СУЧАСНІ ВИМОГИ БЕЗПЕКИ ДО СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМ ОБЛАДНАННЯМ

Частина 2. Функціональна безпека систем управління

(Продовження. Початок див. «Проблеми охорони праці в Україні» 37(2)/2021)

О. Г. Левченко^{1*}, С. Ф. Каштанов¹

¹Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

*E-mail для листування: levchenko.opcb@ukr.net

Отримано: 31 жовтня 2021; Прийнято: 18 листопада 2021

Цитувати як: Левченко, О., Каштанов, С. (2021). Сучасні вимоги безпеки до систем управління промисловим обладнанням (Частина 2. Функціональна безпека систем управління). *Проблеми охорони праці в Україні*, 37(4), 9–15.

Мета: Аналіз та визначення основних сучасних міжнародних вимог безпеки, яких необхідно дотримуватись при проєктуванні, розробленні та експлуатації систем управління промисловим обладнанням, і підтвердження необхідності подальшого удосконалення вітчизняної нормативної бази у цій сфері. Методологія/підхід. Виконано аналітичний огляд вимог сучасних міжнародних стандартів (IEC 62061 та IEC 61508) з безпеки функціонування електричних, електронних і програмованих електронних систем управління промисловим обладнанням; наведено структурований порядок поетапної реалізації систем управління та основні особливості організації їх структур на рівні функціональних блоків та підсистем для забезпечення необхідного рівня повноти функціональної безпеки; проаналізовано особливості процесу проєктування та розробки кожної з підсистем і алгоритм його виконання; визначено порядок оцінки ймовірності небезпечних випадкових відмов апаратних засобів для рекомендованої базової архітектури підсистем (тип А, В, С і D) та самої системи управління; надані рекомендації щодо складу специфікацій вимог безпеки при проєктуванні систем управління; зазначені вимоги до програмного забезпечення. Висновки. Виконано аналіз особливостей функціонування та застосування сучасних міжнародних стандартів безпеки, яких необхідно дотримуватись при проєктуванні, розробленні та експлуатації систем управління промисловим обладнанням, переконливо підтверджує актуальність та необхідність подальшого удосконалення вітчизняної нормативної бази в цій сфері. Наслідки досліджень. Визначено сучасні вимоги щодо організації структури системи управління на рівні функціональних блоків та підсистем для забезпечення необхідного рівня повноти функціональної безпеки електричних, електронних та програмованих електронних систем управління промисловим обладнанням, а також особливості застосування алгоритмів оцінки ймовірності небезпечних випадкових відмов систем управління та їх підсистем. Практичні наслідки. Розробка та впровадження відповідних національних стандартів на основі IEC 62061 та IEC 61508 повинні прискорити подальший розвиток технічного прогресу в Україні у сфері промислової безпеки. Оригінальність/цінність. Визначенні основні особливості функціонування сучасних міжнародних стандартів безпеки, яких необхідно дотримуватись при проєктуванні, розробленні та експлуатації систем управління промисловим обладнанням; надані відповідні рекомендації щодо їх практичного застосування; обґрунтовано та підтверджено актуальність та важливість розробки відповідних гармонізованих національних стандартів на основі стандартів IEC 62061 та IEC 61508.

Ключові слова: функціональна безпека, ризики, системи управління, промислове обладнання, рівень повноти безпеки

MODERN SAFETY REQUIREMENTS FOR INDUSTRIAL EQUIPMENT MANAGEMENT SYSTEMS

Part 2. Safety indicators of control systems

(Continuation. Beginning in «Labour protection problems in Ukraine» 37(2)/2021)

О. Levchenko^{1*}, S. Kashtanov¹

¹National Technical University of Ukraine "Kiev Polytechnic Institute of the Name of Igor Sikorskiy"

*E-mail for correspondence: levchenko.opcb@ukr.net

Received: 31 October 2021; Accepted: 18 November 2021

Cite as: Levchenko, O., Kashtanov, S. (2021). Modern safety requirements for industrial equipment management systems (Part 2. Functional safety of control systems). *Labour Protection Problems in Ukraine*, 37 (4), 8–15.

Purpose: Analysis and determination of the main modern international safety requirements that must be met in the design, development and operation of industrial equipment management systems, as well as confirmation of the need for further improvement of the domestic regulatory framework in this area. Methodology/approach: Performed analysis of the requirements of modern international standards (IEC 62061 and IEC 61508) on the safety of electrical, electronic and programmable electronic control systems for industrial equipment and the existing sequence of protection against hazards; the algorithm of step-by-step realization of control systems and the basic features of the organization of their structures at the level of functional blocks and subsystems for maintenance of necessary level of completeness of functional safety are defined; the peculiarities of the process of design and development of each of the subsystems and the algorithm of its execution are analyzed; defined algorithms for estimating the probability of dangerous accidental hardware failures for the recommended basic architecture of subsystems (type A, B, C and D) and for the control system itself; provided recommendations on the composition of the specification of safety requirements in the design of control systems; reviewed software requirements. Conclusions: The analysis of the features of functioning and application of modern international safety standards, which must be observed in the design, development and operation of industrial equipment management systems convincingly confirms the relevance and need for further improvement of domestic regulations in this area. Research results: Modern requirements for the organization of the control system structure at the level of functional units and subsystems to ensure the required level of completeness of functional safety of electrical, electronic and programmable electronic control systems for industrial equipment are determined, as well as features of application of algorithms for estimating the probability of dangerous accidental failures of control systems and their subsystems. Practical implications: The development and implementation of relevant national standards based on IEC 62061 and IEC 61508 should accelerate the further development of technical progress in

