СУЧАСНІ ВИМОГИ БЕЗПЕКИ ДО СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМ ОБЛАДНАННЯМ

(Частина I. Показники безпеки систем управління)

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: 05 травня 2021; Прийнято: 11 травня 2021

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

Мета: аналіз та визначення основних сучасних міжнародних вимог безпеки, яких необхідно дотримуватись при проєктуванні, розробленні та експлуатації систем управління промисловим обладнанням, а також підтвердження необхідності подальшого удосконалення вітчизняної нормативної бази у цій сфері. Виконано аналітичний огляд вимог сучасних міжнародних стандартів (IEC 62061, IEC 61508) з безпеки функціонування електричних, електронних і програмованих електронних систем управління промисловим обладнанням та поетапної послідовності виконання захисних заходів від наявних небезпек; визначено головні особливості побудови архітектури таких систем управління і надано алгоритми визначення основних показників їх функціональної безпеки (PL; SILPL; PFH_d) та алгоритм забезпечення необхідного рівня безпеки залежно від параметрів існуючих ризиків. Проведений 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. Визначено основні параметри (показники) безпеки функціонування електричних, електронних і програмованих електронних систем управління промисловим обладнанням. Надано рекомендації щодо основних аспектів їх застосування та реалізації відповідно до стандартів IEC 62061 та IEC 61508. Розробка та впровадження національних стандартів на основі IEC 62061 та IEC 61508 мають пришвидшити подальший розвиток технічного прогресу у сфері промислової безпеки. Підтверджено актуальність та важливість необхідності розроблення відповідних гармонізованих національних стандартів на основі стандартів IEC 62061 та IEC 61508.

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

MODERN SAFETY REQUIREMENTS FOR INDUSTRIAL EQUIPMENT MANAGEMENT SYSTEMS

(Part I. Safety indicators of control systems)

O. 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: 05 May 2021; Accepted: 11 May 2021

Cite as: Levchenko, O., Kashtanov, S. (2021). Modern safety requirements for industrial equipment management systems (Part I. Safety indicators of control systems). *Labour Protection Problems in Ukraine*, 37 (2), 9–15.

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. Performed analysis of the requirements of modern international standards (IEC 62061, 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 main features of the architecture of such control systems are identified and algorithms for determining the main indicators of their functional safety (PL; SIL PL; PFH_d) and an algorithm for ensuring the required level of security depending on the parameters of existing risks are provided. 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. The main parameters (indicators) of safety of functioning of electric, electronic and programmable electronic control systems of industrial equipment are determined. Relevant recommendations are provided on the main aspects of their application and implementation according to IEC 62061 and IEC 61508. The development and implementation of relevant national standards based on IEC 62061 and IEC 61508 should accelerate the further development of technical progress in the field of industrial safety. Confirmed relevance and importance of the need to develop relevant national standards based on IEC 62061 and IEC 61508.

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

Постановка проблеми і аналіз сучасних вимог безпеки промислового обладнання

Практичний досвід та аналіз нещасних випадків на виробництві показав, що до тепер в Україні та багатьох інших країнах світу не завжди дотримуються вимог безпеки праці, спеціально закладених у конструкціях

виробничого обладнання. Проте, слід зазначити, що і під час розроблення виробничого обладнання різного призначення вимогами безпеки часто нехтують. Однак в окремих випадках, враховуючи технічні можливості розробників, все ж таки звертали увагу на вимоги безпеки. Наприклад, у деяких видах зварювального обладнання,

зокрема в машинах контактного точкового зварювання, застосовувався пристрій дворучного вмикання [1]. Його використання запобігає потраплянню руки оператора під зварювальний електрод, оскільки обидві руки під час вмикання зварювальної машини задіяні на її вмикання та знаходяться на певній відстані від небезпечної зони.

Враховуючи велику кількість нещасних випадків на виробництві, є зрозумілим, що у будь-якому виробничому обладнанні мають бути передбачені спеціальні системи управління цим обладнанням з обов'язковим урахуванням вимог безпеки праці. Якщо такі системи не були передбачені в існуючому до тепер 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. Але зараз, як відомо із сучасного міжнародного досвіду, на часі вже є спеціальні новітні нормативні вимоги до безпеки промислового обладнання, які мають бути враховані ще на стадії його проектування та розроблення [3–9].

