ПРОЕКТУВАННЯ ТА РОЗРОБКА ПОВ'ЯЗАНИХ З БЕЗПЕКОЮ СИСТЕМ УПРАВЛІННЯ ПРОМИСЛОВИМ ОБЛАДНАННЯМ

Каштанов С. Ф., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського);
Багінський В. О., студент (гр. ТО-51, ТЕФ КПІ ім. Ігоря Сікорського)

Анотація. Проаналізовано основні загальні вимоги стандарту IEC 62061 щодо проектування та розробки пов'язаних з безпекою систем управління промисловим обладнанням, в яких використовуються електричні, електронні та програмовані електронні системи управління (ПБЕСУ), а також визначенні основні особливості і порядок застосування відповідних процедур, що передбачені цим стандартом.

Ключові слова: система управління, безпека, машини, механізми.

Abstract. Analyzed the main general requirements of the IEC 62061 standard for the design and development of electrical, electronic and programmable electronic industrial control systems are analyzed, as well as the main features of the relevant procedures provided for by this standard.

Keywords: control system, safety, machines, mechanisms.

Вступ. Сучасне реформування системи промислової безпеки в Україні на основі подальшої імплементації європейського та національного законодавств передбачає узгодження питань технічного регулювання та приведення існуючої в Україні нормативної бази з безпеки промислового обладнання та продукції у відповідність до існуючих європейських та міжнародних стандартів, що регламентують вимоги безпеки при їх проектуванні, виробництві та експлуатації, включаючи і вимоги безпеки при проектуванні пов'язаних з безпекою систем управління.

Аналіз стану питання. Проектування 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 ISO 12100-1/2, EN 954-1 (ДСТУ EN 954-1: 2003), EN ISO 13849-1 (ДСТУ EN ISO 13849-1-2016) та IEC 62061 [1-6].

Як бачимо, на основі стандарту ISO 13849-1 на даний час вже розроблений національний стандарт ДСТУ EN ISO 13849-1:2016 «Безпечність машин. Деталі систем управління, пов’язані з забезпеченням безпеки. Частина 1. Загальні принципи проектування». Нажаль цього не можна сказати про стандарт 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 електронних систем управління» [6], який на даний час є основним стандартом щодо проектування пов'язаних з безпекою електричних, електронних або програмованих електронних систем управління (ПБЕСУ), на відміну від стандарт ISO 13849-1, який регламентує вимоги безпеки при проектуванні лише електромеханічних систем управління.

Слід також зазначити, що хоча стандарт IEC 62061 і був розроблений як альтернатива стандарту EN ISO 13849-1, але тільки комплексне використання цих стандартів, а саме IEC 62061 та EN ISO 13849-1, і дозволяє створювати високоефективні, з точки зору безпеки, системи управління промислового обладнання. Безумовно, що визначення основних особливостей функціонування та застосування стандарту IEC 62061 і його імплементація у національне законодавство у сфері промислової безпеки є на даний час першочерговою задачею, яку необхідно як найшвидше вирішувати.

Мета роботи: визначення основних особливостей і порядку застосування відповідних процедур, що передбачені стандартом IEC 62061 щодо проектування та розробки пов'язаних з безпекою систем управління промисловим обладнанням, в яких використовуються електричні, електронні та програмовані електронні системи управління (ПБЕСУ).

Методики, матеріали і результати досліджень. Згідно із стандартом IEC 62061 ПБЕСУ повинна бути розроблена (або обрана) з урахуванням специфікації вимог до системи безпеки і, де це необхідно, з урахуванням специфікації вимог до програмного забезпечення системи безпеки.

ПБЕСУ повинна відповідати:

a) вимогам безпеки апаратних засобів, включаючи:

- обмеження архітектури на повноту безпеки апаратних засобів;
- вимоги до ймовірності небезпечних випадкових відмов апаратних засобів:

b) вимогам до систематичної повноті безпеки, включаючи:

- вимоги до можливості уникнути відмови;
- вимоги до управління систематичними помилками;

c) вимогам до поведінки ПБЕСУ при виявленні помилки;

d) вимогам проектування та розроблення пов'язаного з безпекою програмного забезпечення.

