ПРОЕКТУВАННЯ І РЕАЛІЗАЦІЯ ПОВ'ЯЗАНИХ З БЕЗПЕКОЮ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМ ОБЛАДНАННЯМ

Каштанов С. Ф., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Олійник А. П., керівник техн. відділу (ДП «Ітон Електрик»)

Проектування і реалізація пов'язаних з безпекою систем управління промисловим обладнанням повинно здійснюватися з урахуванням вимог Directive 2006/42/EC і діючих у цій сфері технічних регламентів та гармонізованих стандартів EN 954-1 (ДСТУ EN 954-1: 2003), EN ISO 13849-1 (ДСТУ EN ISO 13849-1-2016) та IEC 62061 [1-6]:

1. **EN 954-1 «**Safety of machinery SRP/CS. General principles for design» - «Безпека машин. Загальні принципи проектування».

**Примітки:*

а) Застосовується детерміністський (якісний) підхід щодо визначення показників функції безпеки;

б) для того, щоб класифікувати показники функції безпеки при роботі обладнання, використовується такий параметр, як категорія безпеки.

Категорії безпеки згідно EN 954-1 (Вимоги):

B - (Системи захисту/управління та компоненти)

1 - Додатково до "B" (Перевірені компоненти і принципи, що відповідають вимогам безпеки).

2 - Додатково до "B" (Перевірка функцій безпеки системою управління через необхідні інтервали /тестування та діагностика/).

3 - Додатково до "B" (Відмовостійкість та виявлення несправностей при відповідному рівні технічних засобів).

4 - Додатково до "B" (Відмовостійкість та виявлення несправностей, а також відсутність небезпеки накопичення несправностей).

2. **EN ISO 13849-1/-2** «Safety of machinery - Safety-related parts of control systems» - «Безпека машин - Безпека, що пов’язана з елементами систем управління».

Part 1: «General principles for design» – «Загальні принципи конструювання».

Part 2: «Validation» - «Перевірка».

**Примітки:*

а) На відміну від EN 954-1, в якому використаний детерміністський (якісний) підхід, в EN ISO 13849-1 використовується ймовірнісний підхід, що дозволяє реалізувати кількісний розгляд показників функції безпеки.

б) Для того, щоб класифікувати показники функції безпеки при роботі обладнання використовується п'ять значень рівнів експлуатаційної безпеки PL (a, b, c, d, e,), які визначаються середніми значеннями ймовірності небезпечних відмов за годину. Рівень «а»: вклад функцій управління в зниження ризику найбільш низький, а на рівні PL «е» - найбільш високий.

в) Остаточна перевірка всіх захисних заходів, що забезпечують надійне виконання передбачених функцій безпеки, є обов'язковою складовою частиною EN ISO 13849-2.

3. **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 систем управління».

**Примітка: У загальному випадку IEC 62061, як і EN ISO 12100-1, є начебто альтернативою стандарту EN ISO 13849-1. Рівень безпеки обладнання згідно IEC 62061 визначається трьома рівнями так званої повноти безпеки SIL - «Safety Integrity» (1, 2, 3).*

При визначенні показників безпеки, на додаток до стандартів EN ISO 13849-1/-2 і IEC 62061, необхідно також використовувати:

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

ДСТУ EN ISO 12100:2016 «Загальні принципи проектування та оцінки ризику. Базові концепції».

2. **EN ISO 14121-1** «Principles for risk assessment» - «Принципи оцінки ризику».

Необхідно зазначити, що застосування будь-яких захисних заходів, які використовуються для усунення існуючих небезпек та зниження рівнів можливих ризиків, повинно здійснюватися в певній послідовності у відповідності до вимог EN ISO 12100-1, що проілюстровано на рис.1.

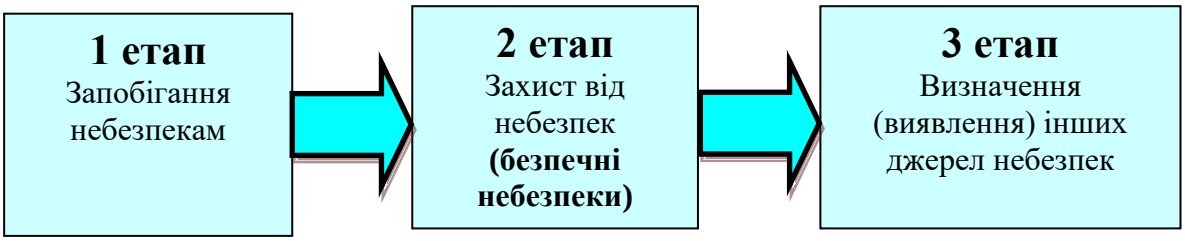

Рис.1. Послідовність виконання захисних заходів згідно з EN ISO 12100-1

1 етап. Запобігання небезпекам: усунення існуючих небезпек та зниження рівнів можливих ризиків за рахунок відповідних конструктивних заходів на етапі проектування та розробки машини.