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 експлуатації мають гарантовано виконувати необхідні функції безпеки та контролю протягом усього життєвого циклу обладнання [3, 4].

Метою цієї роботи є аналіз та визначення сучасних міжнародних вимог безпеки, яких необхідно дотримуватись при проектуванні, розробленні та експлуатації систем управління промисловим обладнанням і підтвердження необхідності удосконалення існуючої вітчизняної нормативної бази у цій сфері.

На тепер процес проектування та розроблення будь-якого промислового обладнання передбачає обов'язкове виконання сучасних міжнародних і вітчизняних гармонізованих вимог: Directive 2006/42/EC і чинних у цій сфері технічних регламентів і 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 [1–7].

Необхідно зазначити, що застосування відповідних захисних заходів, що використовуються для усунення існуючих небезпек і зниження рівнів можливих ризиків, повинно здійснюватися в певній послідовності відповідно до вимог EN ISO 12100-1 (рис. 1).

Рисунок 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 веде до достатнього зниження рівнів можливих ризиків відповідно до вимог EN ISO 12100-1, то ітераційний процес при проектуванні промислового обладнання відповідно до вимог ISO 13849-1 або IEC 62061 має бути використаний також і на 2 етапі – «Безпечні небезпеки». Оцінювання існуючих ризиків здійснюється відповідно до стандарту ISO 14121 «Безпека машин. Принципи оцінювання ризику».

Ті частини систем управління промисловим обладнанням, які вирішують завдання безпеки, визначені в міжнародних стандартах, як «частини, що пов'язані з безпекою в системах управління» («safety-related partsof control systems») (SRP/CS). Відповідно до вимог обох стандартів (ISO 13849-1 та IEC 62061) необхідні функції безпеки мають бути забезпечені саме за рахунок SRP/CS.

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

Для того, щоб класифікувати рівні безпеки систем управління обладнанням застосовується п'ять значень рівнів безпеки (РБ) – це рівні PL (a, b, c, d, e), які залежать від здатності елементів систем управління, пов'язаних із забезпеченням безпеки, виконувати функції безпеки в передбачених обставинах. Ці рівні характеризуються відповідними значеннями середнього часу напрацювання до настання небезпечної відмови (MTTF_d) або ймовірністю небезпечної відмови за годину (PFH_d).

Рівень безпеки (РБ) PL «a» забезпечує найнижчий внесок функцій управління у зниження ризику, а рівень PL «e» – найвищий. Остаточна перевірка всіх захисних заходів, що забезпечують надійне виконання передбачених функцій безпеки (ФБ), є обов'язковою складовою частиною EN ISO 13849-2.

Для стандарту IEC 62061, який по суті є альтернативою стандарту ISO 13849-1, рівень функціональної безпеки систем управління обладнанням визначається трьома рівнями повноти безпеки (РПБ) SIL – «Safety Integrity» (1, 2, 3). РПБ встановлюють вимоги до повноти безпеки електричних, електронних і програмованих електронних систем управління, що пов'язані з безпекою (ПБЕСУ), а також вимоги щодо їх здатності виконувати функції безпеки в передбачених обставинах. Ці дискретні рівні характеризуються відповідними значеннями ймовірності небезпечної відмови за годину (PFH_d).

На рисунку 2 а, б наведено взаємозв'язок ймовірності небезпечної відмови за годину (PFH_d) із рівнем безпеки (РБ) PL (EN ISO 13849) та рівнем повноти безпеки (РПБ) SIL (IEC 62061).

На рисунку 3, з урахуванням існуючого взаємозв'язку стандарту IEC 62061 з іншими стандартами, представлено рекомендований загальний алгоритм його застосування при проведенні оцінки можливих ризиків і подальшого проектування електричних, електронних та програмованих електронних систем управління промисловим обладнанням.

