів, що відмовили, досягає 10% із числа робочих циклів C, заданих для застосування, то при оцінці небезпечних випадкових відмов апаратних засобів підсистем використовуються наступні характеристики:

$PFH_D = \lambda_D \cdot 1\ год.$ - середня ймовірність небезпечних відмов за годину;

DC - охоплення діагностикою;

T_1 - інтервал між контрольними перевірками або термін служби (в залежності від того, що менше);

T_2 - інтервал діагностичних перевірок;

β – так званий бета-фактор, який характеризує сприйнятливість до відмов із загальної причини;

$\lambda = \lambda_S + \lambda_D$, - загальна інтенсивність відмов;

λ_S - інтенсивність безпечних відмов;

λ_D - інтенсивність небезпечних відмов;

$\lambda_D = \lambda_{DD} + \lambda_{DU}$, де λ_{DD} - інтенсивність виявлених (знайдених) небезпечних відмов; λ_{DU} - інтенсивність не виявлених (не знайдених) небезпечних відмов;

$$\lambda_{DD} = \lambda_D \cdot DC;$$
$$\lambda_{DU} = \lambda_D \cdot (1 - DC).$$

**Примітка: Для рівнянь (A) - (D), які будуть розглянуті нижче, інтенсивність відмов елементів підсистеми (λ) передбачається постійною і достатньо низькою (1 >> λ · T), а це означає, що середній час між небезпечними відмовами має бути набагато більше інтервалу між контрольними перевірками або терміну служби підсистеми. Саме тому можна використовувати наступне основне рівняння:*

$$\lambda = 1/MTTF,$$

де: MTTF – середній час напрацювання на відмову.

Базова архітектура підсистеми типу А (стійкість до відмов дорівнює нулю, без функції діагностики)

У даній архітектурі будь-який небезпечна відмова елемента підсистеми викликає відмову ПБФУ. Для архітектури типу А (рис.1) ймовірність небезпечної відмови підсистеми дорівнює сумі ймовірностей небезпечних відмов всіх елементів підсистеми.

$$\lambda_{DssA} = \lambda_{De1} + \ldots\ldots + \lambda_{Den} \quad (1)$$
$$PFH_{DssA} = \lambda_{DssA} \cdot 1\ год.$$

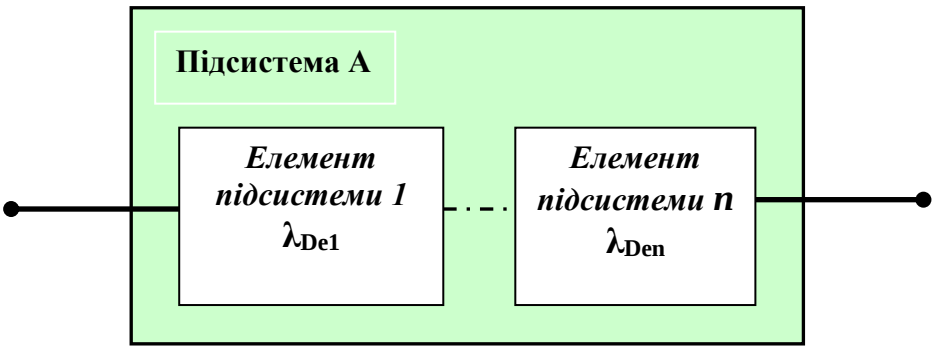

Рис.1. Логічне представлення підсистеми типу А

** Примітка: На рис.1 приведено логічне представлення архітектури підсистеми типу А, яке не повинно розглядатися як її фізична реалізація.*

Базова архітектура підсистеми типу В (стійкість до відмов дорівнює одиниці, без функції діагностики)

У даній архітектурі одиночна небезпечна відмова елемента підсистеми не викликає відмови ПБФУ. Таким чином, повинна відбутися небезпечна відмова більш ніж одного елемента перш, ніж може відбутися відмова ПБФУ. Для архітектури типу В (рис.5) ймовірність небезпечного відмови підсистеми дорівнює:

$$\lambda_{DssB} = (1 - \beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot (\lambda_{De1} \cdot \lambda_{De2})/2 \quad (2)$$
$$PFH_{DssB} = \lambda_{DssB} \cdot 1\ год.,$$

де: T_1 - інтервал між контрольними перевірками або термін служби (в залежності від того, що менше); β – бета-фактор.