Проект ПБЕСУ повинен враховувати можливості і обмеження людини (в тому числі розумно передбачуване неправильне використання) і бути придатним для дій, які виконуються операторами, обслуговуючим персоналом та іншими категоріями осіб, які можуть взаємодіяти з ПБЕСУ.

Також необхідно, щоб при проектуванні всіх інтерфейсів враховувався «людський фактор», а також рівень підготовки або обізнаності оператора, особливо при масовому виробництві підсистем, коли оператором може бути будь-яка людина.

Мета проекту повинна полягати у тому, щоб розумно передбачувані помилки, зроблені оператором або обслуговуючим персоналом, були попереджені або усунені на етапі проектування. Якщо це неможливо, то, щоб мінімізувати можливість виникнення помилок оператора повинні бути також застосовані відповідні додаткові засоби (наприклад, реалізація дії вручну з додатковим підтвердженням перед її виконанням).

З метою сприяння реалізації вищезазначених властивостей, в ході розробки ПБЕСУ повинні бути також розглянуті питання ремонтопридатності та придатності спроектованої ПБЕСУ до тестування. Необхідно, щоб проект

ПБЕСУ, його діагностичні функції і функції реакції на відмову були документально оформлені, при цьому дана документація повинна:

- бути точною, повною і короткою;
- відповідати визначеній меті;
- бути доступною і підтримуваною.

Необхідно також зазначити, що дані, отримані в результаті проектування, розробки та реалізації ПБЕСУ, обов'язково повинні бути на відповідних етапах верифіковані.

У разі виникнення небезпечного збою в будь-який з підсистем, має бути передбачено виконання специфікованої функції реакції на відмову. Така специфікація може містити дії щодо ізоляції несправних частин підсистеми для продовження безпечної експлуатації машини в той час, як відбувається ремонт несправних частин.

Для запобігання систематичним відмовам апаратних засобів повинні бути застосовані наступні заходи:

a) ПБЕСУ повинна бути спроектована та реалізована згідно з планом функціональної безпеки;

b) правильні вибір, склад, схеми, складання та встановлення підсистем, в тому числі кабелів, проводів і будь-яких з'єднань;

c) застосування ПБЕСУ відповідно до специфікації виробника;

d) дотримання вказівок виробника щодо застосування, наприклад, інструкцій з установки та експлуатації (див. ISO 13849-2);

e) застосування підсистем з сумісними робочими характеристиками (див. ISO 13849-2);

f) ПБЕСУ повинна бути захищена відповідно до IEC 60204-1;

g) запобігання втрати функції заземлення відповідно до IEC 60204-1;

h) не повинні використовуватися документально не оформлені режими роботи компонентів (наприклад, «зарезервовані регістри» програмованого обладнання);

i) розгляд передбачуваного неправильного використання, змін умов навколишнього середовища і т.п.

Крім того, повинен бути застосований, принаймні, один з наступних методів і/або заходів, з урахуванням складності ПБЕСУ і рівня повноти безпеки (РПБ) для тих функцій, які будуть реалізовані ПБЕСУ:

a) аналіз проекту апаратних засобів ПБЕСУ (наприклад, за допомогою перевірки або наскрізного контролю) для виявлення в результаті оглядів і/або аналізу розбіжностей між специфікацією і реалізацією;

b) пакети і/або засоби автоматизованого проектування, що забезпечують функції моделювання та/або аналізу, що дозволяють виконувати процедури проектування на систематичній основі з використанням попередньо розроблених і протестованих елементів.

Для управління систематичними збоями повинні бути застосовані наступні заходи:

a) використання знеструмлення – ПБЕСУ повинна бути сконструйована таким чином, щоб при відключені електроживлення машини переходили в безпечний стан і залишалися в ньому;

b) контроль за впливом тимчасових відмов підсистеми - ПБЕСУ повинна бути сконструйована таким чином, щоб, наприклад:

- зміна напруги (переривання, падіння і т.п.) в окремих підсистемах або елементах підсистеми не приводило до виникнення будь-якої небезпеки (наприклад, переривання напруги, що впливає на електричні кола управління двигуном, не повинно привести до його несподіваного запуску в тому випадку, коли електроживлення двигуна відновлено);

c) управління наслідками помилок і іншими наслідками, що виникають в результаті будь-якого процесу передачі даних, включаючи помилки передачі, видалення, вставки, повторне упорядкування, спотворення, затримка і нелегальне проникнення.