Ukraine in the field of industrial safety. Originality/value: Defining the main features of the functioning of modern international safety standards, which must be observed in the design, development and operation of industrial equipment control systems; Appropriate recommendations for their practical application are provided; Substantiated and confirmed the relevance and importance of the development of relevant harmonized national standards based on the standards IEC 62061 and IEC 61508.

Key words: functional safety, risks, control systems, industrial equipment, safety integrity level.

Постановка проблеми і аналіз сучасних вимог безпеки промислового обладнання

Аналіз нещасних випадків на виробництві та практичний досвід свідчать про те, що до тепер в Україні та багатьох інших країнах світу не завжди дотримуються вимог безпеки праці, а виробники промислового обладнання не завжди закладають у конструкції та системи управління цього обладнання спеціальні функції, які би забезпечували необхідний рівень безпеки його експлуатації.

Дуже часто вимогами безпеки просто нехтують при проектуванні виробничого обладнання самого різного призначення. У той же час, враховуючи зростаючий рівень існуючих технічних можливостей, а також наслідки можливих ризиків, розробники все більше намагаються все ж таки враховувати ці фактори та мінімізувати можливі ризики при експлуатації спроектованого обладнання. Наприклад, у деяких видах зварювального обладнання, зокрема в машинах контактного точкового зварювання, що мають підвищений рівень небезпеки, застосовується пристрій дворучного вмикання з електронною системою управління та контролю [1]. Це запобігає потраплянню руки оператора під зварювальний електрод, оскільки обидві руки під час вмикання зварювальної машини задіяні на її вмиканні і знаходяться на певній відстані від небезпечної зони, при цьому електронна система управління ретельно контролює дотримання оператором чинних вимог безпеки.

Враховуючи велику кількість нещасних випадків, отриманих на виробництві, стає зрозумілим, що у будь-якому виробничому обладнанні і особливо в системах його управління обов'язково повинні бути передбачені спеціальні функції безпеки, які би забезпечували при експлуатації цього обладнання дотримання обслуговуючим персоналом правил безпеки праці та запобігали ризикам стосовно можливості отримання травм та професійних захворювань.

Якщо такі системи управління не були передбачені в існуючому дотепер промислового обладнанні, то останнім часом з'явилась можливість його комплектувати спеціальними системами – компонентами безпеки виробничого обладнання, наприклад, відомої корпорації «EATON» [2]. Це дає можливість, певною мірою, забезпечити існуюче виробниче обладнання такими системами і зменшити рівні існуючих ризиків.

Як свідчить сучасний міжнародний досвід, на сьогодні вже постали до впровадження спеціальні новітні нормативні вимоги до безпеки промислового обладнання, які мають бути враховані ще на стадії його проектування та розроблення [3–8]. Так, для забезпечення прийнятних рівнів ризиків щодо можливого негативного впливу на обслуговуючий персонал небезпечних і шкідливих виробничих факторів, системи управління промисловим обладнанням, незалежно від умов їх експлуатації, мають гарантовано виконувати необхідні функції безпеки та контролю протягом усього життєвого циклу обладнання [6–11].

Метою цієї роботи є аналіз та визначення сучасних міжнародних вимог безпеки, яких необхідно дотримуватись при проектуванні, розробленні та експлуатації систем управління промисловим

обладнанням, а також підтвердження необхідності удосконалення існуючої вітчизняної нормативної бази у цій сфері.

Натепер процес проектування та розроблення будь-якого промислового обладнання передбачає обов'язкове виконання сучасних міжнародних та вітчизняних гармонізованих вимог: Directive 2006/42/EC і діючих у цій сфері технічних регламентів та стандартів EN ISO 12100-1/2, ISO 14121, EN 954-1 (ДСТУ EN 954-1), EN ISO 13849-1 (ДСТУ EN ISO 13849-1), IEC 62061 та IEC 61508.

Згідно зі стандартами IEC 62061 та IEC 61508 [7–8], пов'язанні з безпекою системи управління промисловим обладнанням повинні забезпечувати, залежно від умов їх експлуатації, обов'язкове виконання необхідних функцій безпеки (ФБ). Наприклад, це можуть бути такі ФБ, як аварійне відключення, запобігання непередбаченого запуску обладнання (повторних перезапусків), контроль знімних захисних бар'єрів /огорожень/ з блокуванням або без нього, контроль відкритих зон небезпеки, використання двопозиційних органів керування тощо. Саме виконання закладених у систему управління ФБ і гарантує забезпечення прийнятних рівнів ризиків при експлуатації промислового обладнання.