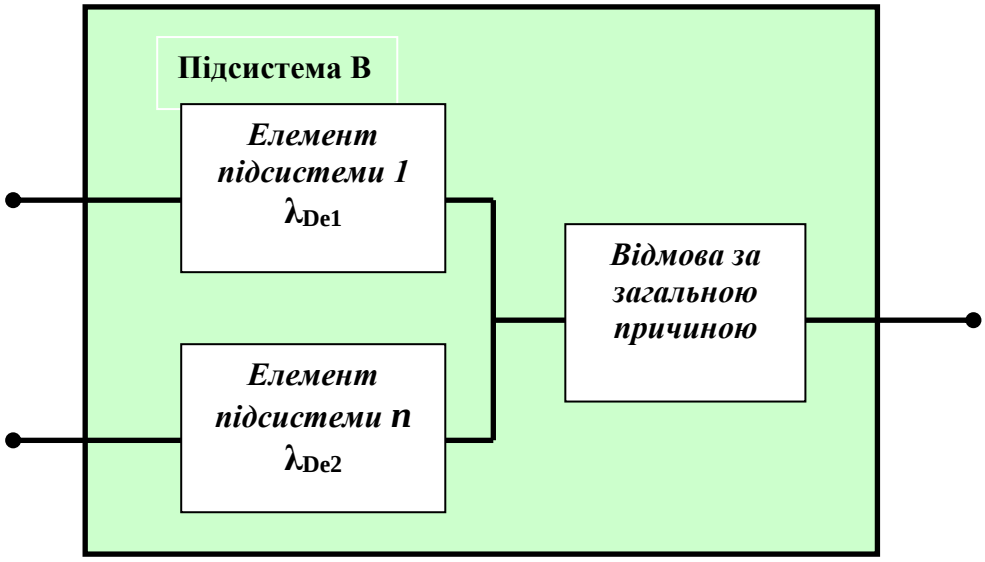

Рис.2. Логічне представлення підсистеми типу В

** Примітка: На рис.2 приведено логічне представлення архітектури підсистеми типу В, яке не повинно розглядатися як її фізична реалізація.*

Базова архітектура підсистеми типу С (стійкість до відмов дорівнює нулю, з функцією діагностики)

У даній архітектурі будь-який не виявлений небезпечний збій елемента підсистеми призводить до небезпечного відмови ПБФУ. Якщо виявлено збій елемента підсистеми, то діагностична (і) функція (ї) ініціює (ють) функцію реакції на збій.