2 етап. Захист від небезпек: зниження рівнів можливих ризиків за рахунок введення необхідних захисних заходів.

3 етап. Визначення (виявлення) інших джерел небезпек: зниження рівнів можливих ризиків за рахунок надання додаткової необхідної інформації /попереджень/ про залишкові ризики.

Якщо остаточний результат 1 етапу "Запобігання небезпекам" не призводить до достатнього зниження рівнів можливих ризиків відповідно до вимог EN ISO 12100-1, то ітераційний процес при проектуванні відповідно до

вимог ISO 13849-1 або IEC 62061 повинен бути використаний також і на 2 етапі – "Безпечні небезпеки".

Ті частини систем управління машиною, які вирішують завдання безпеки, визначені в міжнародних стандартах, як "частини, що пов'язані з безпекою в системах управління" - "safety-related parts of control systems" (SRP/CS). Відповідно до вимог обох стандартів (ISO 13849-1 та IEC 62061) необхідні функції безпеки повинні бути забезпечені саме SRP/CS.

Основними стандартами, які визначають вимоги до проектування і реалізації пов'язаних з безпекою систем управління промисловим обладнанням є стандарти IEC 62061 та ISO 13849-1.

Використання будь-якого з цих стандартів відповідно до сфер їх застосування передбачає виконання відповідних важливих вимог щодо забезпечення безпеки. У таблиці 1 приведені рекомендовані сфери застосування IEC 62061 та ISO 13849-1.

Таблиця 1.

Сфери застосування стандарті IEC 62061 и ISO 13849-1.

	Технологія реалізації пов'язаної (их) з безпекою функції (ій) управління	**ISO 13849-1**	**IEC 62061**
	Не електрична, наприклад, гідравліка	«X»	Не охоплює
	Електромеханічна, наприклад, реле або нескладні електроні пристрої	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = e	Усі архітектури і до РПБ 3
	Складні електронні пристрої, наприклад, програмовані	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = d	Усі архітектури і до РПБ 3
	A в поєднанні з B	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = e	«X» (див. Примітка 3)
	C в поєднанні з B	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = d	Усі архітектури і до РПБ 3
	C в поєднанні з A Або C в поєднанні з A і B	«X» (див. Примітка 2)	«X» (див. Примітка 3)

«X» - означає, що дану технологію регламентує стандарт, зазначений у заголовку колонки таблиці.
РБ – рівень експлуатаційної безпеки (ISO 13849-1); РПБ – рівень повноти безпеки (IEC 62061).
**Примітка:*

1. Встановлені архітектури визначені в ISO 13849-1, додаток B, де дан спрощений підхід для квантифікації рівня експлуатаційної безпеки (РБ). РБ - рівень необхідного мінімального зниження ризику.

2. Для складних електронних пристроїв використовують встановлені архітектури до РБ = d згідно ISO 13849-1 або будь-які архітектури згідно IEC 62061.

3. Елементи, засновані на неелектричній технології, згідно ISO 13849-1 використовують в якості підсистем.

Зв'язок стандарту IEC 62061 з іншими відповідними стандартами в сфері безпеки та вся необхідна інформація щодо рекомендованого застосування цього стандарту та ISO 13849 представлено на рис. 1.