Згідно зі стандартами IEC 62061 та IEC 61508 при розробці структури (архітектури), пов'язаної з безпекою електронної системи управління (ПБЕСУ), кожна пов'язана з безпекою функція управління (ПБФУ), яка зазначена в специфікації вимог до безпеки ПБЕСУ, повинна бути структурно декомпозиційована до рівня функціональних блоків, наприклад так, як це показано на рис. 1. Необхідно, щоб така структура була документально оформлена і включала:

- опис;
- вимоги до безпеки (як функціональні вимоги, так і вимоги до повноти безпеки) для кожного функціонального блоку;
- визначення входів і виходів кожного блоку.

* Примітки:

1. Процес декомпозиції дозволяє сформувати структуру функціональних блоків, яка повністю описує функціональні вимоги і вимоги до повноти безпеки ПБФУ. Цей процес повинен бути застосований до рівня, що дозволяє встановити функціональні вимоги і вимоги до повноти безпеки для кожного функціонального блоку, який буде реалізований в підсистемі.

2. На входах і виходах кожного функціонального блоку може бути інформація, що підлягає обробці (наприклад, про швидкість, положення, режим роботи тощо).

3. Функціональні блоки представляють ПБФУ і не включають діагностичні функції ПБЕСУ (для досягнення цілей стандарту IEC 62061-1 діагностичні функції розглядаються як окремі, що можуть мати структуру, відмінну від ПБЕСУ).

При розробленні та проектуванні ПБЕСУ необхідно, щоб початкова концепція її архітектури була створена відповідно до структури функціональних блоків.

Кожен функціональний блок повинен бути реалізований відповідною підсистемою в архітектурі ПБЕСУ (одна підсистема може реалізовувати в собі більше одного функціонального блоку).

Кожна підсистема і реалізовані в ній функціональні блоки повинні бути чітко визначені.

Необхідно, щоб архітектура була документально оформлена, а її підсистеми і їх взаємозв'язок були детально описані.

ПБФУ мають бути документально оформлені в специфікації вимог до системи безпеки (СВСБ).

СВСБ повинна бути перевірена, щоб забезпечити узгодженість і повноту безпеки для призначеного використання

Рисунок 1 – Декомпозиційована до рівня функціональних блоків структура (архітектура) ПБЕСУ

Вимоги до безпеки для кожного функціонального блоку мають бути сформульовані, як зазначено в специфікації вимог до безпеки відповідної ПБФУ, стосовно:

- функціональних вимог (наприклад, вхідна та вихідна інформація функціонального блоку, внутрішня логіка роботи);

- вимог до повноти безпеки.

Вимоги з безпеки для підсистеми повинні бути такими ж, як і для функціональних блоків, які вона реалізує.

Якщо система реалізує більше одного блоку, то для неї застосовується вимога з найбільшим значенням повноти безпеки.

Процес проектування і розроблення підсистеми повинен чітко дотримуватися визначеної процедури, що враховує всі аспекти, які охоплює конкретний процес. Структура цього процесу та алгоритм його виконання наведено на рис. 2.

Рисунок 2 – Структура процесу проектування і розроблення підсистеми та алгоритм його виконання

При розробленні та проектуванні ПБЕСУ необхідно також враховувати вимоги до рівнів електромагнітної (ЕМ) стійкості. ПБЕСУ повинні мати рівень стійкості відповідно до стандартів з електромагнітної сумісності (Directive 2014/30/EU) [4]. Також повинні бути враховані і вимоги з безпеки експлуатації низьковольтного електричного та електронного обладнання (Directive 2014/35/EU) [5].

При складанні специфікації вимог до повноти безпеки ПБФУ, вимоги до повноти безпеки для кожної ПБФУ повинні визначатися виходячи з оцінки можливого ризику, щоб забезпечити максимальне необхідне його зниження.

Згідно зі стандартами IEC 62061 [7] та IEC 61508 [8-9] вимога до повноти безпеки повинна надаватися у вигляді цільової величини відмов (ймовірності відмов за годину для кожної ПБФУ).

Вимоги до повноти безпеки для кожної ПБФУ повинні задаватися в термінах рівня повноти безпеки (РПБ) відповідно до таблиці 1.

Таблиця 1 – Рівні повноти безпеки.
Цільові величини відмов

Рівень повноти безпеки (РПБ)	Імовірність небезпечних відмов за годину (PFH _D)
3	$\geq 10^{-8} - <10^{-7}$
2	$\geq 10^{-7} - <10^{-6}$
1	$\geq 10^{-6} - <10^{-5}$

* Примітка: Якщо необхідна повнота безпеки ПБФУ менша ніж РПБ 1, то, як мінімум, вимоги категорії B (стандарт ISO 13849-1) повинні бути забезпечені.