Для будь-якої пов'язаної з безпекою системи управління (ПБСУ) повинні бути визначені такі показники (параметри), що пов'язані з безпекою частин (елементів) обладнання та систем управління з урахуванням відмовостійкості апаратних засобів і використовуваних у системі управління діагностичних функцій та їх надійності.

Для стандарту EN ISO 13849 (див. таблицю 1) це:

Structure/category; MTTF_d; B10_d; n_{op}; CCF; DC_{avg}; PL; T10_d, а для стандарту IEC 62061 (див. таблицю 2), це:

Structure/subsystem (SS) architecture; PFH_d; B10; λ_d/λ; C; β; DC; SIL.

Рисунок 2 – Взаємозв'язок ймовірності небезпечної відмови за годину (PFH_d):
а) із рівнем безпеки (РБ) PL (EN ISO 13849); б) із рівнем повноти безпеки (РПБ) SIL (IEC 62061)

Рисунок 3 – Рекомендований загальний алгоритм застосування стандарту IEC 62061 та його взаємозв'язок з іншими стандартами

Таблиця 1 – Параметри (показники) безпеки (Safety parameters) згідно з EN ISO 13849-1

Показники безпеки	Примітка
Structure /category (Cat)/	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 та їх надійності
MTTF_d (Mean Time to Dangerous Failure)	Середній час напрацювання до настання 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 (компонентів), коли ці відмови відбуваються за загальною причиною – в результаті однієї (одиночної) 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 функцій безпеки системою управління, забезпечувати при передбачуваних умовах необхідний рівень безпеки. Класифікація від PL _a (найвища ймовірність відмови) до PL _e (низка 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 (показники) безпеки (Safety parameters) згідно з IEC 62061

Показники безпеки	Примітка
Structure /subsystem (SS) architecture/	Структурні вимоги (архітектура підсистем). Класифікація підсистем, що виконують функції управління та пов'язані з безпекою та які мають архітектуру відповідно до IEC 62061 і виконані з урахуванням вимог до відмовостійкості апаратних засобів і використаних діагностичних функцій та 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)	Число циклів, коли кількість компонентів, що відмовили, досягає 10 %(для електромеханічних компонентів)
λ_d/λ (Ratio 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)	Середнє число робочих циклів, заданих для застосування
β (Beta factor. Common cause failure factor)	Бета-фактор. Коефіцієнт відмови із загальної причини або сприйнятливості до відмов із загальної причини – в результаті однієї (одиночної) 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 функцій безпеки, пов'язаної з безпекою електричних компонентів системи управління машиною. Всього три рівня – 1, 2 і 3. SIL1 (найнижчий рівень), SIL3 (найвищий рівень) безпеки

Застосування обох стандартів, як EN ISO 13849-1, так і IEC 62061 передбачає виконання відповідних важливих вимог щодо забезпечення безпеки залежно від технології,

що використовується для реалізації пов'язаних з безпекою функцій управління обладнанням (див. таблицю 3).

Таблиця 3 – Сфери застосування стандартів ISO 62061 і IEC 13849-1

Варіант	Технологія реалізації зв'язаної (их) з безпекою функції (ій) управління	ISO 13849-1	IEC 62061
A	Неелектрична, наприклад, гідравліка	«X»	Не охоплює
B	Електромеханічна, наприклад, реле або нескладні електронні пристрої	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = PL _e	Усі архітектури і до РПБ = SIL 3
C	Складні електронні пристрої, наприклад, програмовані	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = PL _d	Усі архітектури і до РПБ = SIL 3
D	A у поєднанні з B	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = PL _e	«X» (див. Примітка 3)
E	C у поєднанні з B	Обмежено встановленими архітектурами (див. Примітка 1) і до РБ = PL _d	Усі архітектури і до РПБ = SIL 3
F	C у поєднанні з A, або C в поєднанні з A і B	«X» (див. Примітка 2)	«X» (див. Примітка 3)

Позначка «X» означає, що цю технологію регламентує стандарт, зазначений в заголовку колонки таблиці.