** Примітки:*

1. Більш детальну інформацію можна знайти в IEC 60870-5-1, EN 50159-2 і IEC 61508-2.

2. Термін «нелегальне проникнення» означає, що справжній зміст повідомлення визначено неправильно. Наприклад, повідомлення від небезпечного компонента прийняті як повідомлення від безпечного.

d) якщо в інтерфейсі відбувається небезпечний збій, то повинна бути виконана функція реакції на відмову до того, як може статися небезпека через цей збій. Якщо відбувається збій, який знижує стійкість до відмов апаратних засобів до нуля, то реакція на цей збій повинна бути виконана за час, що не перевищує передбачуваний середній час відновлення /MTTR/. Вимоги, перераховані в даному пункті, відносяться до інтерфейсів, які є входами і виходами підсистем і всіх інших частин підсистем, що включають або використовують кабельні з'єднання в процесі інтеграції (наприклад, вихідний сигнал перемикання пристрою світлової завіси, вихід датчика положення огорожі і т.п.).

** Примітка: Підсистема або її елемент не повинні самі виявляти збій на своїх виходах. Функція реакції на відмову може бути ініційована також будь-якою подальшою підсистемою після виконання діагностичного тесту.*

Для функціональної безпеки ПБЕСУ повинна відповідати наступним критеріям щодо електромагнітної стійкості (Directive 2014/30/EU):

- небезпечні умови або небезпеки не повинні вноситься;

- пов'язані з безпекою функції управління (ПБФУ) повинні виконуватися без збоїв;

- виконання ПБФУ, що реалізуються ПБЕСУ, може бути порушено тимчасово або постійно, якщо безпечний стан машини підтримується або досягнуто до виникнення небезпеки. Якщо електромагнітні (ЕМ) явища можуть призвести до пошкодження компонентів, то необхідно впевнитися (наприклад, шляхом аналізу), що вони не будуть впливати на функціональну безпеку, в

тому числі і для більш низьких значень параметрів ЕМ явищ, які можуть привести до часткового пошкодження компонентів.

При проектуванні та розробці ПБЕСУ повинні виконуватися наступні основні загальні вимоги:

1. ПБЕСУ повинна бути спроектована і розроблена відповідно до специфікації вимог до безпеки ПБЕСУ.

2. Необхідно дотримуватися чітко структурованого процесу проектування, який повинен бути документально оформлений.

3. Якщо для досягнення необхідної повноти безпеки при виявленні збою є потреба у застосуванні діагностики, то ПБЕСУ повинна забезпечувати виконання заданої функції реакції на відмову.

4. Якщо ПБЕСУ або компонент ПБЕСУ (тобто її підсистема (и)) реалізує (ють) ПБФУ і інші функції, які не стосуються безпеки, то всі її технічні засоби і програмне забезпечення повинні розглядатися як пов'язані з безпекою до тих пір, поки не буде встановлено, що ПБФУ і інші не пов'язані з безпекою функції виконуються досить незалежно (тобто відмова будь-якої функції, що не стосується безпеки, не стане причиною відмови ПБФУ).

5. Якщо ПБЕСУ або її підсистеми реалізують ПБФУ з різними РПБ, то вимоги до апаратних засобів і програмного забезпечення ПБЕСУ або її підсистем повинні визначатися ПБФУ з найвищим РПБ, якщо не буде встановлено, що виконання ПБФУ з різними РПБ досить незалежно.

6. З'єднання (наприклад, провідники, кабелі), крім тих, що використовуються для цифрової передачі даних, повинні розглядатися як елементи однієї з підсистем, до якої вони підключені.

7. Якщо система цифрової передачі даних реалізується як частина ПБЕСУ, то вона повинна задовольняти відповідним вимогам IEC 61508-2 відповідно до цільового значенням РПБ для ПБФУ.