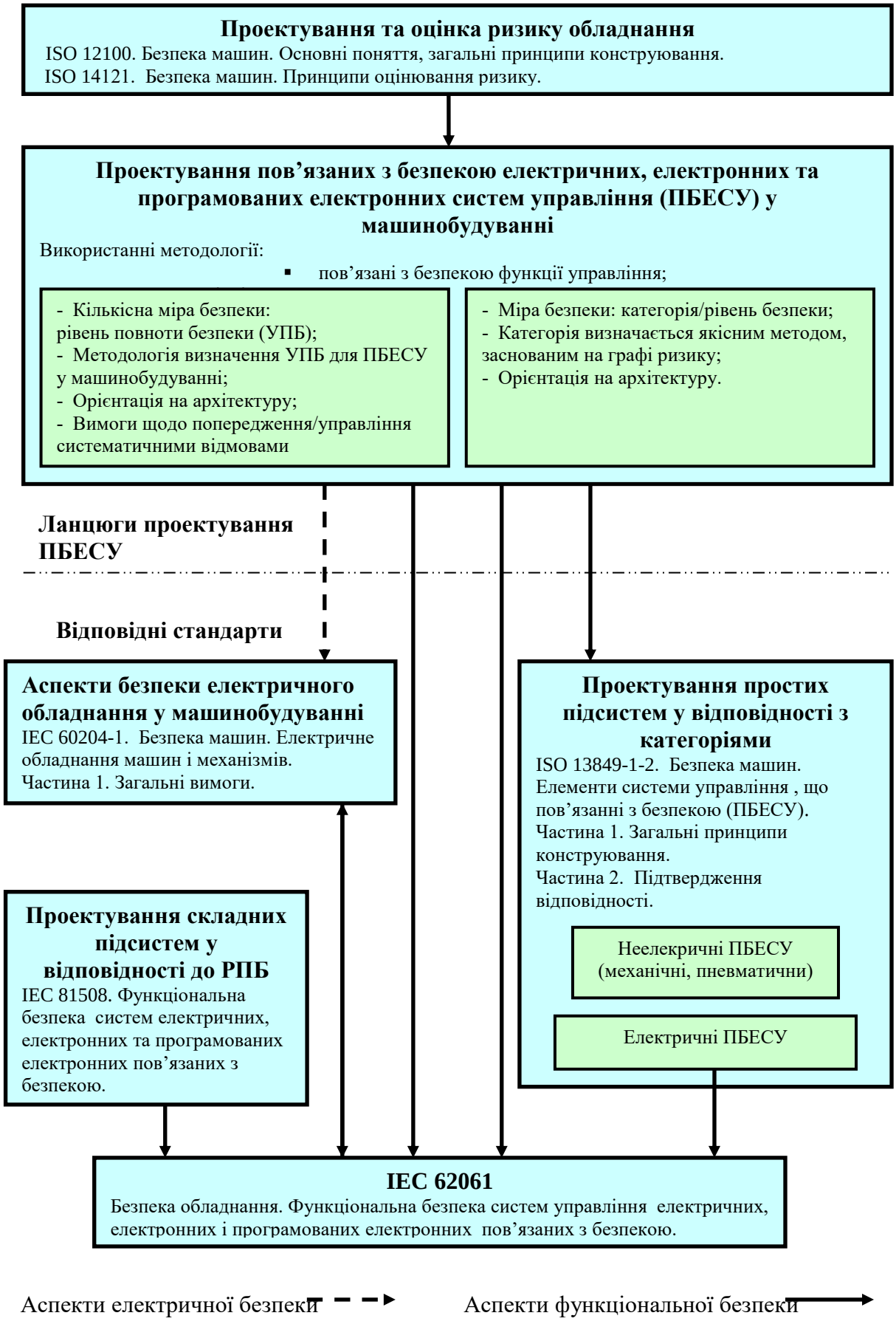
Проектування та оцінка ризику обладнання
ISO 12100. Безпека машин. Основні поняття, загальні принципи конструювання.
ISO 14121. Безпека машин. Принципи оцінювання ризику.
Проектування пов'язаних з безпекою електричних, електронних та програмованих електронних систем управління (ПБЕСУ) у машинобудуванні
Використанні методології:
пов'язані з безпекою функції управління;
- Кількісна міра безпеки:
рівень повноти безпеки (УПБ);
- Методологія визначення УПБ для ПБЕСУ у машинобудуванні;
- Орієнтація на архітектуру;
- Вимоги щодо попередження/управління систематичними відмовами
- Міра безпеки: категорія/рівень безпеки;
- Категорія визначається якісним методом, заснованим на графі ризику;
- Орієнтація на архітектуру.
Ланцюги проектування ПБЕСУ
Відповідні стандарти
Аспекти безпеки електричного обладнання у машинобудуванні
IEC 60204-1. Безпека машин. Електричне обладнання машин і механізмів.
Частина 1. Загальні вимоги.
Проектування простих підсистем у відповідності з категоріями
ISO 13849-1-2. Безпека машин.
Елементи системи управління , що пов'язанні з безпекою (ПБЕСУ).
Частина 1. Загальні принципи конструювання.
Частина 2. Підтвердження відповідності.
Неелекричні ПБЕСУ (механічні, пневматичны)
Електричні ПБЕСУ
Проектування складних підсистем у відповідності до РПБ
IEC 81508. Функціональна безпека систем електричних, електронних та програмованих електронних пов'язаних з безпекою.
IEC 62061
Безпека обладнання. Функціональна безпека систем управління електричних, електронних і програмованих електронних пов'язаних з безпекою.
Аспекти електричної безпеки
Аспекти функціональної безпеки

Рис. 1

*****Примітка****: ПБЕСУ – пов'язана з безпекою електрична система управління (Safety-Related Electrical Control System - /SRECS/), а саме електрична система управління, відмова якої може безпосередньо привести до збільшення ризику (ризиків). ПБЕСУ включає у себе усі елементи електричної системи управління, відмова якої може привести до зниження або втрати функціональної безпеки, а також може включати в себе електричні кола електроживлення та 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».