ОЦІНКА ПОВНОТИ БЕЗПЕКИ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМ ОБЛАДНАННЯМ

Каштанов С. Ф., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Денисюк О. В., інженер (ДП «Ітон Електрик»)

Процес розробки та проектування пов'язаних з безпекою систем управління промисловим обладнанням передбачає обов'язкове виконання вимог Directive 2006/42/EC і діючих у цій сфері стандартів EN ISO 12100-1/2, EN ISO 13849-1 (ДСТУ EN ISO 13849-1- 2016), IEC 61508 та IEC 62061 [1-5].

Основним стандартом, який визначає вимоги безпеки до електричних, електронних та програмованих електронних систем управління промисловим обладнанням є 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» [5].

**Примітка: Рівень безпеки згідно IEC 62061 визначається трьома рівнями так званої повноти безпеки SIL - «Safety Integrity» (1, 2, 3).*

Мета роботи - визначення основних вимог стандарту IEC 62061 щодо проведення процедури оцінки повноти безпеки для систем управління промисловим обладнанням.

Слід зазначити, що рівень повноти безпеки (РПБ), який може бути досягнутий у пов'язаній з безпекою електричній, електронній або програмованій електронній системі управління (ПБЕСУ), повинен розглядатися окремо для кожної пов'язаної з безпекою функцією управління (ПБФУ), що виконується ПБЕСУ. РПБ визначається ймовірністю небезпечних випадкових відмов технічних засобів, а також архітектурними обмеженнями і систематичної повнотою безпеки підсистем, які входять до складу ПБЕСУ. Таким чином, досягнутий РПБ буде менше або дорівнюватиме найменшому значенню граничної вимоги до РПБ будь-якої з підсистем для існуючих архітектурних обмежень і систематичної повноти безпеки.

Імовірність небезпечного відмови кожної ПБФУ через випадкові небезпечні відмови технічних засобів повинна бути менше або дорівнювати цільовій величині відмов, заданої в специфікації вимог до безпеки. Цільові значення відмов, що пов'язані з РПБ наведені в таблиці 3.

Імовірність небезпечного відмови кожної СБФУ через випадкові відмови технічних засобів повинна бути оцінена з урахуванням:

a) архітектури ПБЕСУ, оскільки це стосується кожної розглянутої ПБФУ;

b) частоти відмов кожної підсистеми для функціональних блоків, які вона реалізує, в будь-яких режимах, що здатні викликати небезпечну відмову ПБЕСУ.

Оцінка імовірності небезпечних відмов 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}):

$$PFH_D = PFH_{D1} + \ldots\ldots + PFH_{Dn} + P_{TE}$$

** 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.

РПБ, який досягається ПБЕСУ у відповідності з архітектурними обмеженнями, менше або дорівнює найменшому значенню граничного вимоги до РПБ будь-якої з підсистем, що беруть участь у виконанні ПБФУ.

Наприклад, ПБЕСУ, що складається з двох послідовно з'єднаних підсистем (підсистема 1 і підсистема 2), у яких частка безпечних відмов (ЧБВ) і стійкість до відмов дорівнюють значенням, що вказані у таблиці 1.

Таблиця 1

Характеристики підсистем 1 і 2 (приклад з оцінки РПБ).

Підсистема	**Стійкість до відмов технічних засобів**	**ЧБВ**	**Граничні вимоги до РПБ відповідно до обмежень архітектури**
1	1	95%	УПБ 3
2	1	80%	УПБ 2

Оцінка PFH_D для ПБЕСУ - $8 \cdot 10^{-8}$, що відповідає РПБ 3. Проте, архітектурне обмеження підсистеми 2 лімітує РПБ, яке може бути досягнуто ПБЕСУ, до УПБ 2.

Таким чином, показники безпеки підсистеми характеризуються граничними вимогами до РПБ, що визначаються її архітектурними обмеженнями, граничною вимогою до РПБ для систематичної повноти і ймовірністю випадкових небезпечних відмов апаратних засобів.

** Примітки:*

1. Граничну вимогу до РПБ підсистеми встановлює граничне значення для максимального рівня повноти безпеки, яке може бути затребуване ПБФУ, що реалізовується цією підсистемою.

2. Інформація про всі три аспекти необхідна для визначення РПБ, який досягається ПБЕСУ, що реалізує відповідну ПБФУ.

Найбільш високий рівень повноти безпеки апаратних засобів, який може знадобитися для виконання функції безпеки, обмежується стійкістю до відмов

апаратних засобів і часткою безпечних відмов підсистем, які виконують цю пов'язану з безпекою функцію управління.

Найбільший рівень повноти безпеки, який може знадобитися для ПБФУ, яку реалізує підсистема з урахуванням стійкості до відмов апаратних засобів і частки безпечних відмов цієї підсистеми, визначається за допомогою таблиці 2.

Таблиця 2

Архітектурні обмеження підсистеми. Максимальне значення РПБ, яке може бути досягнуто цією підсистемою

Частка безпечних відмов	**Відмовостійкість апаратних засобів**		
	N=0	*N*=1	*N*=2
< 60 %	Не обмовляється	РПБ 1	РПБ 2
60 % - 90 %	РПБ 1	РПБ 2	РПБ 3
90 % – 99 %	РПБ 2	РПБ 3	РПБ 3 (див. Примітку 2)
≥ 99 %	РПБ 3	РПБ 3 (див. Примітку 2)	РПБ 3 (див. Примітку 2)

** Примітки*

1. Відмовостійкість апаратних засобів N означає, що N + 1 відмова призведе до втрати пов'язаної з безпекою функції управління.