8. Інформація щодо застосування ПБЕСУ повинна визначати методи і заходи, необхідні для використання протягом проектних стадій життєвого циклу ПБЕСУ і забезпечення відповідного РПБ.

Проектування і розробка ПБЕСУ повинні виконуватися відповідно до чітко визначеного процесу, що враховує всі пов'язані з ним аспекти. У стандарті IEC 62061 використовується підхід, заснований на застосуванні структурованого процесу проектування ПБЕСУ. Нижче наведено порядок процесу проектування і термінологія, яка застосовується на різних його стадіях:

1. Визначити пропоновані ПБЕСУ для кожної ПБФУ відповідно до специфікації вимог до системи безпеки (СВСБ).

2. Для кожної функції виконати декомпозицію ПБФУ до функціональних блоків і створити початкову концепцію архітектури.

3. Деталізувати вимоги безпеки для кожного функціонального блоку.

4. Виділити функціональні блоки для підсистем ПБЕСУ.

5. Виконати верифікацію.

Що стосується проектування архітектури ПБЕСУ, то кожна ПБФУ, як зазначено в специфікації вимог до безпеки ПБЕСУ, повинна бути структурно

декомпозована до рівня функціональних блоків, наприклад, як це показано на рис.1.

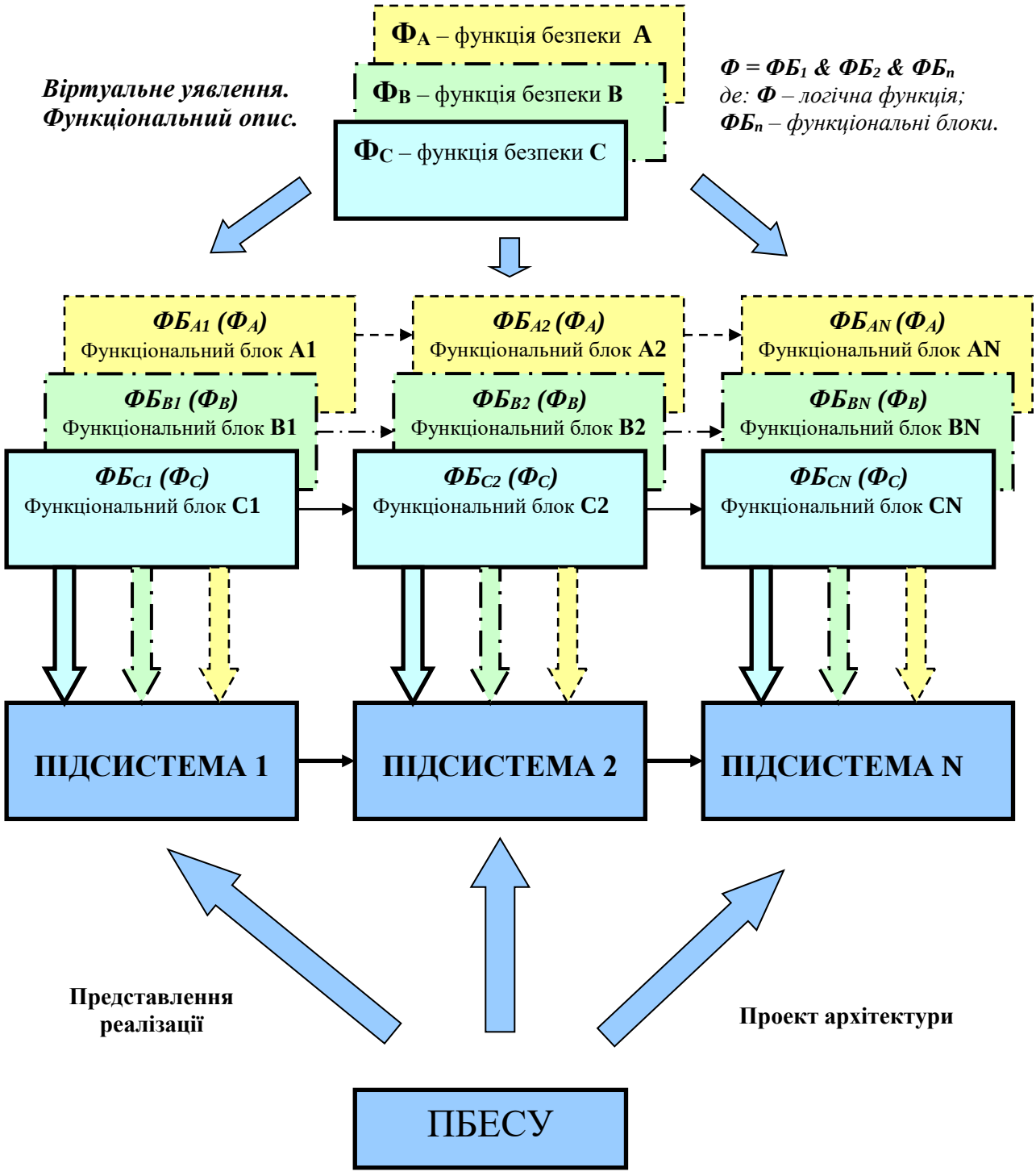

Рис. 1. Розподіл вимог до безпеки між функціональними блоками в підсистемах

Обов’язково необхідно, щоб така структура була документально оформлена і включала:

- її опис;

- вимоги до безпеки (функціональні вимоги та до повноти безпеки) для кожного функціонального блоку;

- визначення входів і виходів кожного блоку.

** Примітки:*

1. Процес декомпозиції дозволяє сформувати структуру функціональних блоків, яка повністю описує функціональні вимоги і вимоги до повноти ПБФУ. Цей процес повинен бути застосований до рівня, що дозволяє встановити функціональні вимоги і вимоги до повноти безпеки для кожного функціонального блоку, який буде реалізований в підсистемі.

2. На входах і виходах кожного функціонального блоку може бути інформація, що підлягає обробці (наприклад, про швидкість, положення, режим роботи тощо).

