ВИМОГИ БЕЗПЕКИ ДО МАШИН, МЕХАНІЗМІВ ТА СИСТЕМ ЇХ УПРАВЛІННЯ І КОНТРОЛЮ

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

Відповідно до існуючих вимог сучасного європейського та українського законодавств у сфері безпеки машин, механізмів та систем управління і контролю [1-7], будь яке виробниче обладнання в залежності від умов його експлуатації повинно забезпечувати виконання відповідних функцій безпеки, а також мати відповідні гарантії щодо можливості їх забезпечення.

Основною метою даної роботи є визначення основних особливостей функціонування та застосування діючих стандартів з безпеки машин, механізмів та систем управління і контролю, а також надання відповідних практичних рекомендацій щодо забезпечення існуючих за даними стандартами параметрів (показників) безпеки.

Спеціалістами корпорації «EATON/MOELLER», яка є одним із лідерів у сфері виробничої та промислової безпеки, розроблені відповідні керівництва/довідники [8-9], в яких, з урахуванням вимог Directive 2006/42/EC, стандартів EN 60204-1 (ДСТУ EN 60204-1:2015), EN 954-1 (ДСТУ EN 954-1:2003), EN ISO 13849-1 (ДСТУ EN ISO 13849-1-2016), IEC 62061 та інших діючих у цій сфері гармонізованих стандартів, технічних регламентів та відповідних Директив Європейського Співтовариства, надані практичні рекомендації щодо забезпечення необхідного рівня безпеки машин, механізмів та систем їх управління і контролю, запропоновані відповідні схеми управління та заходи з безпеки при ремонті, обслуговуванні та експлуатації промислового обладнання, а також ефективні методи захисту персоналу від ураження електричним струмом.

Крім того, у відповідних розділах керівництва/довідника «EATON/MOELLER» [8] запропоновані та апробовані ефективні алгоритми визначення основних параметрів (показників) безпеки виробничого обладнання у разі застосування:

- схем аварійного відключення;
- схем запобігання непередбаченого запуску обладнання (повторних перезапусків);
- схем контролю з'ємних захисних бар'єрів /огороджень/ з блокуванням або без нього;
- схем контролю відкритих зон небезпеки;
- схем використання двопозиційних (дворучних) органів управління (типів I, II та III) тощо.

Для кожної із запропонованих в керівництві/довіднику схем управління безпекою промислового обладнання наведені характерні для них значення основних показників безпеки у відповідності до вимог EN 954-1, EN ISO 13849-1 и IEC 62061, а також приведений перелік прийнятих при цьому

допущень.

Незалежний від виробника інструмент розрахунку «SISTEMA» Інституту охорони праці та здоров'я німецького соціального страхування від нещасних випадків (IFA), який також використовується і спеціалістами «EATON/MOELLER», надає ефективну допомогу в оцінці компонентів систем управління, що пов'язані з безпекою в контексті стандарту EN ISO 13849-1, і дозволяє значно спростити аналіз та оцінку існуючих ризиків.

Згідно існуючої нормативно-правової бази, визначення параметрів (показників) безпеки виробничого обладнання повинно здійснюватися за наступними основними стандартами:

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.

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 PLs (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 наступні стандарти:

1. **EN ISO 12100-1/2 «**Safety of machinery General principles for design and risk evaluation. Basic concepts» - «Загальні принципи проектування та оцінки ризику. Базові концепції».

ДСТУ EN ISO 12100:2016 «Безпечність машин. Загальні принципи проектування оцінювання ризиків та зменшення ризиків»

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

**Примітка: 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, а саме у три етапи:*

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

2 етап – *це захист від небезпек: зниження рівнів можливих ризиків за рахунок введення необхідних захисних заходів (безпечні небезпеки).*

3 етап *– це 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 (підсистеми), 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.

Також системи управління, які пов'язані з безпекою окремих блоків обладнання, повинні забезпечувати надійне послідовне виконання наступних функцій безпеки:

- прийом вхідного сигналу безпеки (датчик);
- обробка сигналу безпеки (логіка);
- подача сигналу на виконавчі пристрої (привід).