*Примітки:

1. Встановлені архітектури визначені в EN ISO 13849-1, де надано спрощений підхід для квантифікації рівня безпеки (РБ) PL. РБ – рівень необхідного мінімального зниження ризику.
2. Для складних електронних пристроїв використовують встановлені архітектури до РБ = PL_d згідно з EN ISO 13849-1 або будь-які архітектури згідно з IEC 62061.
3. Елементи, які засновані на неелектричній технології, відповідно до EN ISO 13849-1, використовують в якості підсистем.

Згідно з вимогами EN ISO 13849-1 (див. таблицю 1), структури (архітектури) елементів системи управління, які пов'язані з безпекою, визначаються в залежності від вибраної категорії:

• **Категорія В – базова категорія** (структура наведена на рис. 4).

Елементи системи управління, що пов'язані з безпекою, мають бути, як мінімум, розроблені та сконструйовані відповідно до сучасного рівня техніки та протистояти очікуванім зовнішнім впливам.

Рисунок 4 – Структура для категорії В (одноканальна)

• **Категорія 1** (рисунок 5).

Елементи системи управління, що пов'язані з безпекою, мають бути розроблені та сконструйовані з використанням перевірених компонентів і надійних принципів безпеки.

Рисунок 5 – Структура для категорії 1 (одноканальна)

• **Категорія 2** (рисунок 6).

Функції елементів системи управління, які пов'язані з безпекою, необхідно періодично контролювати (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 настанням можливої небезпечної ситуації.

Рисунок 6 – Структура для категорії 2 (одноканальна контрольована)

• **Категорія 3** (рисунок 7).

Одна відмова в елементах системи управління, що пов'язані з безпекою, не веде до втрати функції безпеки всієї системи. У той же час, оскільки в системі управління не використовується функція самоконтролю через що не всі несправності можуть бути виявлені, то накопичення таких невиявлених несправностей все ж таки може з часом призвести до небезпечної ситуації.

Рисунок 7 – Структура для категорії 3 (двоканальна без функції самоконтролю)

• **Категорія 4** (рисунок 8).

Одна відмова в елементах системи управління, що

пов'язані з безпекою, не веде до втрати функції безпеки всієї системи. При використанні функції самоконтролю ця несправність має бути виявлена негайно або до виникнення наступної потенційної небезпеки. Якщо це неможливо, то потрібно забезпечити умови, за яких накопичення несправностей не повинно призводити до втрати функції безпеки всієї системи управління.

Рекомендований для застосування алгоритм (граф) визначення необхідного рівня безпеки (РБ)PL (a, b, c, d, e) промислового обладнання за стандартом ENISO 13849 наведено на рис. 9.

Рисунок 8 – Структура для категорії 4
(двоканальна із функцією самоконтролю)

Рівень «а» = самий низький рівень ризику (low risk)

Рівень «е» = найбільш високий рівень ризику (high risk)

Рисунок 9 – Алгоритм визначення необхідного рівня безпеки (РБ)

**Параметри ризику:
(Risk parameters):**

S - тяжкість травми

S1 незначні (зазвичай
виліковні травми)

S2 серйозні (як правило,
невиліковні) травми

F – частота і/або
схильність до
небезпеки

F1 – зрідка, не дуже
часто і/або

короткочасна дія
F2 – часто, скоріше
безперервно і/або
довгострокова дія

P - можливість
уникнути небезпеки
або обмеження
завданої шкоди

P1 – можливо за
певних умов

P2 - навряд чи можливо
(малоймовірно)

Структурні вимоги щодо побудови архітектури системи управління та її підсистем за стандартами ІЕС 62061 і ІЕС 61508, а також алгоритми визначення їх основних параметрів (показників) безпеки буде розглянуто у другій частині цієї роботи – Частина II. Функціональна безпека систем управління. (Планується до опублікування у наступному номері Збірника).

Висновки

Слід одразу ж зазначити, що хоча стандарти (ІЕС 62061 та ІЕС 61508) є основними стандартами щодо дотримання вимог функціональної безпеки при розробці, проектуванні та експлуатації пов'язаних з безпекою електричних, електронних та електронних програмованих систем управління (ПБЕСУ), але на їх основі все ще не розроблені відповідні їм національні державні стандарти. Це ускладнює процес імплементації вітчизняного законодавства до сучасного європейського у сфері промислової безпеки, і, безумовно, потребує як найшвидшого виправлення.

Необхідно також зауважити, що з точки зору подальшого розвитку технічного прогресу у сфері

промислової безпеки, саме електричні, електронні та електронні програмовані системи управління промисловим обладнанням є найбільш перспективними, а їх частка з часом лише збільшується, що також свідчить про нагальну необхідність розробки відповідних національних стандартів.

Для підтвердження актуальності та важливості таких дій і для більш глибокого розуміння їх необхідності у цій роботі і були проаналізовані та визначенні основні особливості щодо дотримання за стандартами ІЕС 62061 та ІЕС 61508 сучасних вимог з функціональної безпеки ПБЕСУ в процесі всього їх життєвого циклу та наданні відповідні рекомендації щодо основних аспектів їх реалізації.

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. Системы безопасности с двуручным управлением. *Сварщик*. 2019. № 2. 45–49.
2. Левченко О. Г., Каштанов С. Ф., Олійник А. П. Інноваційні розробки в сфері безпеки – основа професійної підготовки випускників КПІ ім. Ігоря Сікорського. *Проблеми охорони праці в Україні : зб. наук. праць*. Київ: ДУ «ННДІПБОП», 2019. 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. Про затвердження Технічного регламенту безпеки машин. Постанова КМ України від 30 січня 2013 р. № 62 (із змінами, внесеними згідно з Постановою КМ № 632 від 28.08. 2013 року).
5. EN ISO 12100-1/2 «Safety of machinery General principles for design and risk evaluation. Basic concepts».
6. EN 954-1 «Safety of machinery SRP/CS. General principles for design».
7. EN ISO 13849-1/-2 «Safety of machinery - Safety-related parts of control systems».
8. IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems».
9. IEC 61508 (all parts) «Functional safety electrical/electronic/programmable electronic safety-related systems».

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 vypusknikov 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. Pro zatverdzhennia Tekhnichnoho rehlementu bezpeky mashyn. Postanova KM Ukrainy vid 30 sichnia 2013 r. № 62 (iz zminamy, vnesenymy zghidno z Postanovoiu KM № 632 vid 28.08.2013).
5. EN ISO 12100-1/2 «Safety of machinery General principles for design and risk evaluation. Basic concepts».
6. EN 954-1 «Safety of machinery SRP/CS. General principles for design».
7. EN ISO 13849-1/-2 «Safety of machinery - Safety-related parts of control systems».
8. IEC 62061 «Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems».
9. IEC 61508 (all parts) «Functional safety electrical/electronic/programmable electronic safety-related systems».

О. Левченко, С. Каштанов

СОВРЕМЕННЫЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ К СИСТЕМАМ УПРАВЛЕНИЯ ПРОМЫШЛЕННЫМ ОБОРУДОВАНИЕМ (Часть 1. Показатели безопасности 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. Выполнен аналитический обзор требований современных международных стандартов (IEC 62061, IEC 61508) по безопасности функционирования электрических, электронных и программируемых электронных систем управления промышленным оборудованием и поэтапной последовательности выполнения защитных мероприятий от существующих опасностей; определены основные особенности построения архитектуры таких систем управления и предоставлены алгоритмы определения основных показателей их функциональной безопасности (PL; SILPL; PFHd), а также алгоритм обеспечения необходимого уровня безопасности в зависимости от параметров существующих рисков. 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. Определены основные параметры (показатели) безопасности функционирования электрических, электронных и программируемых электронных систем управления промышленным оборудованием. Предоставлены соответствующие рекомендации по основным аспектам их применения и реализации по стандартам IEC 62061 и IEC 61508. Разработка и внедрение соответствующих национальных стандартов на основе IEC 62061 и IEC 61508 должны ускорить дальнейшее развитие технического прогресса в сфере промышленной безопасности. Подтверждена актуальность и важность необходимости разработки соответствующих национальных стандартов на основе стандартов IEC 62061 и IEC 61508.

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