Згідно із стандартом IEC 62061 структури (архітектури) систем управління машин і механізмів, які пов'язані з безпекою, визначаються базовими архітектурами підсистем, що входять до складу ПБЕСУ і можуть мати такі типи: A, B, C і D (див. відповідно рис. 3 – рис. 6).

* Примітка: На рис. 3 – рис. 6 наведено логічні представлення архітектур підсистем, типи A, B, C і D, які не повинні розглядатися як їх фізична реалізація.

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

У цій архітектурі будь-яка небезпечна відмова елемента підсистеми призводить до відмови ПБФУ.

Рисунок 3 – Логічне представлення архітектури підсистеми типу А

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

У цій 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.

Рисунок 4 – Логічне представлення архітектури підсистеми типу В

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

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

Рисунок 5 – Логічне представлення архітектури підсистеми типу С

*Примітка: Наведена функція діагностики може використовуватись:

- підсистемою, що діагностується;
- іншими підсистемами ПБЕСУ;
- підсистемами, які не беруть участі у виконанні пов'язаних з безпекою функцій управління.

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

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

Рисунок 6 – Логічне представлення архітектури підсистеми типу D

* Примітки: 1. Наведена функція діагностики може використовуватись:

- 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.

Слід зазначити, що у разі реалізації функцій діагностики, кожна підсистема має 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 (її) діагностики ПБЕСУ має бути врахована при оцінці ймовірності небезпечної відмови ПБФУ.

Також має бути представлено чіткий та ясний опис функції (її) діагностики ПБЕСУ, їх здатності виявити відмову або їх реакції на відмову, а також повинен бути

виконаний аналіз їх вкладу в повноту безпеки відповідних ПБФУ.

Розглянемо більш детально основні особливості викладеного у стандарті ІЕС 62061 спрощеного підходу щодо оцінки ймовірності небезпечних випадкових відмов апаратних засобів для існуючих базових архітектур підсистем, що використовуються у ПБЕСУ, а також відповідні формули, що 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 умови: $1 \gg \lambda \cdot T_1$, де: λ – загальна інтенсивність відмов; T_1 – найменше значення з інтервалу значень між контрольними перевірками або строку служби для підсистем, що працюють у режимі з високою частотою запитів.

При оцінці небезпечних випадкових відмов апаратних засобів підсистем використовуються характеристики:

$PFH_D = \lambda_D \cdot 1 \text{ год.}$ – 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 сприйнятливості 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 (А) – (D), які будуть розглянуті нижче, інтенсивність відмов елементів підсистеми (λ) передбачається постійною і достатньо низькою ($1 \gg \lambda \cdot T$), а це означає, що середній час між небезпечними відмовами має бути набагато більший ніж інтервал між контрольними перевірками або терміну служби підсистеми. Саме тому можна використовувати наступне основне рівняння:*

$$\lambda = 1/MTTF,$$

де $MTTF$ – середній час напрацювання на відмову.

Для електромеханічних пристроїв інтенсивність відмов визначається за допомогою величини $B10$ (число циклів, коли кількість компонентів, що відмовили, досягає 10 %) і числа робочих циклів C , заданих для застосування:

$$\lambda = 0,1 \cdot C / B10.$$

Для базової архітектури типу А (рис. 3) ймовірність небезпечної відмови підсистеми дорівнює сумі ймовірностей небезпечних відмов всіх елементів підсистеми.

$$\lambda_{DssA} = \lambda_{De1} + \dots + \lambda_{Den} \quad (\text{тип А})$$

$$PFH_{DssA} = \lambda_{DssA} \cdot 1 \text{ год.}$$

Для базової архітектури типу В (рис. 4) ймовірність небезпечної відмови підсистеми дорівнює:

$$\lambda_{DssB} = (1 - \beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot (\lambda_{De1} \cdot \lambda_{De2}) / 2 \quad (\text{тип В})$$

$$PFH_{DssB} = \lambda_{DssB} \cdot 1 \text{ год.},$$

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

Для базової архітектури типу С (рис. 5) ймовірність небезпечної відмови підсистеми дорівнює:

$$\lambda_{DssC} = \lambda_{De1} \cdot (1 - DC_1) + \lambda_{Den} \cdot (1 - DC_n) \quad (\text{тип С})$$

$$PFH_{DssC} = \lambda_{DssC} \cdot 1 \text{ год.}$$

Для базової архітектури типу D (рис. 6):

- при застосуванні елементів підсистеми різної конструкції:

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

$$PFH_{DssD} = \lambda_{DssD} \cdot 1 \text{ год.},$$

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.

- при застосуванні елементів підсистеми однакової конструкції:

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

$$PFH_{DssD} = \lambda_{DssD} \cdot 1 \text{ год.},$$

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

Оцінка ймовірності небезпечних відмов (PFH_D) повинна бути заснована на ймовірності випадкових небезпечних відмов апаратних засобів кожної відповідної підсистеми.