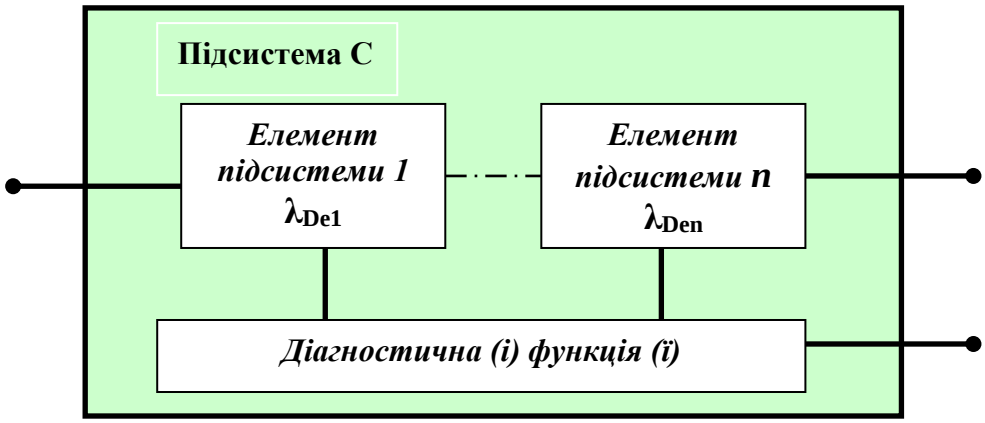

Рис.3. Логічне представлення підсистеми типу С

** Примітка: На рис.3 показано логічне представлення архітектури підсистеми типу С, яке не повинно розглядатися як її фізична реалізація.*

Показана функція діагностики може здійснюватися:

- підсистемою, що діагностується;

- іншими підсистемами ПБЕСУ;

- підсистемами, які не беруть участі у виконанні пов'язаних з безпекою функцій управління.

Для архітектури типу C (рис.3) ймовірність небезпечного відмови підсистеми дорівнює:

$$\lambda_{DssC} = \lambda_{De1} \cdot (1 - DC_1) + \lambda_{Den} \cdot (1 - DC_n)$$
$$PFH_{DssC} = \lambda_{DssC} \cdot 1 \text{ год.} \quad (3)$$

Базова архітектура підсистеми типу D
(стійкість до відмов дорівнює одиниці, з функцією діагностики)

У даній архітектурі одиночна відмова будь-якого елемента підсистеми не викликає відмови ПБФУ.

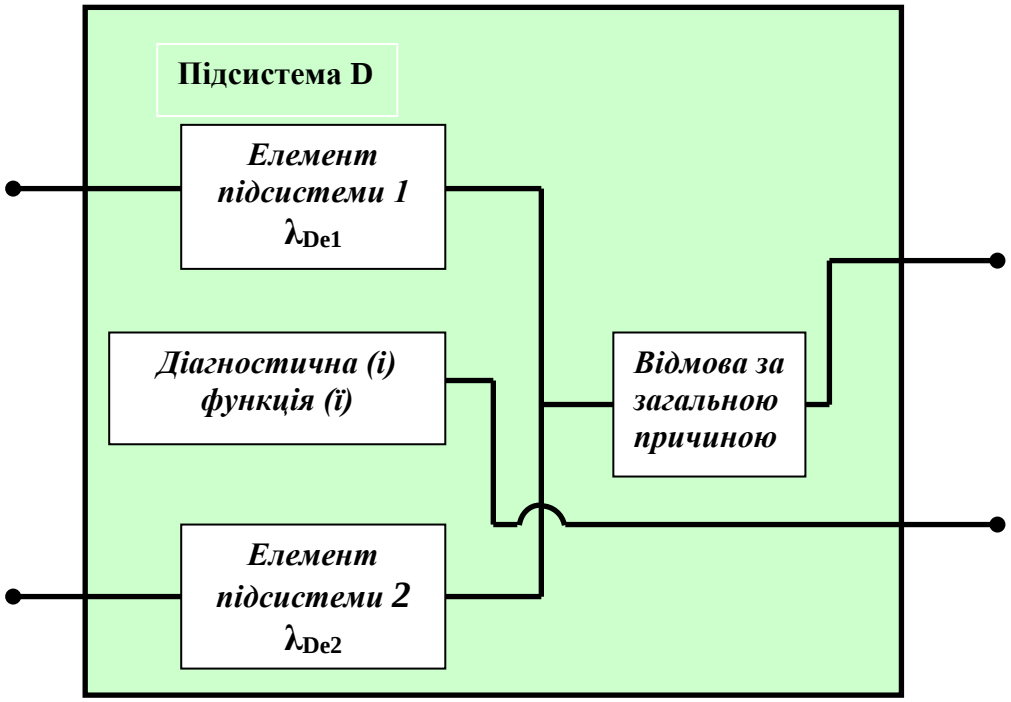

Рис.4. Логічне представлення підсистеми типу D

** Примітки:*

1.На рис.4 показано логічне уявлення архітектури підсистеми типу D, яке не повинно розглядатися як її фізична реалізація Показана функція діагностики може здійснюватися:

- підсистемою, що діагностується;

- іншими підсистемами ПБЕСУ;

- підсистемами, які не беруть участі у виконанні ПБФУ.