3. Функціональні блоки представляють функції ПБФУ і не включають діагностичні функції ПБЕСУ (для досягнення цілей стандарту IEC 62061-1 діагностичні функції розглядаються як окремі, що можуть мати структуру, відмінну від ПБЕСУ).

Необхідно, щоб початкова концепція архітектури ПБЕСУ була створена відповідно до структури функціональних блоків.

Кожен функціональний блок повинен бути реалізований відповідної підсистемою в архітектурі ПБЕСУ (одна підсистема може реалізовувати в собі більше одного функціонального блоку).

Кожна підсистема і реалізовані в ній функціональні блоки повинні бути чітко визначені.

Необхідно, щоб архітектура була документально оформлена, а її підсистеми і їх взаємозв'язок були детально описані.

Вимоги до безпеки для кожного функціонального блоку повинні бути сформульовані, як зазначено в специфікації вимог до безпеки відповідної ПБФУ, а саме стосовно:

- функціональних вимог (наприклад, вхідна та вихідна інформація функціонального блоку, внутрішня логіка роботи);

- вимог до повноти безпеки.

Вимоги з безпеки для підсистеми повинні бути такими ж, як і для функціональних блоків, які вона реалізує. Якщо система реалізує більше одного блоку, то для неї застосовується вимога з найбільшим значенням повноти безпеки. Ці вимоги повинні бути документально оформлені у вигляді специфікації вимог до безпеки системи.

Процес проектування і розробки підсистеми повинен чітко дотримуватися визначеної процедури, що враховує всі аспекти, які охоплюються цим процесом. Структура даного процесу приведена на рис.2.

Висновки. Приведені в даній роботі матеріали повинні допомогти інженерно-технічним працівника щодо запровадження у процес проектування та виготовлення промислового обладнання стандарту IEC 62061, який регламентує вимоги безпеки при проектуванні та розробці пов'язаних з

безпекою систем управління, в яких використовуються електричні, електронні та програмовані електронні системи управління.

Також ці матеріали свідчать про необхідність подальшої прискореної імплементації вітчизняного та європейського законодавств в сфері промислової безпеки.