Ймовірність 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 у разі потреби ймовірність небезпечних помилок цифрової передачі даних комунікаційних процесів (P_{TE}):

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

Необхідно зазначити, що РПБ, який досягається ПБЕСУ відповідно з архітектурними обмеженнями, повинен бути меншим або дорівнювати найменшому значенню граничної вимоги до РПБ будь-якої з підсистем, що беруть участь у виконанні ПБФУ.

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

Таблиця 2 – 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 %	РПБ 3
2	1	80 %	РПБ 2

При цьому оцінка ймовірності відмови за годину для такої ПБЕСУ дорівнює $PFH_D = 8 \cdot 10^{-8}$, що відповідає РПБ 3. Проте, архітектурне обмеження підсистеми 2 лімітує РПБ, який може бути досягнутий ПБЕСУ, до РПБ 2.

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

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 6.

Обмеження архітектури, наведені у таблиці 3, мають застосовуватися в кожній підсистемі відповідно до вимог:

Таблиця 3 – 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 оговорується	РПБ 1	РПБ 2
60 % – 90 %	РПБ 1	РПБ 2	РПБ 3
90 % – 99 %	РПБ 2	РПБ 3	РПБ 3
≥ 99 %	РПБ 3	РПБ 3	РПБ 3

* Примітки

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

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

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

б) якщо одна помилка безпосередньо призводить до однієї або більше наступних помилок, то її розглядають як одиничну помилку;

с) у визначенні стійкості до відмов апаратних засобів деякі помилки можуть бути виключені за умови, що ймовірність їх настання дуже мала відносно вимог повноти

безпеки підсистеми (будь-які винятки помилок мають бути обгрунтовані і документально оформлені).

Обмеження архітектури згідно з таблицею 3 повинні застосовуватись до кожної підсистеми, що реалізує функціональний блок ПБФУ.

Якщо система розроблена відповідно до ISO 13849-1 та її підтвердження відповідності виконано згідно з ISO 13849-2, то в контексті архітектурних обмежень можуть бути застосовані тільки співвідношення відповідно до таблиці 4.

Таблиця 4 – Архітектурні обмеження.
Зв'язок категорій з граничними вимогами за 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 ніж 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 ніж одиниця.

4. Підсистема категорії 4 потребує значення ЧБВ більшого ніж 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, має бути виконана оцінка ЧБВ.

При оцінці ЧБВ для кожної підсистеми потрібно провести аналіз (наприклад, аналіз дерева відмов, видів і наслідків відмов), щоб визначити всі відповідні відмови та їх види. Чи є відмова безпечною або небезпечною, залежить від ПБЕСУ і виконуваних ПБФУ, включно із функцією реакції на відмову.

Імовірність кожного виду відмови має бути визначена на підставі ймовірності настання пов'язаного (их) з нею збою (ів) з урахуванням заданого застосування підсистеми і може бути отримана з таких джерел, як:

- а) надійні дані про інтенсивність відмов, що зібрані з урахуванням практичного досвіду виробника і пов'язані з заданим застосуванням;
- б) дані про відмову компонента з визначених галузевих джерел і пов'язані із заданим застосуванням;
- в) дані про інтенсивність відмов, отримані за результатами тестування та аналізу.

Стосовно виконання процедури оцінки внесків відмов із загальної причини (ВЗП) до ймовірності небезпечних випадкових відмов технічних засобів підсистеми, то для цього, безумовно, потрібні знання щодо сприйнятливості підсистеми до відмов із загальної причини. Імовірність відмов із загальної причини, як правило, залежить від сполучення технології, архітектури, застосування і навколишнього середовища.

Для ефективного запобігання багатьом видам ВЗП необхідно використовувати відповідну методологію оцінки чутливості до ВЗП, яка приведена у додатку F стандарту ІЕС 62061-1. Ця методологія, що використовує простий якісний підхід для оцінки ВЗП, полягає в такому. Запропонований проєкт підсистеми необхідно оцінити, щоб встановити ефективність заходів, застосованих для захисту від ВЗП. З урахуванням таблиці 5 мають бути визначені застосовані для кожного конкретного випадку заходи, а також загальна оцінка, яка в подальшому використовується для визначення фактора ВЗП або бета-фактора (β) (у відсотках) за допомогою таблиці 6.