2. Передбачається, що реакцією на відмову такої підсистеми є припинення відповідної операції.

Для елементів підсистеми різної конструкції (рис.4):

$$\lambda_{DssD} = (1 - \beta)^2 \cdot \{[\lambda_{De1} \cdot \lambda_{De2} \cdot (DC_1 + DC_2)] \cdot T_2/2 + [\lambda_{De1} \cdot \lambda_{De2} \cdot (2 - DC_1 - DC_2)] \cdot T_1/2\} + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$$
$$PFH_{DssD} = \lambda_{DssD} \cdot 1 \text{ год.}, \quad (4)$$

де: λ_{De1} - інтенсивність небезпечних відмов 1-го елемента підсистеми; λ_{De2} - інтенсивність небезпечних відмов 2-го елемента підсистеми; DC_1 - охоплення діагностикою 1-го елемента підсистеми; DC_2 - охоплення діагностикою 2-го елемента підсистеми.

Для елементів підсистеми однакової конструкції:

$$\lambda_{DssD} = (1-\beta)^2 \cdot \{[\lambda_{De}^2 \cdot (2 \cdot DC)] \cdot T_2/2 + [\lambda_{De}^2 \cdot (1-DC)] \cdot T_1\} + \beta \cdot (\lambda_{De})$$
$$PFH_{DssD} = \lambda_{DssD} \cdot 1 \text{ год.}, \quad (5)$$

де: λ_{De} – ітенсивність небезпечних відмов 1-го або 2-го елементів підсистеми; DC - охоплення діагностикою 1-го або 2-го елементів підсистеми.

У разі реалізації функцій діагностики, кожна підсистема повинна бути забезпечена пов'язаними з нею функціями діагностики, які необхідні для виконання вимог щодо архітектурних обмежень та до ймовірності небезпечних випадкових відмов технічних засобів.

Функції діагностики розглядаються як окремі, що можуть мати відмінну від ПБФУ структуру і можуть виконуватися:

- самою підсистемою, що потребує діагностики;
- іншими підсистемами ПБЕСУ;
- підсистемами ПБЕСУ, які не виконують ПБФУ.

Функції діагностики повинні відповідати наступним вимогам, які можуть застосовуватися до пов'язаних з ними ПБФУ стосовно:

- запобігання систематичним відмовам;
- управління систематичними відмовами.

Ймовірність відмови функції (ій) діагностики ПБЕСУ повинна бути врахована при оцінці ймовірності небезпечного відмови ПБФУ.

** Примітка: Тимчасові обмеження, що застосовуються до тестування підсистеми, яка виконує функції діагностики, можуть відрізнятися від тих, які застосовуються до ПБФУ, і в загальному випадку інтервал тестування повинен відповідати вимогам, які застосовуються до підсистеми зі стійкістю до відмов апаратних засобів, що дорівнює 1.*

Повинний бути представлений чіткий та ясний опис функції (й) діагностики ПБЕСУ, їх здатності виявити відмову або їх реакції на відмову, а також повинен бути виконаний аналіз їх вкладу в повноту безпеки відповідних ПБФУ.

