ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ПРОЦЕДУР ПІДТВЕРДЖЕННЯ ВІДПОВІДНОСТІ ТА ІНТЕГРАЦІЇ, ПОВ'ЯЗАНИХ З БЕЗПЕКОЮ СИСТЕМ УПРАВЛІННЯ

Каштанов С. Ф., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Анотація. Проаналізовано основні вимоги та особливості використання стандарту IEC 62061 при проведені процедур підтвердження відповідності та інтеграції пов'язаних з безпекою електричних, електронних і програмованих електронних систем управління машин та механізмів і надані відповідні практичні рекомендації щодо їх застосування.

Ключові слова: безпека, системи управління, проектування, тестування.

Abstract. The basic requirements and peculiarities of the use of the IEC 62061 standard in the conformity assessment and integration procedures for the safety of electrical, electronic and programmable electronic control systems of machines and mechanisms are analyzed and appropriate practical recommendations are given for their application.

Keywords: safety, control systems, design, testing.

Вступ. Застосування пов'язаних з безпекою систем управління машин та механізмів дозволяє значно підвищити рівень їх безпеки. До складу таких систем, як правило, входять різноманітні пристрої безпеки для управління налаштуваннями промислового обладнання, захисні огорожі, світлові бар'єри, пристрої двопозиційного управління та аварійної зупинки тощо. Слід зазначити, що робота будь-якого промислового обладнання, в обов'язковому порядку повинна постійно контролюватися, а саме обладнання, у разі необхідності (аварійна ситуація, відмова, відключення електропостачання тощо) повинно гарантовано приводитися у безпечний стан.

Аналіз стану питання. Основні нормативні документи, що регламентують вимоги безпеки в сфері розробки, проектування та експлуатації машин і механізмів та систем їх управління, це Directive 2006/42/EC [1], а також діючі технічні регламенти та стандарти EN 954-1 (ДСТУ EN 954-1: 2003), EN ISO 13849-1 (ДСТУ EN ISO 13849-1-2016), IEC 62061 та IEC 61508 [2-7].

Серед цих нормативних документів особливе місце займає стандарт IEC 62061 [6], який був розроблений спеціально для пов'язаних з безпекою електричних, електронних та програмованих електронних систем управління машинами і механізмами, які в наш час є найбільш поширеними системами управління у цій галузі. Необхідно одразу ж зазначити, що саме цей стандарт у максимально повному обсязі регламентує вимоги безпеки до подібних систем управління машинами та механізмами, а також порядок проведення всіх необхідних процедур при їх проектуванні, розробці та експлуатації.

Мета роботи: визначення основних вимог стандарту IEC 62061, а також особливостей його використання у разі проведення таких важливих з точки зору безпеки процедур, як підтвердження відповідності та інтеграції пов'язаних

з безпекою електричних, електронних і програмованих електронних систем управління машинами та механізмами, а також надання відповідних практичних рекомендацій щодо їх застосування.

Методики, матеріали і результати досліджень.

Процедура підтвердження відповідності. Згідно стандарту IEC 62061 [6], процедура підтвердження відповідності систем управління машин та механізмів вимогам безпеки включає у себе перевірку та тестування пов'язаних з безпекою електричних, електронних та програмованих електронних систем управління (ПБЕСУ) машин та механізмів для забезпечення досягнення вимог, що визначені у відповідній специфікації вимог з безпеки ПБЕСУ.

**Примітка: Підтвердження відповідності програмованої СБЕСУ включає підтвердження відповідності як механічних засобів, так і програмного забезпечення.*

Всі ПБФУ, зазначені в специфікації вимог до ПБЕСУ, і всі процедури експлуатації та технічного обслуговування ПБЕСУ повинні пройти процедуру підтвердження відповідності за допомогою випробувань і/або аналізу.

Повинна бути створена відповідна документація щодо виконання для ПБЕСУ підтвердження відповідності безпеки, в якій для кожної ПБФУ вказуються:

a) застосована версія плану підтвердження відповідності безпеки для ПБЕСУ;

b) ПБФУ, що тестується (або аналізується), а також конкретні посиланнями на вимоги, які визначені під час планування підтвердження відповідності безпеки для ПБЕСУ;

c) інструменти та обладнання, що використовуються а також дані щодо їх калібрування;

d) результати дій щодо підтвердження відповідності безпеки;

e) розбіжності між очікуваними і фактичними результатами.