Таблиця 5 – Критерії оцінки ВЗП

Захід	Посилання	Оцінка
Поділ / виділення		
Чи всюди в ПБЕСУ прокладено різні сигнальні кабелі у різних каналах або чи достатньо вони екрановані?	1a	5
Де використовується інформація кодування/декодування, чи достатньо її для виявлення помилок передачі сигналу?	1b	10
Чи всі сигнальні та силові кабелі в ПБЕСУ відокремлено один від одного або чи достатньо вони екрановані?	2	5
Якщо елементи підсистеми можуть сприяти ВЗП, то чи розподілено фізичні пристрої, що їх регулюють, по окремим корпусам?	3	5
Диверсифікація / надмірність		
Чи реалізовано в підсистемах різні електричні технології, наприклад, одна підсистема електронна або програмована електронна, а інша використовує електромеханічні реле?	4	8
Чи застосовуються в підсистемі пристрої, реалізовані на різних фізичних принципах (наприклад, датчики захисних дверцят, що використовують механічні та магнітні методи вимірювання)?	5	10
Чи застосовуються в підсистемі елементи з різним часом виконання функцій і /або видів відмов?	6	10
Чи є в підсистемі елементи, які мають інтервал діагностичних перевірок ≥ 1 хв.?	7	10
Складність / конструкція / застосування		
Чи запобігає перехресний зв'язок між каналами обміну будь-якою інформацією, крім тієї, що використовується для діагностичного тестування?	8	2
Оцінка/аналіз		
Чи були вивчені результати аналізу видів впливу відмов для того, щоб встановити джерела відмов із загальної причини, і чи усунено при проєктуванні попередньо відомі джерела відмов із загальної причини?	9	9
Чи всі можливі відмови були повністю проаналізовані та враховано в проєкті?	10	9
Компетентність / навчання		
Чи розуміють розробники підсистеми причини і наслідки відмов із загальної причини	11	4
Контроль стану навколишнього середовища		
Чи можливо, що елементи підсистеми будуть працювати в заданих діапазонах температури, вологості, корозії, пилу, вібрації тощо, в яких їх робота була перевірена, без використання зовнішнього контролю стану навколишнього середовища?	12	9
Чи стійка підсистема до несприятливих впливів електромагнітного випромінювання в межах, зазначених в Додатку E стандарту ІЕС 62061-1?	13	9

* Примітка: У таблиці 1 наведено альтернативні заходи (наприклад, 1a і 1b), при цьому передбачається, що претендувати на внесок до запобігання ВЗП може тільки найбільш придатна з них.

Таблиця 6 – Оцінка фактора ВЗП або бета-фактора (β)

Загальна оцінка	Фактор відмови за загальною причиною або бета-фактор (β)
< 35	10 % (0,1)
35 – 65	5 % (0,05)
65 – 85	2 % (0,02)
85 – 100	1 % (0,01)

* Примітка: Отримане значення β -фактора слід використовувати при оцінці ймовірності небезпечної відмови відповідно до вимог, викладених раніше.

Використовуючи таблицю 5, необхідно вибирати ті заходи, які впливають на проєкт підсистеми, потім скласти відповідні їм значення оцінок, щоб отримати загальну сумарну оцінку для реалізованого проєкту. Якщо можна показати, що еквівалентний ефект із запобігання ВЗП може бути досягнутий за рахунок застосування інших конкретних заходів при проєктуванні (наприклад, використання оптоізольованих пристроїв, замість екранованих кабелів), то для цього заходу також може бути заявлена відповідна оцінка і можна вважати, що вона робить такий же внесок щодо запобігання ВЗП.

Що стосується програмного забезпечення ПБЕСУ, як

вбудованого так і прикладного, то згідно з вимогами ІЕС 62061 та ІЕС 61508, якщо програмне забезпечення повинно використовуватись в частинах, пов'язаних з безпекою програмованих електронних систем управління (ПБЕСУ), які реалізують пов'язані з безпекою функції управління (ПБФУ), то потрібно розробити й документально оформити відповідну специфікацію вимог стосовно безпеки програмного забезпечення, яка повинна бути розроблена для кожної підсистеми на основі специфікації і архітектури ПБЕСУ. Алгоритм поетапної реалізації ПБЕСУ з урахуванням вимог стандарту ІЕС 61508 [8–9] наведено на рис. 7.

Рисунок 7 – Алгоритм поетапної реалізації ПБЕСУ

Специфікація вимог до безпеки програмного забезпечення для кожної підсистеми має бути отримана з урахуванням:

- 1) вимог безпеки, заданих для ПБФУ;
- 2) вимог, що впливають з архітектури ПБЕСУ;
- 3) будь-яких вимог з планування функціональної безпеки.

Ця інформація повинна бути доступна для розробника програмного забезпечення.

Специфікація вимог до безпеки програмного забезпечення має бути достатньо детальною для забезпечення виконання існуючих стадій проєктування і впровадження ПБЕСУ для досягнення необхідної повноти безпеки і повинна дозволити виконання процедури верифікації.

Висновки

Проведений у роботі аналіз особливостей функціонування та застосування сучасних міжнародних

стандартів (ІЕС 62061 та ІЕС 61508) з безпеки функціонування електричних, електронних і програмованих електронних систем управління промисловим обладнанням дозволив виокремити ті найважливіші вимоги та параметри, які необхідно забезпечити для отримання максимально високого рівня безпеки виробничого обладнання в процесі його експлуатації. Це дає можливість проєктувати системи управління виробничим обладнанням на більш якісному рівні.