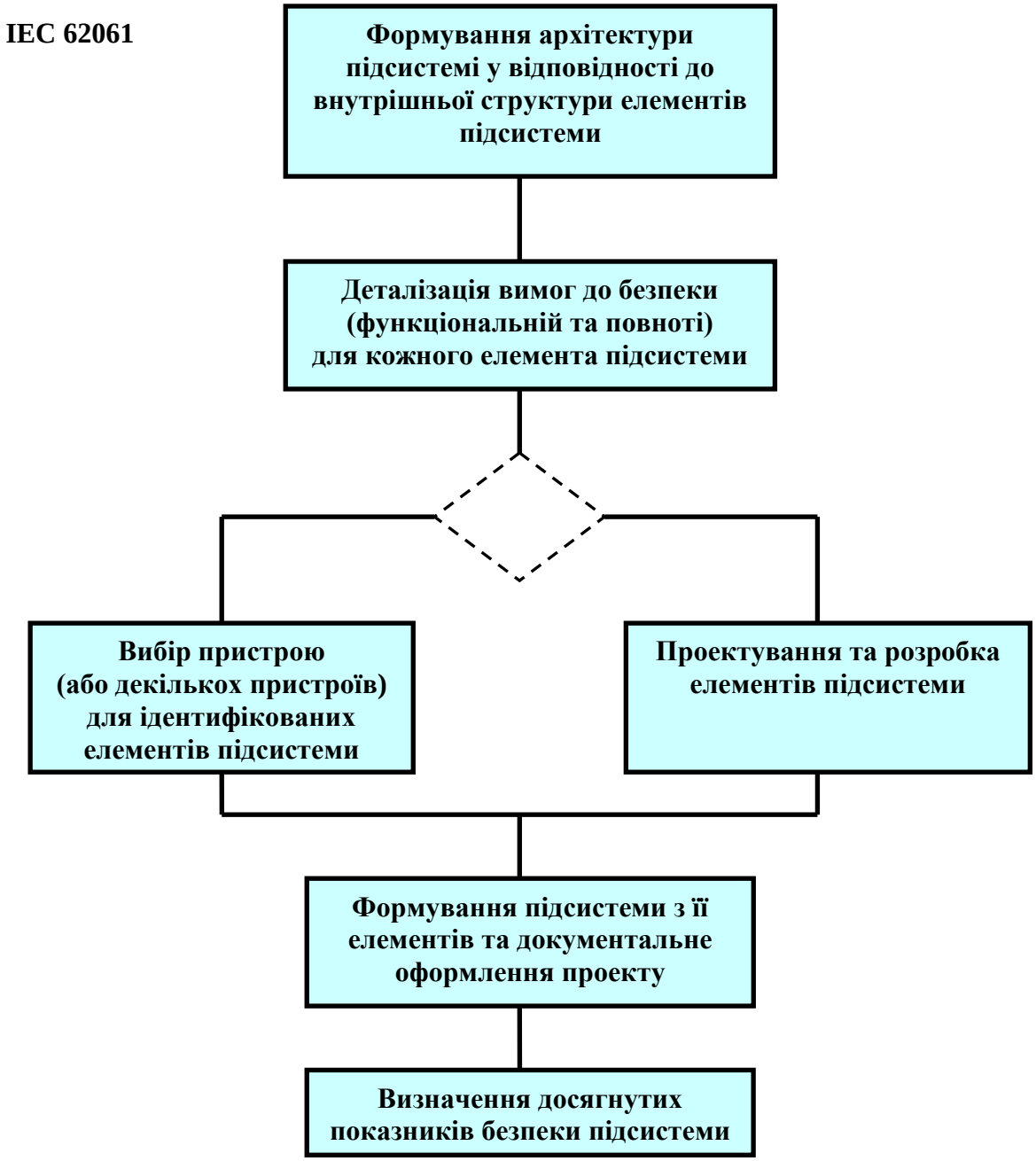

Рис. 2. Структура процесу проектування та розробки підсистеми

Необхідність впровадження стандарту IEC 62061, який регламентує вимоги безпеки при проектуванні та розробці ПБЕСУ промисловим обладнанням, безумовно, є першочерговою задачею, яку необхідно вирішити, і зробити це

необхідно як найшвидше. Без вирішення цієї задачі Україна не в змозі буде в подальшому ефективно конкурувати на європейському та світовому ринках.

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».