Безумовно, що кінцева мета полягає в розробці такої системи управління і контролю, яка забезпечила би усі передбачені функції безпеки управління в разі виникнення несправностей чи аварій, а також необхідний рівень зниження можливих ризиків.

Згідно вимог EN ISO 13849-1 (EN 954-1) системи управління машин і механізмів, які пов'язані з безпекою, класифікуються за наступними категоріями:

• **Категорія B** – **базова категорія** (структура на рис. 1).

Пов'язані з безпекою елементи системи управління повинні бути, як мінімум, сконструйовані відповідно до сучасного рівня техніки і повинні протистояти очікуваним зовнішнім впливам.

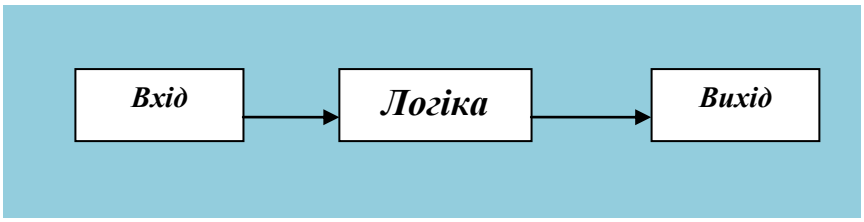

Рис.1. Структура для категорії В (одноканальна)

• **Категорія 1** (структура на рис. 2).

Пов'язані з безпекою елементи системи управління повинні бути розроблені і сконструйовані з використанням перевірених компонентів і надійних принципів безпеки.

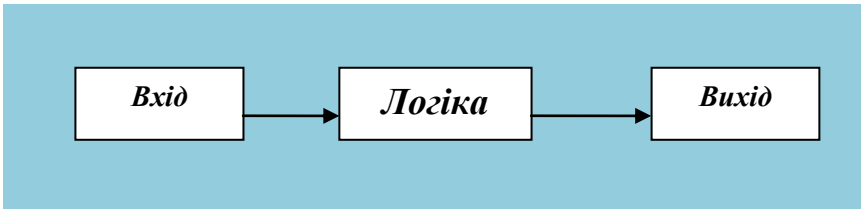

Рис.2. Структура для категорії 1 (одноканальна)

• **Категорія 2** (структура на рис. 3).

Функції елементів системи управління, які пов'язані з безпекою, повинні періодично контролюватися (тестування, діагностика) з відповідними часовими інтервалами. Як правило, тестування (діагностика) здійснюється періодично під час роботи з урахуванням аналізу існуючих ризиків. Тестування (діагностика) може здійснюватися автоматично або вручну, але обов'язково при кожному запуску і, бажано, перед виникненням можливої небезпечної ситуації.

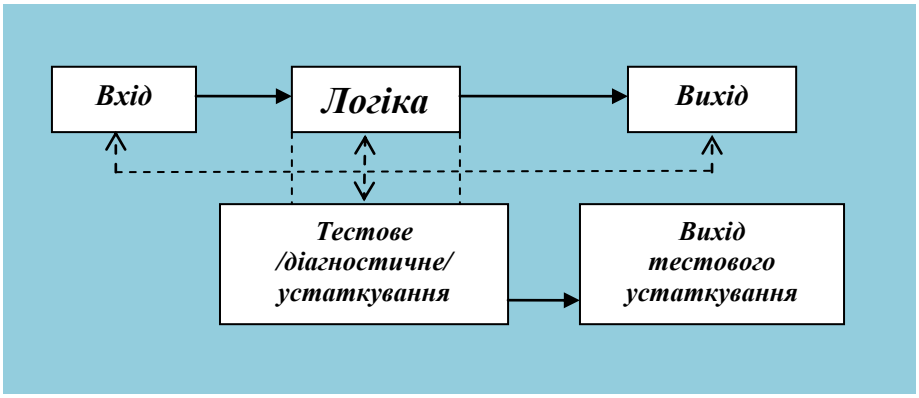

Рис.3.Одноканальна контрольована структура (категорія 2)

• **Категорія 3** (структура на рис. 4).