Надані рекомендації щодо особливостей практичного застосування цих стандартів для забезпечення необхідного рівня повноти функціональної безпеки систем управління промисловим обладнанням також повинні сприяти підвищенню ефективності процесу проєктування таких систем. У першу чергу, це стосується: порядку поетапної реалізації систем управління та основних особливостей організації їх структур на рівні

функціональних блоків та підсистем для забезпечення необхідного рівня повноти функціональної безпеки; особливостей процесу проектування та розробки кожної з підсистем і алгоритм його виконання; порядку оцінки імовірності небезпечних випадкових відмов апаратних засобів для рекомендованої базової архітектури підсистем (тип А, В, С і D) і систем управління; особливостей складання специфікації вимог безпеки в процесі проектування систем управління; визначення вимог безпеки до програмного забезпечення тощо.

Отриманні в роботі (Частина I та Частина II) результати щодо особливостей функціонування та застосування сучасних міжнародних стандартів безпеки, яких необхідно дотримуватись при проектуванні, розробленні та експлуатації систем управління промисловим обладнанням, та надані рекомендації щодо їх практичного застосування переконливо свідчать про необхідність та актуальність подальшого удосконалення вітчизняної нормативної бази в цій сфері. У першу чергу, це стосується необхідності розробки нових національних стандартів на основі стандартів ІЕС 62061 та ІЕС 61508, які мають стати основними стандартами щодо дотримання вимог функціональної безпеки при розробці, проектуванні та експлуатації пов'язаних з безпекою електричних, електронних та електронних програмованих систем

управління (ПБЕСУ) протягом усього їх життєвого циклу і, тим самим, забезпечити більш ефективне впровадження інноваційних розробок у сфері промислової безпеки.

Відсутність національних стандартів у цій сфері, по-перше, не тільки гальмує розвиток технічного прогресу у сфері промислової безпеки, бо саме електричні, електронні та електронні програмовані системи управління промисловим обладнанням на сьогодні є найбільш перспективними і їх частка з часом буде лише збільшуватись, а по-друге, і це дуже важливо, значно ускладнює процес імплементації вітчизняного законодавства з промислової безпеки до сучасного європейського згідно із чинною угодою між країнами Європейського Союзу та Україною [12]. Без вирішення цієї задачі наша держава не в змозі буде у подальшому ефективно конкурувати на європейському та світовому ринках.

Висловлення вдячності

Автори висловлюють вдячність адміністрації університету за надання можливості проведення дослідження

Конфлікт інтересів

У авторів конфлікт інтересів, пов'язаний з цим дослідженням, відсутній.

ЛІТЕРАТУРА

1. Левченко О. Г., Каштанов С. Ф., Олейник А. П. (2019). Системы безопасности с двуручным управлением. *Сварщик*. 2. 45–49.
2. Левченко О. Г., Каштанов С. Ф., Олійник А. П. (2019). Інноваційні розробки в сфері безпеки – основа професійної підготовки випускників КПП ім. Ігоря Сікорського. *Проблеми охорони праці в Україні*: зб. наук. праць. Київ: ДУ «ННДІПБОП», Вип. 35(1). 20–24.
3. 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. 24–86/
4. Каштанов С.Ф. (2015). Особливості європейського законодавства з електромагнітної сумісності електрообладнання та радіоелектронної апаратури. *Вісник НТУУ «КПІ», Сер. Радіотехніка радіоапаратобудування*. Вип. 63. 136–143.
5. Каштанов С.Ф. (2016). Особливості європейського законодавства з безпеки радіо, телекомунікаційного та низьковольтного обладнання. *Вісник НТУУ «КПІ», Сер. Радіотехніка радіоапаратобудування*. Вип. 65. 130–141.
6. EN ISO 13849-1/-2 «Safety of machinery - Safety-related parts of control systems».
7. IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems».
8. IEC 61508 (all parts) «Functional safety electrical/electronic/programmable electronic safety-related systems».
9. Kashtanov, Serhii F., Polukarov, Yuri O., Polukarov, Oleksiy I., Mitiuk, Liudmyla O., Kachynska, Nataliia F. (2021). Specifics of modern security requirements for software of electronic machine control systems. *Incas Bulletin*, volume 13, special issue/ 87–97.
10. Егоров Ю. П., Пятаков А. И., Егоров Д. П. (2017). Обеспечение надежности интегрированных автоматизированных систем специального назначения на этапах проектирования. *Автоматизация процессов управления*. 4 (50). 4–13.
11. Стариков Д. П., Михайлов В. В., Соловьёв С. Ю. (2021). Система мониторинга и обеспечения безопасности персонала SiWatch как подсистема платформы SIMATIC WinCC Open Architecture (Siemens). *ИСУП, Сер. Функциональная безопасность*. 4(94). 23–27.
12. Угода про асоціацію між Україною з однієї сторони та Європейським Союзом і їхніми державами-членами, з іншої сторони. *Офіційний Урядовий сайт Кабінету Міністрів України*. URL: [http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_\(body\).pdf](http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_(body).pdf).