** Примітка: У разі розбіжності між очікуваними і фактичними результатами повинні бути виконані коригувальні дії та повторне тестування (в разі необхідності) і ці дії повинні бути документально оформлені.*

Для підтвердження відповідності ПБЕСУ систематичній повноті безпеки повинно бути виконано наступне:

a) Функціональне тестування для виявлення відмов на стадіях специфікації, проектування та інтеграції, а також для запобігання відмов в процесі підтвердження відповідності програмного забезпечення та апаратних засобів ПБЕСУ. Функціональне тестування повинно ґрунтуватися на специфікації вимог з безпеки і містити верифікацію (наприклад, шляхом перевірки і випробувань), щоб оцінити, чи захищена ПБЕСУ від несприятливих впливів навколишнього середовища;

b) тестування стійкості до електромагнітних впливів, при цьому випробування на стійкість до електромагнітних впливів підсистем ПБЕСУ або елементів підсистем виконувати не обов'язково, якщо за допомогою відповідного аналізу може бути показано, що для передбачуваного застосування їх стійкість адекватна стійкості ПБЕСУ;

c) тестування з введення несправностей, якщо потрібна частка безпечних

відмов ≥ 90%. У таких випробуваннях вводяться або імітуються несправності в технічних засобах ПБЕСУ, а отриманий результат документально оформлюється.

Крім того, повинні застосовуватися одна або декілька з наступних груп аналітичних методів з урахуванням складності ПБЕСУ і заданого рівня повноти безпеки (РПБ):

a) статистичний аналіз і аналіз відмов;

** Примітка: Таке поєднання аналітичних методів підходить для ПБЕСУ із заданими РПБ, що не перевищують РПБ 2.*

b) статистичний аналіз, динамічний аналіз і аналіз відмов;

** Примітка: Таке поєднання аналітичних методів не рекомендується для ПБЕСУ, які реалізують ПБФУ з заданими РПБ нижче РПБ 2.*

c) моделювання та аналіз відмов.

** Примітка: Таке поєднання аналітичних методів підходить тільки для ПБЕСУ з заданими РПБ, що не перевищують РПБ 2.*

Також, повинні застосовуватися одна або декілька з наступних груп методів тестування з урахуванням складності ПБЕСУ і заданого РПБ:

a) тестування методом «чорного ящика»: тест (и) динамічної поведінки в реальних умовах функціонування виявляє (ють) невідповідності з функціональною специфікацією ПБЕСУ, а також оцінюють корисність і надійність ПБЕСУ;

b) тестування з введенням (включенням) несправностей повинні проводиться, якщо необхідна доля безпечних відмов <90%, при цьому в таких випробуваннях вводяться або імітуються несправності в технічних засобах ПБЕСУ, а отримані результати документально оформлюються;

c) тестування «найгіршого випадку» має виконуватися для оцінки екстремальних (тобто найгірших) випадків, визначених із застосуванням аналітичних методів;

** Примітка: Операційна здатність ПБЕСУ тестується при найгірших випадках. Умови навколишнього середовища змінюються до їх максимально допустимих граничних значень.*

d) практичний досвід: використання практичного досвіду із різних застосувань, як один із заходів, що дозволяють уникнути збоїв під час виконання підтвердження відповідності ПБЕСУ.

Процедура інтеграції. ПБЕСУ повинна бути інтегрована у відповідності до конкретного проекту ПБЕСУ. В рамках інтеграції всі підсистеми і елементи підсистем ПБЕСУ повинні пройти випробування у відповідності до конкретних тестів інтеграції. Ці випробування повинні показати, що всі модулі взаємодіють правильно при виконанні функцій, для яких вони призначені і не виконують непередбачених функцій.

Інтеграція пов'язаного з безпекою програмного забезпечення ПБЕСУ включає тести, які визначаються на стадії проектування і розробки для забезпечення сумісності програмного забезпечення з апаратними засобами і вбудованою платформою програмного забезпечення за умови дотримання функціональних вимог і вимог безпеки.

Для тестування інтеграції ПБЕСУ повинна бути розроблена відповідна документація, що встановлює результати випробувань і визначає чи досягнуті цілі та критерії, визначені на стадії проектування і створення системи. У разі відмови повинні бути документально оформлені її причини, а також виконані відповідні коригувальні дії та повторне тестування.

При випробуваннях інтеграції ПБЕСУ повинна бути документально оформлена наступна інформація:

a) версія специфікації випробувань;

b) критерії прийняття випробувань інтеграції;

c) версія ПБЕСУ, що випробовується;

d) засоби випробувань та обладнання, що використовуються, а також дата їх повірки;

e) результати кожного випробування;

f) будь-яка невідповідність між очікуваними і фактичними результатами;

g) проведений аналіз і прийняте рішення про продовження випробувань або випуску запиту щодо необхідності змін (при наявності невідповідності).

При проведенні тестів, що визначають систематичну повноту безпеки в процесі інтеграції ПБЕСУ повинні бути проведені наступні випробування:

a) функціональні тести, в яких для ПБЕСУ використовуються дані, що адекватно характеризують операції (вихідні дані тестів порівнюються з наведеними в специфікації, при цьому відхилення від специфікації і вказівки щодо неповної її перевірки повинні бути документально оформлені);

b) динамічні випробування для перевірки динамічної поведінки в реальних умовах функціонування і виявлення відмов відповідно до функціональної специфікації ПБЕСУ, а також для оцінки надійності і корисності ПБЕСУ.