Одна помилка у частинах системи управління, що пов'язані з безпекою, не призводить до втрати функції безпеки всієї системи. В той же час, оскільки в системі управління не використовується функція самоконтролю і тому не всі несправності можуть бути виявлені, то накопичення таких невиявлених несправностей все ж таки може з часом викликати небезпечну ситуацію.

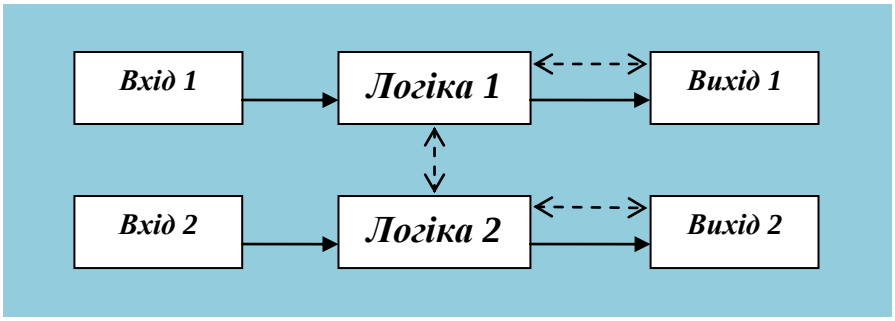

Рис.4. Двоканальна структура без функції самоконтролю (категорія 3)

• **Категорія 4** (структура на рис. 5).

Одна помилка у частинах системи управління, що пов'язані з безпекою, не призводить до втрати функції безпеки всієї системи. При використанні функції самоконтролю ця помилка повинна бути виявлена негайно або до виникнення наступної потенційної небезпеки. Якщо це неможливо, то повинні бути забезпечені умови, при яких накопичення несправностей не повинно призводити до втрати функції безпеки всієї системи управління.

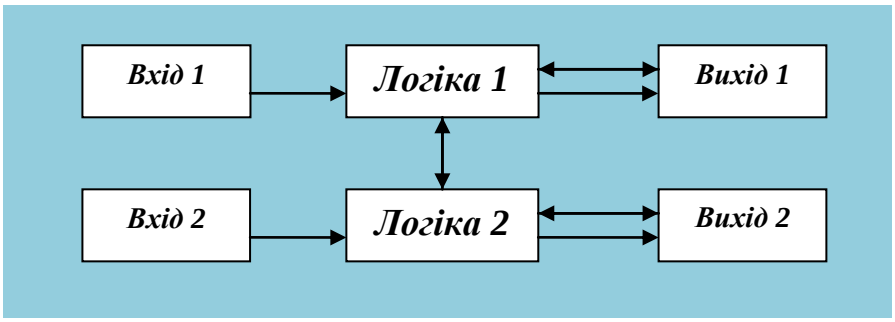

Рис.5. Двоканальна структура із функцією самоконтролю (категорія 4)

Для визначення рівня безпеки будь-якого промислового обладнання, в першу чергу, повинні бути визначенні наступні параметри (показники), що пов’язані з безпекою частин (елементів) обладнання та систем управління з урахуванням відмовостійкості апаратних засобів і використовуваних в системі управління діагностичних функцій і їх надійності. Для стандарту EN ISO 13849 (таблиця 1) це: **Structure/category**; **$MTTF_d$**; **$B10_d$**; **n_{op}**; **CCF**; **DC_{avg}**; **PL**; **$T10_d$**, а для стандарту IEC 62061 (таблиця 2) це: **Structure/category**; **PFH_d**; **B10**; **λ_d/λ**; **C**; **β**; **DC**; **SIL** (всього по 8 основних показників).

Таблиця 1.