REFERENCES

1. Levchenko O. G., Kashtanov S. F., Olejnik A. P. (2019). Sistemy bezopasnosti s dvuruchnym upravlenim. *Svarshchik*, 2, 45–49.
2. Levchenko O. H., Kashtanov S. F., Oliinyk A. P. (2019). Innovatsiini rozrobky v sferi bezpeky – osnova profesiinoi pidhotovky vypuskniv KPI im. Ihoria Sikorskoho. *Problemy okhorony pratsi v Ukraini*, 35(1), 20–24.
3. Machinery Directive: Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006. *Official Journal of the European Union*, L157, 24–86.
4. Kashtanov S. F. (2015). Features of European legislation on electromagnetic compatibility of electrical equipment and electronic equipment. *Visnyk NTUU KPI, Seriya-Radiotekhnika Radioaparatobuduvannia*. I 63, 136–143.
5. Kashtanov S. F. (2016). Features of the European legislation on the safety of radio, telecommunications and low voltage equipment. *Visnyk NTUU KPI, Seriya-Radiotekhnika Radioaparatobuduvannia*. 65, 130–141.
6. EN ISO 13849-1/-2 «Safety of machinery – Safety-related parts of control systems».
7. IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems».
8. IEC 61508 (all parts) «Functional safety electrical/electronic/programmable electronic safety-related systems».

9. Kashtanov, Serhii F., Polukarov, Yury O., Polukarov, Oleksiy I., Mitiuk, Liudmyla O., Kachynska, Nataliia F. (2021). Specifics of modern security requirements for software of electronic machine control systems. *Incas Bulletin*, volume 13, special issue/ 87–97.
10. Egorov Yu. P., Pyatakov A. I., Egorov D. P. (2017). Ensuring the reliability of integrated automated systems for special purposes at the design stages // *Automation of control processes*. 4 (50). 4–13.
11. Starikov D. P., Mikhailov V. V., Soloviev S. Yu. (2021). Si Watch personnel monitoring and safety system as a subsystem of the SIMATIC Win CC Open Architecture (Siemens) platform *ISUP, Seriya-Functional safety*. 4 (94). 23–27.
12. Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part *Official Government Website of Ukraine*. URL: [http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_\(body\).pdf/](http://www.kmu.gov.ua/kmu/docs/EA/00_Ukraine-EU_Association_Agreement_(body).pdf/)

О. Г. Левченко, С. Ф. Каштанов

СОВРЕМЕННЫЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К СИСТЕМАМ УПРАВЛЕНИЯ ПРОМЫШЛЕННЫМ ОБОРУДОВАНИЕМ (Часть II. Функциональная безопасность систем управления)

Цель: Анализ и определение основных современных международных требований безопасности, которые необходимо соблюдать при проектировании, разработке и эксплуатации систем управления промышленным оборудованием, а также подтверждение необходимости дальнейшего совершенствования отечественной нормативной базы в этой сфере. Методология / подход: Выполнен аналитический обзор требований современных международных стандартов (IEC 62061, IEC 61508) по безопасности функционирования электрических, электронных и программируемых электронных систем управления промышленным оборудованием; определен структурный порядок поэтапной реализации систем управления и основные особенности организации их структур на уровне функциональных блоков и подсистем для обеспечения необходимого уровня полноты функциональной безопасности; проанализированы особенности процесса проектирования и разработки каждой из подсистем и алгоритм его выполнения; определен порядок оценки вероятности опасных случайных отказов аппаратных средств для рекомендованной базовой архитектуры подсистем (тип А, В, С и D) и самой системы управления; даны рекомендации по составлению спецификаций требований безопасности при проектировании систем управления; рассмотрены требования к программному обеспечению. Выводы: Проведенный анализ особенностей функционирования и применения современных международных стандартов безопасности, которые необходимо соблюдать при проектировании, разработке и эксплуатации систем управления промышленным оборудованием, убедительно подтверждает актуальность и необходимость дальнейшего совершенствования отечественной нормативной базы в этой сфере. Результаты исследований: Определены современные требования по организации структуры системы управления на уровне функциональных блоков и подсистем для обеспечения необходимого уровня полноты функциональной безопасности электрических, электронных и программируемых электронных систем управления промышленным оборудованием, а также особенности применения алгоритмов для оценки вероятности опасных случайных отказов систем управления и их подсистем. Практические результаты: Разработка и внедрение соответствующих национальных стандартов на основе IEC 62061 и IEC 61508 должны ускорить дальнейшее развитие технического прогресса в Украине в области промышленной безопасности. Оригинальность / ценность: Определены основные особенности функционирования современных международных стандартов безопасности, которые необходимо соблюдать при проектировании, разработке и эксплуатации систем управления промышленным оборудованием; даны соответствующие рекомендации по их практическому применению; обоснована и подтверждена важность и необходимость скорейшей разработки соответствующих гармонизированных национальных стандартов на основе стандартов IEC 62061 и IEC 61508.

Ключевые слова: функциональная безопасность, риски, системы управления, промышленное оборудование, уровень полноты безопасности.