2. РПБ 4 в якості граничної вимоги в цьому стандарті не розглядається. Про РПБ 4 див. IEC 61508-1.

3. Виняток: для підсистеми зі стійкістю до збоїв апаратних засобів, що дорівнює нулю, в якій виключення збою може привести до небезпечної відмови, граничне вимога до РПБ через обмеження щодо архітектури такої підсистеми обмежена максимальним значенням РПБ 2.

Обмеження архітектури, наведені в таблце 2, повинні застосовуватися в кожній підсистемі відповідно до наступних вимог:

a) стійкість до відмов апаратних засобів N означає, що відмова N + 1 може привести до втрати ПБФУ (при визначенні стійкості до відмов не повинні враховуватися засоби, які могли б керувати впливом помилок, наприклад, засоби діагностики);

b) якщо одна помилка безпосередньо призводить до однієї або більше наступним, то її розглядають як одиночну помилку;

c) у визначенні стійкості до відмов апаратних засобів деякі помилки можуть бути виключені за умови, що імовірність їх виникнення дуже мала по відношенню до вимог повноти безпеки підсистеми (будь-які винятки помилок повинні бути обгрунтовані і документально оформлені).

Обмеження архітектури згідно з таблицею 2 повинні застосовуватися до кожної підсистемі, що реалізує функціональний блок ПБФУ.

Якщо система розроблена відповідно до ISO 13849-1 і її підтвердження відповідності виконано згідно з ISO 13849-2, то в контексті архітектурних обмежень можуть бути застосовані тільки наступні співвідношення відповідно до таблиці 3.

** Примітка: Для досягнення необхідного РПБ слід також виконати вимоги до ймовірності небезпечних відмов і систематичної повноті безпеки.*

Таблиця 3

Архітектурні обмеження. Зв'язок категорій з граничними вимогами по РПБ.

Категорія	**Стійкість до відмов апаратних засобів**	**Частка безпечних відмов (ЧБВ)**	**Максимальне значення граничної вимоги до РПБ, що відповідає обмеженням архітектури**
	Передбачається, що підсистеми з вказаною категорією мають характеристики, наведені нижче		
1	0	< 60 %	див. Примітку 1
2	0	60 % - 90 %	РПБ 1
3	1	< 60 %	РПБ 1
	1	60 % - 90 %	РПБ 2
4	>1	60 % - 90 %	РПБ 3 (див. Примітку 3)
	1	>90 %	РПБ 3 (див. Примітку 4)

* Примітки:

1. Вважається, що підсистеми категорій 1 і 2, у яких ЧБВ <60%, не задовольняють вимогам ISO 13849-1, тому підсистеми, розроблені відповідно до ISO 13849-1, на практиці будуть досягати значень ЧБВ більше 60%.

2. Передбачається, що для підсистем категорії 2 значення ЧБВ > 90% не буде досягнуто застосуванням вимог до її розробки, представлених в ISO 13849-1.

3.. Передбачається, що для підсистем категорії 4 охоплення діагностики буде <90%, якщо стійкість до відмов апаратних засобів (накопиченим відмовам) більше одиниці.

4. Підсистема категорії 4 вимагає значення ЧБВ більше 90%, якщо стійкість до відмов апаратних засобів такої підсистеми дорівнює одиниці.

5. Вважається, що підсистема категорії В, яка задовольняє вимогам ISO 13849-1, не досягає РПБ 1.

Для визначення граничних вимог до РПБ з урахуванням архітектурних обмежень, де це необхідно, повинна бути виконана оцінка ЧБВ.

При оцінці ЧБВ для кожної підсистеми повинен бути проведений аналіз (наприклад, аналіз дерева відмов, видів і наслідків відмов), щоб визначити всі відповідні відмови і їх види. Чи є відмова безпечною або небезпечною, залежить від ПБЕСУ і виконуваних ПБФУ, включаючи функцію реакції на відмову. Імовірність кожного виду відмови повинна бути визначена на підставі ймовірності виникнення пов'язаного (их) з нею збою (їв) з урахуванням заданого застосування підсистеми і може бути отримано з таких джерел, як:

a) Надійні дані про інтенсивність відмов, що зібрані з урахуванням практичного досвіду виробника і пов'язані з заданим застосуванням;

b) Дані про відмову компонента з визнаних галузевих джерел і пов'язані з заданим застосуванням;

c) Дані про інтенсивність відмов, що отримані за результатами тестування і аналізу.

Виняток: Для підсистеми зі стійкістю до збоїв апаратних засобів рівною нулю, в якій виключення збою може привести до небезпечної відмови, граничне вимога до РПБ через обмеження архітектури обмежена максимальним значенням РПБ 2.

Застосування виключення збою повинно бути обгрунтовано (наприклад, шляхом аналізу) і документально оформлено.

** Примітка: Виключення збою допустимо відповідно до п.3.3 та таблицею D.5 ISO 13849-2.*

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. EN ISO 12100-1/2 «Safety of machinery General principles for design and risk evaluation. Basic concepts».

3. ДСТУ EN ISO 13849-1:2016 «Безпечність машин. Деталі систем управління, пов’язані з забезпеченням безпеки. Частина 1. Загальні принципи проектування».

4. IEC 61508-4 «Functional safety electrical/electronic/programmable electronic safety-related systems».

5. IEC 62061 «Safety of machinery – Functional safety of electrical, electronic and programmable electronic control systems».