Параметри безпеки (Safety parameters) відповідно до вимог EN ISO 13849-1

Параметр безпеки	**Примітка**
Structure /category/	Структурні вимоги /категорія/ Класифікація, що пов'язана з безпекою частин (елементів) обладнання і системи управління та визначається з урахуванням відмовостійкості апаратних засобів і використаних в системі управління діагностичних функцій і їх надійності.
$MTTF_d$ Mean Time to Dangerous Failure	Середній час напрацювання до виникнення небезпечних відмов.
$B10_d$ Number of cycles until 10% of a number of tested and worn components (e.g. electromechanical components) have failed	Кількість циклів, коли кількість компонентів, що відмовили, досягає 10% (для електромеханічних компонентів).
n_{op} Mean number of annual operations	Середнє число операцій за рік.
CCF Common Cause Failure	Відмови різних елементів (деталей), коли ці відмови відбуваються за загальною причиною - в результаті однієї (одиничної) події.
DC_{avg} Average Diagnostic Coverage	Середня величина діагностичного покриття тих функцій управління, які гарантують необхідний рівень безпеки. Забезпечує зниження ймовірності небезпечних відмов у результаті виконання автоматичних діагностичних тестів.
PL Performance Level	Рівень експлуатаційної безпеки. Дискретний рівень, який використовується для визначення здатності частин (елементів) обладнання, пов'язаних з виконанням функції безпеки системою управління, забезпечувати при передбачуваних умовах необхідний рівень безпеки. Класифікація від PL a (найвища ймовірність відмови) ... до PL e (низька ймовірність відмови).
$T10_d$ Operating time, time of use of the safety-related control function	Середній час роботи, пов'язаний із забезпеченням функцій безпеки і контролю в системі управління (це час, протягом якого 10% компонентів мають небезпечні відмови)

Таблиця 2.

Параметри безпеки (Safety parameters) відповідно до вимог IEC 62061

Параметр безпеки	**Примітка**
Structure /category, subsystem architecture/	Структурні вимоги (категорія, архітектура підсистем). Класифікація підсистем, що виконують функції управління і пов'язані з безпекою, і які мають архітектуру відповідно до IEC 62061 та виконані з урахуванням вимог до відмовостійкості апаратних засобів і використаних діагностичних функцій і їх надійності.
PFH_d Average probability of dangerous failure per hour.	Ймовірність небезпечних відмов за годину
B10 Number of cycles until 10% of a number of tested and worn components (e.g. electromechanical components) have failed	Кількість циклів, коли кількість компонентів, що відмовили, досягає 10% (для електромеханічних компонентів).
λ_d/λ Patio between the dangerous failure rate and the total failure rate proportion of dangerous failures.	Відношення інтенсивності небезпечних відмов до загальної інтенсивності відмов за годину.
C Mean number of hourly cycles.	Среднее число часовых циклов.
β Beta factor. Common cause failure factor.	Бета-фактор. Коефіцієнт відмови із загальної причини або сприйнятливість до відмов із загальної причини - в результаті однієї (одиничної) події.
DC Diagnostic Coverage.	Середня величина діагностичного покриття тих функцій управління, які гарантують необхідний рівень безпеки. Забезпечує зниження ймовірності небезпечних відмов у результаті виконання автоматичних діагностичних тестів.
SIL Safety Integrity Level	Рівень повноти безпеки. Показник рівня функції безпеки, пов'язаної з безпекою електричних компонентів системи управління машиною. Всього три рівня 1, 2 і 3. SIL1 (найнижчий рівень) ..... .SIL3 (найвищий рівень) безпеки.

Виконаний в даній роботі аналіз особливостей функціонування та застосування сучасної законодавчої бази з безпеки машин, механізмів та систем управління і контролю та наданні на його основі практичні рекомендації щодо забезпечення існуючих за даними стандартами параметрів (показників) безпеки повинні сприяти більш ефективному підвищенню загального рівня виробничої та промислової безпеки в Україні.

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. ДСТУ EN 60204-1:2015 «Безпечність машин. Електрообладнання машин. Частина 1. Загальні вимоги».

4. ДСТУ EN ISO 12100:2016 «Безпечність машин. Загальні принципи проектування оцінювання ризиків та зменшення ризиків».

5. ДСТУ EN 954-1:2003 «Безпечність машин. Елементи безпечності систем керування. Частина 1. Загальні принципи проектування».

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

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

8. Safety Manual: «Safety technology for machines and systems in accordance with the international standards EN ISO 13849-1 and IEC 62061». http://moeller.kiev.ua/rukovodstvo-po-bezopasnosti

9. Керівництво/довідник «Обладнання промислової безпеки». http://moeller.kiev.ua/images/uploads/pdf_catalogs/172/Safety_spravochnik_2004.pdf