Для виконання спрощеного підходу при оцінці ймовірності випадкових небезпечних відмов технічних засобів підсистем застосовується наступне:

- якщо для досягнення необхідної імовірності небезпечної випадкової відмови технічних засобів необхідна функція (і) діагностики ПБЕСУ і підсистема має стійкість до збоїв апаратних засобів більше нуля, то виявлення збою і задана реакція на збій повинні бути виконані до настання небезпечної ситуації через цей збій;

- при реалізації функції (й) діагностики ПБЕСУ має бути, як мінімум, прийнято, що ймовірність випадкової відмови технічних засобів і систематична повнота безпеки однакові і дорівнюють значенню, заданому для відповідної (их) ПБФУ;

** Примітка: Обмеження архітектури на повноту безпеки апаратних засобів не застосовується при реалізації функції (й) діагностики.*

- якщо значення ймовірності небезпечної випадкової відмови технічних засобів на порядок більше, ніж задано для ПБФУ, то повинна бути виконана перевірка, щоб визначити чи будуть працездатні функції діагностики або діагностуючі пристрої. Передбачається, що така перевірка повинна бути виконана як мінімум 10 разів у проміжку між контрольними перевірками підсистеми.

** Примітки:*

1. Перевірка функції (й) діагностики повинна, наскільки це практично можливо, охоплювати на 100% ті компоненти, які реалізують функцію (і) діагностики.

2. Якщо функція діагностики реалізується логічним пристроєм ПБЕСУ, то немає необхідності окремо виконувати її тестування, так як її відмова може бути виявлена, як відмова ПБФУ.

3. Перевірка може бути виконана або зовнішніми засобами (наприклад, за допомогою випробувального обладнання), або за допомогою внутрішніх динамічних перевірок (наприклад, вбудованих в логічний пристрій) ПБЕСУ.

Оцінка імовірності небезпечних відмов (PFH_D) повинна бути заснована на імовірності випадкових небезпечних відмов апаратних засобів кожної відповідної підсистеми. Імовірність випадкових відмов апаратних засобів в ПБЕСУ є сумою ймовірностей небезпечних випадкових відмов апаратних засобів всіх підсистем (PFH_{Dn}), що беруть участь в реалізації ПБЕСУ, і включає в разі потреби імовірність небезпечних помилок цифрової передачі даних комунікаційних процесів (P_{TE}):

$$PFH_D = PFH_{D1} + \ldots\ldots + PFH_{Dn} + P_{TE} \qquad (7)$$

** Примітки:*

1. Даний підхід заснований на визначенні функціонального блоку, тобто відмова будь-якого функціонального блоку може призвести до відмови ПБФУ.

2. Взаємодії, відмінні від цифрової передачі даних, вважаються частиною підсистем.

Висновки. Визначенні основні особливості застосування за стандартом IEC 62061 так званого спрощеного підходу щодо виконання процедури оцінки ймовірності виникнення небезпечних відмов пов’язаних з безпекою електричних, електронних та програмованих електронних систем управління (ПБЕСУ) машин і механізмів.

Приведені в даній роботі матеріали повинні допомогти інженерно-технічним працівника щодо запровадження у процес проектування та виготовлення промислового обладнання стандарту IEC 62061, який регламентує вимоги безпеки при проектуванні та розробці пов'язаних з

безпекою електричних, електронних та програмованих електронних систем управління.

Література

1. Machinery Directive: Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006. / Official Journal of the European Union — 09.06.2006. — L157. — pp. 24-86.
2. Постанова КМ України від 30 січня 2013 р. № 62 про затвердження Технічного регламенту безпеки машин (із змінами, внесеними згідно з Постановою КМ № 632 віл 28.08. 2013 року).
3. EN ISO 12100-1/2 «Safety of machinery General principles for design and risk evaluation. Basic concepts.».
4. ДСТУ EN 954-1:2003 «Безпечність машин. Елементи безпечності систем керування. Частина 1. Загальні принципи проектування».
5. ДСТУ EN ISO 13849-1:2016 «Безпечність машин. Деталі систем управління, пов’язані з забезпеченням безпеки. Частина 1. Загальні принципи проектування».
6. IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems».