ВІДПОВІДНІСТЬ ВБУДОВАННОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЕЛЕКТРОНИХ СИСТЕМ УПРАВЛІННЯ СУЧАСНИМ ВИМОГАМ БЕЗПЕКИ

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

Анотація. Проаналізовано основні вимоги стандартів IEC 62061 та IEC 61508 щодо відповідності вбудованого програмного забезпечення електронних систем управління машинами та механізмами сучасним вимогам безпеки і надані відповідні рекомендації щодо особливостей практичного застосування цих стандартів.

Ключові слова: безпека, системи управління, програмне забезпечення.

Abstract. The main requirements of IEC 62061 and IEC 61508 standards for conformity of the embedded software of electronic control systems of machines and mechanisms with the modern safety requirements are analyzed, are given and the corresponding recommendations on the practical application of these standards are given.

Keywords: safety, control systems, software.

Вступ. Застосування на виробництві будь-яких захисних заходів та засобів, які використовуються для усунення існуючих небезпек та зниження рівнів можливих ризиків щодо отримання травм та професійних захворювань, повинно здійснюватися у певній послідовності відповідно до вимог EN ISO 12100-1 [1].

Як правило, необхідний рівень безпеки виробничого обладнання, і в першу чергу машин та механізмів,, може бути забезпечений лише у разі використання пов’язаних з безпекою систем управління, в тому числі і програмованих електронних. До складу таких систем, як правило, входять різноманітні пристрої безпеки для управління налаштуваннями промислового обладнання, захисні огорожі, світлові бар'єри, пристрої аварійної зупинки тощо. За допомогою таких систем управління виконання всіх технологічних операцій на будь-якому обладнанні, в обов'язковому порядку повинно постійно контролюватися, а саме обладнання, у разі необхідності (аварійна ситуація, відмова, відключення електропостачання тощо) повинно гарантовано приводитися у безпечний стан.

Основні функції безпеки, які можуть бути реалізовані за допомогою пов’язаних з безпекою систем управління, це:

- контроль відкритих зон небезпеки;
- аварійне відключення обладнання;
- запобігання непередбаченого запуску обладнання (повторних перезапусків);
- контроль світлових бар’єрів;
- контроль рухомих (з’ємних) захисних огороджень (без блокування або з блокуванням);

- контроль двопозиційного управління (типу I, II або III) тощо.

Аналіз стану питання. Основними нормативними документами, що регламентують вимоги безпеки щодо розробки, проектування та експлуатації машин і механізмів та систем управління їх безпекою є Directive 2006/42/EC і діючі у цій сфері 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 [1-7].

Серед цих нормативних документів особливе місце займає стандарт IEC 62061 [6], який було розроблено спеціально для пов'язаних з безпекою електричних, електронних та програмованих електронних систем управління машинами і механізмами. Необхідно підкреслити, що саме програмовані електронні системи управління вважаються на даний час найбільш перспективними системами управління у цій сфері.

Згідно вимог [6-7], якщо програмне забезпечення має використовуватися в будь-якій частині пов'язаних з безпекою програмованих електронних систем управління (ПБЕСУ), що реалізують пов'язані з безпекою функції управління (ПБФУ) машин та механізмів, то необхідно розробити і документально оформити специфікацію вимог до безпеки програмного забезпечення.

Специфікація вимог до безпеки програмного забезпечення, як вбудованого так і прикладного, повинна бути розроблена для кожної підсистеми на основі специфікації і архітектури ПБЕСУ.

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

1) вимог безпеки, заданих для ПБФУ;

2) вимог, що випливають 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 повинна бути досить детальною для того, щоб забезпечити виконання існуючих стадій проектування і впровадження ПБЕСУ для досягнення необхідної повноти безпеки і дозволити виконати верифікацію.

Розробник програмного забезпечення повинен переглянути інформацію, що міститься в специфікації для того, щоб гарантувати, що вимоги визначені адекватним чином. Зокрема, розробник програмного забезпечення повинен відповідно до стандарту IEC 62061 врахувати:

- пов'язані з безпекою функції управління;
- конфігурацію або архітектуру системи;
- продуктивність і час відгуку;
- інтерфейси обладнання та оператора;
- всі відповідні режими роботи обладнання;
- діагностичні тести зовнішніх пристроїв (наприклад, датчиків і виконавчих елементів).

Задані для безпеки програмного забезпечення вимоги повинні бути виражені і структуровані так, щоб вони:

- були ясними, придатними для верифікації, тестування, підтримки і виконання, а також пропорційними з рівнем повноти безпеки;
- були придатними для того, щоб можна було визначити їх джерело в специфікації вимог безпеки ПБЕСУ;
- не містили інформації та описів, які є неоднозначними.

Специфікація вимог до безпеки програмного забезпечення повинна виражати необхідні характеристики кожної підсистеми, надаючи інформацію, що дозволяє виконати вибір обладнання, який відповідає існуючим вимогам безпеки. Також повинні бути визначені наступні вимоги для програмування ПБФУ:

- логіка (тобто функціональність) всіх функціональних блоків, яка виконується кожною підсистемою;
- вхідні та вихідні інтерфейси, призначені для кожного функціонального блоку;
- формат і діапазони значень вхідних та вихідних даних і їх зв'язок з функціональними блоками;
- відповідні дані, що описують будь-які обмеження кожного функціонального блоку, наприклад, максимальний час відгуку, граничні значення для перевірки достовірності;
- функції, які дозволяють машині досягати чи підтримувати безпечний стан;
- функції, пов'язані з виявленням, оповіщенням і обробкою помилок;
- функції, пов'язані з періодичним тестуванням ПБФУ в автономному та неавтономному режимах;
- функції, що запобігають несанкціонованим змінам в ПБЕСУ;
- інтерфейси функцій, не пов'язаних з безпекою;
- продуктивність і час відгуку.

** Примітка: Інтерфейси включають в себе засоби програмування як в автономному, так і неавтономному режимах.*

План функціональної безпеки повинен визначати стратегію розробки, інтеграції, верифікації та підтвердження відповідності програмного забезпечення.

Мета роботи: визначення основних вимог стандартів IEC 62061 та IEC 61508 щодо відповідності вбудованого програмного забезпечення електронних систем управління машинами та механізмами сучасним вимогам безпеки.

Методики, матеріали і результати досліджень. Вбудоване програмне забезпечення, яке включене в підсистеми, має відповідати вимогам IEC 61508-3 і необхідному рівню повноти безпеки (РПБ) за стандартом IEC 62061.

У програмному забезпеченні, заснованому на параметризації, пов'язані з безпекою параметри повинні розглядатися як зв'язані з безпекою аспекти проектування ПБЕСУ, які описані в специфікації вимог до безпеки програмного

забезпечення. Параметризація повинна виконуватися за допомогою спеціального інструментального засобу, що надається постачальником ПБЕСУ або зв'язаний з підсистемою (ами). Цей інструментальний засіб повинен мати свою ідентифікацію (назва, версія тощо).

Повинна підтримуватися повнота всіх даних, що використовуються для параметризації. Досягти цього можливо шляхом застосування відповідних заходів щодо управління:

- діапазоном допустимих вхідних даних;
- пошкодженими даними перед передачею;
- наслідками помилок в процесі передачі параметрів;
- наслідками неповної передачі параметрів;
- наслідками збоїв і відмов технічних засобів і програмного забезпечення в інструментальних засобах, які використовуються для параметризації.

Необхідно, щоб інструментальний засіб, який використовується для параметризації, відповідав:

- всім відповідним вимогам до підсистеми відповідно до IEC 62061 для забезпечення коректної параметризації;
- використовувалася спеціальна процедура для установки пов'язаних з безпекою параметрів.

Ця процедура повинна включати підтвердження:

- вхідних параметрів для ПБЕСУ шляхом повторної передачі змінених параметрів в інструментальний засіб параметризації, або застосуванням інших засобів, що підтверджують повноту параметрів;
- результату (наприклад, автоматичною перевіркою інструментальним засобом параметризації).

** Примітка: Це особливо важливо, якщо параметризація здійснюється за допомогою пристрою, який спеціально не призначений для цієї мети (наприклад, персонального комп'ютера або аналогічного пристрою).*

Для запобігання систематичних відмов різноманітності в функції (ях) необхідно використання модулів програмного забезпечення, призначених для кодування або декодування в процесі прийому/передачі, і модулів програмного забезпечення, призначених для візуалізації користувачеві пов'язаних з безпекою параметрів.

В документації на програмне забезпечення, заснованому на параметризації, повинні зазначатися дані, що використовуються (наприклад, попередньо визначені набори параметрів), а також інформація, необхідна для ідентифікації параметрів, пов'язаних з ПБЕСУ, в тому числі, про особу (іб), що здійснює (ють) параметризацію разом з іншою відповідною інформацією, наприклад, такою, як дата параметризації.

Також застосовуються наступні дії з верифікації для програмного забезпечення на основі параметризації:

- верифікація правильності установки для кожного пов'язаного з безпекою параметра (мінімальне, максимальне і репрезентативні значення);

- верифікація того, що пов'язані з безпекою параметри перевіряються на достовірність (наприклад, шляхом виявлення неприпустимих значень і т.ін.);

- верифікація того, що несанкціоновані зміни пов'язаних з безпекою параметрів неможливі;

- верифікація того, що дані /сигнали/ для параметризації створюються і обробляються таким чином, що можливі збої не можуть привести до втрати ПБФУ.

** Примітка: Це особливо важливо, якщо параметризація здійснюється за допомогою пристрою, спеціально не призначеного для цієї мети (наприклад, персонального комп'ютера або аналогічного пристрою).*

Висновки. Необхідний рівень безпеки машин та механізмів може бути забезпечений лише за умови, що розробка будь-якого вбудованого програмного забезпечення ПБЕСУ машинами та механізмами, що реалізують ПБФУ, здійснюється з урахуванням вимог стандартів IEC 62061 та IEC 61508 щодо відповідності такого програмного забезпечення сучасним вимогам безпеки і, в першу чергу, за умови обов’язкового складання відповідної специфікації вимог щодо безпеки програмного забезпечення та дотримання таких процедур, як параметризація та верифікація, а також процедури підтвердження відповідності вбудованого програмного забезпечення.

Література

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

2. 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.

3. 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).

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».