** Примітки:*

1.Функції системи або програми виконуються в конкретному оточенні з конкретними тестовими даними, які були отримані систематично з специфікації вимог до безпеки ПБЕСУ відповідно до встановлених критеріїв. Отримана поведінка ПБЕСУ порівнюється зі специфікацією. Мета полягає в тому, щоб визначити чи правильно ПБЕСУ і/або її підсистеми виконують всі функції, задані в специфікації. Методика формування класів еквівалентності є одним з підходів формування тестових даних при тестуванні методом «чорного ящика». Простір вхідних даних розділяється на конкретні діапазони вхідних значень (класів еквівалентності) за допомогою специфікації. Потім формуються тестові приклади з:

- даних з допустимих діапазонів;

- даних з неприпустимих діапазонів;

- даних з граничних значень діапазонів;

- екстремальних значень;

- комбінацій з перерахованих вище класів еквівалентності.

2. Для вибору тестових прикладів в різних випробуваннях (наприклад, тестування модуля, тестування інтеграції та тестування системи) можуть бути ефективні і інші методи

ПБЕСУ повинна бути встановлена відповідно до плану функціональної безпеки для остаточного підтвердження відповідності системи.

Повинні бути проведені відповідні записи щодо встановлення ПБЕСУ, а також щодо всіх результатів випробувань. У разі відмови ПБЕСУ, її причини

повинні бути обов’язково зареєстровані.

Також слід зазначити, що ПБЕСУ обов’язково повинна бути забезпечена відповідною документацією щодо установки, експлуатації та технічного обслуговування, що дозволить користувачеві розробляти такі процедури, які гарантують підтримання необхідної функціональної безпеки ПБЕСУ під час експлуатації та технічного обслуговування машини.

Дана документація повинна включати у себе:

a) повний опис обладнання, установки і монтажу;

b) звіт про передбачуване використанні ПБЕСУ і будь-які заходи, які можуть бути необхідні для запобігання розумно передбачуваного неправильного використання;

c) відомості про фізичне середовище (наприклад, освітлення, вібрація, рівні шуму, атмосферні забруднення, тощо) в разі необхідності;

d) огляд блок-схем, у разі потреби;

e) принципові схеми;

f) інтервал контрольних перевірок або термін життя;

g) опис (включаючи програми взаємозв'язків) взаємодії (якщо такі є) між функцією (ями) електричної системи управління машини;

h) опис необхідних заходів, що гарантують поділ функцій ПБЕСУ і електричної системи управління машиною;

i) опис заходів та засобів захисту, передбачених для забезпечення безпеки (наприклад, якщо необхідно призупинити ПБФУ для ручного програмування або верифікації програм);

j) інформацію щодо програмування, де це необхідно;

k) опис вимог щодо технічного обслуговування, що застосовується для ПБЕСУ, в тому числі:

1) журнал для запису хронології технічного обслуговування машини;

2) стандартні дії, які повинні бути виконані для підтримки функціональної безпеки ПБЕСУ, включаючи планову заміну компонентів із заздалегідь визначеним терміном експлуатації;

3) підтримання процедур, яких слід дотримуватися при появі збою або відмови в ПБЕСУ, в тому числі:

- процедури діагностики і усунення збою;
- процедури, яка підтверджує правильність роботи після ремонту;
- вимог до запису про технічне обслуговування.

4) інструментальні засоби, необхідні для технічного обслуговування і повторного введення в експлуатацію, а також процедури для підтримки інструментальних засобів і обладнання;

5) специфікації для періодичних випробувань (тестувань), профілактичного та позапланового технічних обслуговувань.

** Примітки:*

1. Періодичні випробування - це такі функціональні випробування, які необхідні для підтримки правильності роботи і виявлення збоїв;

2. Профілактичне технічне обслуговування - це заходи, що застосовуються для підтримки необхідних робочих характеристик;

3. Позаплановий технічне обслуговування включає в себе заходи, вжиті після настання конкретного (их) збою (ів), які повертають ПБЕСУ в стан «як спроектовано».

Висновки. Проведений в даній роботі аналіз переконливо свідчить про те, що необхідний рівень безпеки машин та механізмів може бути гарантовано забезпечений лише у разі виконання всіх основних вимог стандарту IEC 62061 стосовно особливостей проведення таких важливих з точки зору безпеки процедур, як підтвердження відповідності та інтеграції пов'язаних з безпекою електричних, електронних і програмованих електронних систем управління машинами та механізмами.

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».
7. IEC 61508 (all parts) «Functional safety electrical/electronic/programmable electronic safety-related systems».